AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE 1 OF PAGES 497

2. CONTRACT (Proc. Inst. Ident.) NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
NNN12AA01C	10/1/12	

5. ISSUED BY	CODE	6. ADMINISTERED BY (If other than item 5)	CODE
NASA Management Office 4800 Oak Grove Drive Pasadena, CA 91109	NMO		

7. NAME AND ADDRESS OF CONTRACTOR	8. DELIVERY
California Institute of Technology 1200 East California Boulevard Pasadena, CA 91125-0001	☐ FOB ORIGIN ☑ OTHER (See below)
	9. DISCOUNT FOR PROMPT PAYMENT: N/A
CODE FACILITY CODE	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO ADDRESS SHOWN IN — ITEM

11. SHIP TO/MARK FOR	CODE	12. PAYMENT WILL BE MADE BY	CODE
See Section D herein		NASA/Goddard Space Flight Center Accounts Department, Code 155/Bldg 17, Room S240 Greenbelt, MD 20771	NMO

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
☑ 10 USC 2304(c) ( ) ☐ 10 USC 253(c) ( )	

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F AMOUNT
	See Section B herein				
				15G. TOTAL AMOUNT OF CONTRACT ▶	B-2

16. TABLE OF CONTENTS

	SEC	DESCRIPTION — PART I — THE SCHEDULE	PAGE		SEC	DESCRIPTION — PART II — CONTRACT CLAUSES	PAGE
✓	A	SOLICITATION/CONTRACT FORM	1	✓	I	CONTRACT CLAUSES	145
✓	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2			PART III – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
✓	C	DESCRIPTION/SPECS/WORK STATEMENT	14	✓	J	LIST OF ATTACHMENTS	172
✓	D	PACKAGING AND MARKING	24			PART IV — REPRESENTATIONS, CERTIFICATIONS	
✓	E	INSPECTION AND ACCEPTANCE	25		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
✓	F	DELIVERIES OR PERFORMANCE	26		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
✓	G	CONTRACT ADMINISTRATION DATA	32		M	EVALUATION FACTORS FOR AWARD	
✓	H	SPECIAL CONTRACT REQUIREMENTS	57				

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

☑ 17. CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 2 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)

☐ 18. AWARD (Contractor is not required to sign this document.) Your offer on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.

19A. NAME AND TITLE OF SIGNER (Type or print)	20A. NAME OF CONTRACTING OFFICER
Dean Currie, Vice President for Business & Finance	Angel A. Castillo

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
BY CALIFORNIA INSTITUTE OF TECHNOLOGY (Signature of person authorized to sign)	8/15/2012	BY Angel A. Castillo (Signature of Contracting Officer)	8/16/2012

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is usable

STANDARD FORM 26 (REV. 12/2002)
Prescribed by GSA FAR (48 CFR) 53.214(c)

TABLE OF CONTENTS

SECTION A—SF 26 1

PART I—THE SCHEDULE 2

SECTION B—SUPPLIES OR SERVICES AND PRICE/COSTS 2
- B-1 Scope 2
- B-2 Estimated Cost 2
- B-3 Cost and Performance Incentives for Tasks 3
- B-4 Budgetary Estimates and Funding 3
- B-5 Allowable Costs 4
- B-6 Contractor Financing by Letter of Credit (LOC) 12
- B-7 Fixed Fee 13
- B-8 Contractor Evaluation 13

SECTION C—DESCRIPTION/SPECIFICATION/WORK STATEMENT 14
- C-1 Description of Work 14
- C-2 Resources for Performance of the Contract 18
- C-3 Use of Other Facilities and Locations 18
- C-4 Facilities Management Provisions 19
- C-5 Excess and Surplus Equipment 22
- C-6 Specific Agreement on Organizational Authority 22
- C-7 Authorized Work 22

SECTION D—PACKAGING AND MARKING 24
- D-1 Packaging and Marking 24

SECTION E—INSPECTION AND ACCEPTANCE 25
- E-1 Listing of Clauses Incorporated by Reference 25

SECTION F—DELIVERIES OR PERFORMANCE 26
- F-1 Term of this Contract 26
- F-2 Deliveries 26
- F-3 Stop-Work Order (FAR 52.242-15) (AUG 1989) (ALT I) (APR 1984) (Deviation) 26
- F-4 Bills of Lading (NFS 1852.247-73) (JUN 2002) (Deviation) 27
- F-5 General Reports and Plans 28

SECTION G—CONTRACT ADMINISTRATION DATA 32
- G-1 Listing of Clauses Incorporated by Reference 32
- G-2 Cost Segregation and Reporting 32
- G-3 Property Reporting 37
- G-4 List of Government Property Furnished Pursuant to FAR 52.245–1 (JAN 2011) (NFS 1852.245-76) (Deviation) 37
- G-5 Task Ordering Procedure (NFS 1852.216-80) (OCT 1996) (Deviation) 38
- G-6 Transfers of Funds Between Task Orders 40
- G-7 Funds Procedure for Termination of Task Orders 41
- G-8 Identification and Marking of Government Equipment 42
- G-9 Small Business Subcontracting Plan 42
- G-10 Program/Project Management 43

G-11 Use of Department of Defense Services 45
G-12 References to FAR “Rights in Data” Clause 45
G-13 NASA Issuance System and Government Policies....45
G-14 Export Control Regulations 47
G-15 Facilities....49
G-16 Designation of New Technology Representative and Patent Representative (NFS 1852.227-72) (JUL 1997)....50
G-17 Management and Oversight of Property at Overseas Tracking Stations 51
G-18 Allocated Direct Cost Reporting....51
G-19 Whole Agreement 53
G-20 NFS 1852.245-70, Contractor Requests for Government-Provided Equipment (JAN 2011)(ALT I)(JAN 2011)....53
G-21 Financial Management....55
G-22 Cost Accruals....55
G-23 Travel 56
G-24 NFS 1852.245-78, Physical Inventory of Capital Personal Property (JAN 2011)....56
SECTION H—SPECIAL CONTRACT REQUIREMENTS 57
H-1 Listing of Clauses Incorporated by Reference....57
H-2 Representations and Certifications 58
H-3 Key Personnel and Facilities....58
H-4 Management Controls....59
H-5 Executive Orders....60
H-6 Wages, Salaries and Personnel Data....60
H-7 Safety, Health, and Mission Assurance 60
H-8 Environmental Matters....86
H-9 Energy Management 88
H-10 Occupational Health Services....90
H-11 External Communications and Visitor Requests From Elected Officials and Those Known To Be Seeking Elected Office....91
H-12 Handling, Protection and Release of Restricted Information 91
H-13 Subcontract New Technology and Patent Follow-Up 96
H-14 Patent and New Technology Services....97
H-15 NASA Offices....98
H-16 Property Rights in Records....99
H-17 Service Contracts 102
H-18 Limitation of Liability....102
H-19 Support for Historically Black Colleges and Other Minority Universities....103
H-20 Construction Clauses 103
H-21 Audit Negotiation—Access to Computers....103
H-22 Competition in Subcontracting 104
H-23 Application of Cross-Waivers of Liability 104
H-24 Advisory and Assistance Services 104
H-25 Subcontractor Progress Payments....105
H-26 Additional NASA Requirements 105
H-27 Clause Flowdown Requirement....106

H-28 Printing, Duplicating, and Copying 107
H-29 Clauses Applicable on a Task Order Basis 108
H-30 Cost Accounting Standards—JPL Subcontractors 109
H-31 Protection of Scientific and Technical Information of National Interest 110
H-32 End of Contract Options 111
H-33 Transition Activities 114
H-34 Transition From Contract NAS7-03001 115
H-35 Stop-Work Order 117
H-36 Security 117
H-37 Agreement on Computer Software 121
H-38 Agreement on Establishment of Rights, Technology Transfer, and Distribution of Income With Respect to Mask Works 122
H-39 Government-Furnished Computer Software and Related Technical Data 123
H-40 Payment of Overtime Premiums 125
H-41 Required Sources of Supplies and Services 125
H-42 Use of Facilities Plan 125
H-43 Information Technology 125
H-44 Litigation Management Plan 128
H-45 Integration of Environment, Safety, and Health Into the Contractor's Management System 129
H-46 NASA Authority During Emergencies 132
H-47 NASA Office of the Inspector General Programs 132
H-48 Response to Information Correction Requests 133
H-49 Coordination With NASA on Notices and Corrective Actions 133
H-50 Aircraft Operations 134
H-51 Transportation Efficiency 136
H-52 Reserved 136
H-53 Limitation of Future Contracting 136
H-54 Advance Payments 138
H-55 Liability for Subcontractor's Defective Cost or Pricing Data 139
H-56 Requirement for Information Technology Budget Plan 139
H-57 Reserved. 140
H-58 Monthly Property Financial Reporting 140
H-59 American Recovery and Reinvestment Act ("Recovery Act") 140
H-60 Systems Engineering 141
H-61 Software Engineering Requirements 141
H-62 Non-Applicability of Lower-Tier Documents 142
H-63 Responsibilities of Contractor Personnel 142
H-64 Flight Projects Product Data Management 142
H-65 Implementation of FAR 52.222-54, Employment Eligibility Verification (JAN 2009) 142
H-66 Post-Retirement Benefits Liability Re-Opener Clause 142
H-67 Reserved 143
H-68 Contractor's Use of Government Property 143
H-69 Implementation oF FAR 52.203-13, Contractor Code of Business Ethics and Code of Conduct (APR 2010) 144

H-70 Implementation of NFS 1852.235-73, Final Scientific and Technical Reports (DEC 2006) 144

PART II—CONTRACT CLAUSES 145

SECTION I—CONTRACT CLAUSES 145
I-1 Listing of Clauses 145
I-2 Incorporation in Full Text 150
I-3 Clauses Incorporated by Reference (FAR 52.252-2) (FEB 1998) 150
I-4 Ombudsman (NFS 1852.215-84) (NOV 2011) (Alternate I) (JUN 2000) 150
I-5 Subcontracts (FAR 52.244-2) (OCT 2010) (ALT I) (JUNE 2007) (Deviation) ..151
I-6 Security Classification Requirements (NFS 1852.204-75) (SEP 1989) 154
I-7 Security Requirements for Unclassified Information Technology Resources, NFS 1852.204-76 (JANUARY 2011) (Deviation) 154
I-8 Restriction on Funding Activity with China (1852.225-71) (FEB 2012) (Mod 6) 1577
I-9 Allowable Cost and Payment (FAR 52.216-7) (JUN 2011) (Deviation) 157
I-10 Termination for Convenience of the Government (Educational and Other Nonprofit Institutions)(FAR 52.249-5) (SEP 1996) (Deviation) 160
I-11 Advance Payments (FAR 52.232-12) (MAY 2001) (ALT II) (MAY 2001) (ALT IV) (APR 1984) (ALT V) (MAY 2001) as Modified by NFS 1852.232-70 (MAR 2010) (Deviation) 163
I-12 Limitation of Costs (FAR 52.232-20) (APR 1984); Limitation of Funds (FAR 52.232-22) (APR 1984) (Deviation) 169
I-13 Notification Prior to Acquiring Information Technology Systems from Entities Owned, Directed or Subsidized by the People's Republic of China, NFS 1852.225-74 (JUNE 2013)(DEVIATION) (from PIC 13-04) (Mod 7**)……..172**

PART III—LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS 174

SECTION J—LIST OF ATTACHMENTS 174
J-1 List of Documents, Exhibits, and Attachments 174

ATTACHMENTS
A — Foreign Travel .... 1 of 1
B — NASA-JPL Policies and Procedures Regarding Public Information Programs and New Issuances .... 1 of 3
C — Bibliography of NASA Directives Contractually Implemented .... 1 of 17
D — Small Business Subcontracting Plan .... 1 of 16
E — Contract Data Requirements List (Mod 6) .... 1 of 11
F — DD Form 254 .... 1 of 3
G — Agreement and Conditions for Evaluation of Proposals .... 1 of 1
H — JPL NPR 1600, NASA Physical and Program Security .... 1 of 72
I — JPL NM 1600-96, Personnel Security .... 1 of 17
J — JPL NPR 1620.2, Facility Security Assessments .... 1 of 16
K — JPL NPR 1620.3, Physical Security Requirements for NASA Facilities and Property .... 1 of 106
L — JPL NPR 1660.1B,Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements .... 1 of 1
M — JPL NM 1600-95, ID and Credential Management .... 1 of 63

APPENDIX 1—NASA and Caltech Understanding Concerning the Jet Propulsion Laboratory ..... 1 of 4

PART I—THE SCHEDULE

SECTION B—SUPPLIES OR SERVICES AND PRICE/COSTS

B-1 SCOPE

(a) This Contract is the sponsoring agreement between the National Aeronautics and Space Administration (NASA) and the California Institute of Technology (Contractor), a private nonprofit educational institution, which establishes the relationship for the operation of the Federally Funded Research and Development Center (FFRDC) known as the Jet Propulsion Laboratory (JPL). This Contract is the only document that constitutes the sponsoring agreement between the parties.

(b) As reflected in FAR 35.017, contractors operating FFRDCs are allowed access to Government and supplier data, including sensitive and proprietary data, and to Government employees and facilities beyond that which is common to the normal contractual relationship. Because of this special relationship, JPL shall be operated in the public interest with objectivity and independence, be free from organizational conflicts of interest, and have full disclosure of its affairs to NASA. Additionally, the Contractor shall not use its privileged information or access to facilities to compete with the private sector in contravention of FAR 35.017. Notwithstanding the special relationship created by this sponsoring agreement, the California Institute of Technology is acting as a contractor and not as an agent of the Government.

(c) The Contractor shall perform the work that is designated in task orders issued by the Contracting Officer using procedures set forth in Article G-5 (Task Ordering Procedure). The general areas of such work for which the Contractor is encouraged to maintain its expertise to provide a quick response capability, are described in Article C-1 (Description of Work).

B-2 ESTIMATED COST

(a) The estimated cost of this Contract will be the sum of the estimated costs set forth in task orders issued hereunder, including all amendments thereto. It is anticipated that the Government will allot funds to task orders from time to time, and such funds shall be available for the payment of allowable costs incurred in the performance of work under the task orders, until the funds allotted equal the estimated costs set forth in the task orders. The amount of such allotted funds, as it may be changed from time to time, shall be specified in each task order.

(b) The minimum amount of supplies or services that shall be ordered during the effective period of this contract is $1,000,000. The maximum amount of supplies or services that may be ordered for the five (5) year period of the contract is $8,500,000,000. Notwithstanding the maximum amount of the Contract, the Government is not obligated to order work under this Contract beyond the minimum amount set forth above.

(c) The minimum amount is reached when the sum of the dollar amounts of all ordered supplies or services, except for any adjustments made pursuant to the Limitation of Cost or Limitation of Funds clause, equals or exceeds the minimum amount stated in paragraph (b) above.

(d) The maximum amount is reached when the sum of the dollar amounts of all ordered supplies or services, except for any adjustments made pursuant to the Limitation of Cost or Limitation of Funds clause, equals the maximum amount stated in paragraph (b) above.

(e) The maximum amount, if reached, precludes the issuance of new orders for supplies or services under this Contract. However, reaching the maximum amount does not preclude adjustments to the dollar amounts of existing placed orders, for actions that are within the scope of the placed orders, and which are made pursuant to existing contract authority, such as the Changes clause.

B-3 COST AND PERFORMANCE INCENTIVES FOR TASKS

The Government may require the incorporation of cost and/or performance incentives for task orders issued under this Contract. The performance incentives will measure the performance against the salient performance requirement, called "unit(s) of measurement," e.g., months in service or amount of data transmitted, identified in the task order. Performance incentives will be incorporated in the task order in accordance with Article G-5 (Task Ordering Procedure). These incentive fees are in addition to and not inclusive of the Contract's fixed fee.

B-4 BUDGETARY ESTIMATES AND FUNDING

(a) The Contractor shall prepare and submit budgetary estimates as directed by the Contracting Officer. The estimates shall set forth the funding requirements for each succeeding fiscal year remaining in the term of each task order under which the Contractor anticipates work will be performed. The budgetary estimates shall be supported by detailed discussions of the funding requirements, by a list of major procurements to the extent known at the time, and by such additional information as the Contracting Officer may need for planning purposes. The Contractor shall also prepare and submit budgetary estimates in the formats required by NASA in order to support NASA's annual Planning, Programming, Budgeting, and Execution (PPBE) submission. The Contractor shall submit the PPBE information per annual guidance supplied by NASA. The PPBE submission will be forwarded to the NASA Enterprises with a copy to the Contracting Officer.

(b) From time to time, the Contractor may submit revised budgetary estimates and recommend changes in the approved funding of any task order, or the issuance of new task orders. The Contracting Officer shall inform the Contractor of the action taken with respect thereto. In the event the Contracting Officer initiates changes in the approved funding, as much advance notice thereof as possible shall be provided to the Contractor.

(c) In the event of changes in approved funding, the Contracting Officer shall promptly issue task orders or task order amendments, in accordance with the procedure established in Article G-5 (Task Ordering Procedure), reflecting the changes.

B-5 ALLOWABLE COSTS

(a) General. For the purpose of determining the amounts payable to the Contractor under this Contract, the allowability of costs shall be determined by the Contracting Officer in accordance with:

(1) Federal Acquisition Regulation (FAR) Subpart 31.2, Contracts with Commercial Organizations, and

(2) The terms of this Contract.

Notwithstanding other requirements of this contract, when determining the allowability of costs relative to the institutional indirect costs, benefits, and Interdivisional Authorizations, such determinations will be consistent with A-21 cost principles, as stated in paragraph (c) below. In the case of an inconsistency between the provisions of this Contract and FAR Subpart 31.2, the provisions of this clause shall govern.

(b) Direct Costs. All costs incurred by the Contractor in connection with the operation of JPL under this Contract, except for those costs identified in paragraph (c), Institutional Indirect Costs, shall be considered direct costs.

(c) Institutional Indirect Costs. Allowable items of institutional indirect costs (also referred to as Facilities and Administration costs), originating from the campus of the Contractor and being charged to this Contract shall include the following:

(1) Campus Work. The Contractor shall be reimbursed for institutional indirect costs of work performed on the campus of the Contractor or at the Contractor's other non-JPL facilities during each of the Contractor's fiscal years. Reimbursement will be on the basis of those overhead rates for such fiscal years as are negotiated between the Contractor and representatives of the Government for those Government contracts under which the preponderance (in dollar amount) of Government work is performed on the campus of the Contractor. If a negotiated rate is provisional, the Contractor shall be reimbursed on the basis of this provisional rate, subject to an appropriate adjustment when the final rate for that period is established.

(2) JPL Work. In lieu of institutional indirect costs applicable to all other work performed by the Contractor for each of the Contractor's fiscal years, the Contractor shall be reimbursed in an amount negotiated between the parties for that fiscal year. The negotiated lump sum for institutional indirect costs will be an offset to the Contractor's total institutional indirect costs prior to the application of the overhead rate discussed in subparagraph (c)(1), above. Such negotiated amounts, and the period to which they apply, shall be set forth in modifications to this Contract. Pending an agreement as to such negotiated amount for each period, the Contractor shall be paid provisionally on a monthly basis in an amount of one-twelfth of the last negotiated amount. If the Government determines that the total amount of such provisional payments will substantially exceed the anticipated final negotiated amount for that period, the Contracting Officer will direct the suspension or reduction of future payments and/or request a prompt refund of excess payments as appropriate. In addition, the

Contracting Officer may reduce or withhold such provisional payments in the event the Contracting Officer determines that the Contractor has not submitted timely information to support its institutional indirect costs for such period.

Lump Sum Amounts Established By Bilateral Modifications:

YEAR	LUMP SUM AMOUNT	ACTUAL OR PROVISIONAL	MOD #
2012	$18,774,685	Actual	Mod 1
2013	$18,269,000	Provisional	Mod 1

(d) Discretionary Research Funds. The discretionary research funds are as follows:

(1) President/Director Research & Development Fund (PDRDF). In addition to funding otherwise made available to the Contractor for the performance of work under this Contract, the Contracting Officer shall, by separate task order, make available to the Contractor funding for use in the performance of discretionary research and development. This additional funding shall be used at the discretion of the President of Caltech and JPL's Director to fund joint research and technology efforts between Caltech Campus and JPL researchers. These efforts will fall within JPL's purpose and mission or special competencies and shall be known collectively as the "President/Director Research and Development Fund". The amount to be provided each year shall be $4,000,000. An appropriate amount will also be provided by non-NASA sponsors based upon work performed for them under Section C-1(b).

(2) Independent Research and Technology Development Program (IR&TD). NASA seeks to create an environment that encourages the Contractor to (i) expand knowledge in science and engineering, (ii) improve technology in areas consistent with the purpose and mission of JPL as NASA's FFRDC, (iii) enrich and broaden the spectrum of technology available to NASA, and (iv) establish and nurture collaboration with universities, other NASA centers, government laboratories, and industry.

(i) The parties agree that the Contractor's IR&TD Program will annually fund research and technology efforts. The Contractor's IR&TD projects will fall within the purpose and mission of JPL as an FFRDC as defined in Article C-1(a) of this Contract, and be conducted pursuant to the policies and procedures approved by the Contracting Officer. The Contractor shall obtain the Contracting Officer's

approval that all IR&TD program projects fall within the purpose and mission of JPL as an FFRDC.

(ii) The costs incurred by the Contractor for IR&TD activities are recognized by NASA as necessary costs of doing business, particularly in cutting-edge technologies required to meet current and future scientific requirements. IR&TD costs incurred by the Contractor shall be reimbursable as allocated direct expenses to the extent they are allocable, reasonable, and not otherwise unallowable by law under FAR 31.205-18. The cost of the Contractor's IR&TD projects shall be allocated through the general pool of the Contractor's allocated direct cost structure. The total annual budget for IR&TD projects shall not exceed three (3) percent of the Contractor's projected Modified Total Cost base at the beginning of each fiscal year.

(e) Other Advance Understandings. Allowable costs shall also include the items of cost listed in subparagraphs (1) through (13) below. Reimbursement of such costs shall be subject to the requirement that any such costs be reasonable in amount and allocable under applicable cost principles identified in paragraph (a), above.

(1) Anticipatory Costs. The parties agree that costs shall be allowable if incurred by the Contractor in anticipation of (i) this Contract, or (ii) a subsequently executed task order or task order amendment there under, which, if incurred after the execution thereof, would have been allowable items of cost. When the Contractor's management decides to incur costs prior to the execution of a task order or task order amendment pursuant to this subparagraph (1), the Contractor will simultaneously notify the Contracting Officer in writing.

(2) Public Information and Outreach. In order to assist NASA in the implementation of its mandate under the National Aeronautics and Space Administration Act of 1958, as amended (the "Space Act"), the Contractor will distribute and otherwise make information about NASA programs and accomplishments and about space and science developments freely available to the public. Costs for Government program-related printed, electronic (e.g., Internet) or other distributable information, displays or exhibits, media access, mailings, photographs, audio or video recordings, approved collections of information from the public, or other related expenses incurred by the Contractor to interact with and inform the public about space, science and technology developments for public events, activities marking accomplishments under this Contract, or educational outreach shall be allowable.

(3) Patent Infringement Litigation Costs. Costs of legal, accounting and other services, and related costs, incurred in connection with the defense of patent infringement litigation based on the performance of this Contract, of Contracts NAS7-03001, NAS7-1407, NAS7-1260, NAS7-918, NAS7-920(F), NAS7-100, or of NAS7-270(F), shall be allowable, provided the Contractor has complied with the requirements of FAR 52.227-2, Notice and Assistance Regarding Patent and Copyright Infringement, of this Contract, or of a similar provision in Contract(s) NAS7-03001, NAS7-1407,

NAS7-1260, NAS7-918, NAS7-920(F), NAS7-100 or NAS7-270(F), with respect to such litigation.

(4) Technology Transfer Activities. In furtherance of NASA's policy objective of encouraging technology transfer, costs incurred in promoting and facilitating U.S. public and private sector technology transfer consistent with the requirements of this Contract shall be allowable.

(5) Facilities Rearrangement and Alteration Costs. Costs incurred in special facilities modification or rearrangement shall be allowable where performed in accordance with the terms of this Contract (including any task order issued expressly therefore).

(6) Terminal Costs. In the event the Contract is terminated by the government for convenience or expires, the parties will engage in good faith negotiations to reach agreement on a settlement of costs associated with such termination or expiration, as dictated by the circumstances. For purposes of this clause, the parties acknowledge that any settlement reached in connection with a termination for convenience or Contract expiration will be referred to as the "termination settlement". The following cost types will be considered allowable cost types under a termination or expiration. These costs are illustrative of the types of allowable costs and are not intended to be all-inclusive.

(i) The Government agrees that it is reasonable for the Contractor to acquire necessary supplies and services on the assumption that the Contract will be renewed or extended. Unless the Government notifies the Contractor that the Contract will not be renewed or extended, the Government will not object to a termination, phase-down, or closeout inventory, reasonable when acquired, on the basis that the inventory is excess to the requirements of the performance of the work under contract for the term during which the inventory was acquired.

(ii) The termination settlement shall include an amount, to be determined on an actuarial basis, to compensate the Contractor for the allocable portion of future health and life insurance premiums for employees of the Contractor vested for retirement or retiring during the term of this Contract or of the preceding Contract NAS7-03001, Contract NAS7-1407, Contract NAS7-1260, Contract NAS7-918, Contract NAS7-920(F), Contract NAS7-100, Contract NAS7-270(F), or NASW-6 or retired upon or as a result of the termination of this Contract, to the extent that such employees' qualifications for such health and life insurance benefits were based on their service in performing work under this Contract, Contract NAS7-03001, Contract NAS7-1407, Contract NAS7-1260, Contract NAS7-918, Contract NAS7-920(F), Contract NAS7-100, Contract NAS7-270(F), or NASW-6.

(iii) Except as otherwise restricted by Article H-32(e)(6), the termination settlement shall include an allocable portion of terminal leave benefit payments (including, but not limited to accrued vacation time, severance, unused sick leave, and otherwise unfunded early retirement costs and pension obligations) made or owed to terminated and retired employees and employees who will be terminated or

retired in the future to the extent that such employees' entitlements were based on their service in performing work under this Contract, Contract NAS7-03001, Contract NAS7-1407, Contract NAS7-1260, Contract NAS7-918, Contract NAS7-920(F), Contract NAS7-100, Contract NAS7-270(F), or Contract NASW-6.

(iv) The termination settlement shall include an amount equal to the cost that it is estimated the Contractor will incur subsequent to termination in discharging its obligations under the provisions and clauses of this contract which require retention of Contractor records.

(v) The termination settlement shall include a provisional amount equal to the estimated cost of benefits which the Contractor will be required to pay into any state unemployment fund subsequent to the termination for convenience of this Contract, based on compensation paid to employees in the performance of this Contract, Contract NAS7-03001, Contract NAS7-1407, Contract NAS7-1260, Contract NAS7-918, Contract NAS7-920(F), Contract NAS7-100, Contract NAS7-270(F), or Contract NASW-6. The provisional amount will be adjusted to reflect the actual amount of payments made into such unemployment funds, as soon as the actual amount of payments can be finally determined under applicable state and federal law. This understanding is based on the fact that the Contractor has elected to finance its liability for unemployment compensation and related benefits on a cost-of-benefits basis.

(vi) The termination settlement shall include a provisional amount equal to the estimated cost of workers' compensation and employer's liability benefits (including benefits under the Longshoremen's and Harbor Workers' Compensation Act) which the Contractor will be obligated to pay over to the State Compensation Insurance Fund of the State of California, or to any other state compensation or employer's liability carrier, subsequent to the termination for convenience of this Contract, based on injuries or death resulting from such injuries sustained in the performance of this Contract, Contract NAS7-03001, Contract NAS7-1407, Contract NAS7-1260, Contract NAS7-918, Contract NAS7-920(F), Contract NAS7-100, Contract NAS7-270(F), or Contract NASW-6. This provisional amount will be adjusted to reflect the actual amount of payments made to such fund or carrier, as soon as the actual amount of payments can be finally determined under the provisions of the applicable insurance contract or applicable state or federal law.

(7) Treatment of CERCLA Environmental Costs. NASA has designated both the Department of the Army and the California Institute of Technology (Contractor) as potentially responsible parties (PRP) under the Comprehensive Environmental Response, Compensation and Liability Act (CERCLA), as amended by 42 U.S.C. §9601 (et seq.,) for purposes of allocating the cost of responding to JPL CERCLA contamination. In 1992, the facility known as JPL was placed on the National Priorities List of Superfund sites. The designation of PRP was made in accordance with the CERCLA. This clause shall govern the extent to which the Contractor can charge its

CERCLA environmental costs as a PRP to this Contract. This clause does not recognize or create any Government liability for the Contractor's PRP CERCLA liability in the absence of a contract between the Contractor and NASA to operate JPL as an FFRDC. Additionally, this clause does not create or constitute an admission of liability by the Contractor. The parties agree that, at a minimum, any allowable costs flowing from PRP CERCLA liability associated with the Contractor's business organization referred to as JPL can be treated as an allocated direct cost (ADC) to this Contract. To the extent a cost arises from environmental wrongdoing, as defined in the DCAA manual, NASA shall not consider it an allowable cost under this Contract. The Contractor specifically reserves the right to contest determinations of allowability, including the appropriateness and/or application of the DCAA standard of environmental wrongdoing, pursuant to the Disputes provision of this Contract. Any other PRP liability apportioned to the California Institute of Technology (Caltech) which constitutes an allowable cost can be treated as an institutional F&A cost. Additionally, Caltech agrees, when cost effective, to pursue any insurance claims relative to its liability under CERCLA as a PRP. The parties agree that insurance proceeds that the California Institute of Technology receives as reimbursement for CERCLA liability shall be applied as a credit against CERCLA environmental costs which were or would be otherwise allowable under this Contract.

(8) Caltech Faculty Consulting Costs. In addition to work performed by Caltech faculty for JPL under interdivisional transfers issued to the Contractor's campus by JPL, Caltech faculty may be utilized by JPL as consultants only if the needs of the Laboratory cannot be met by JPL staff or more cost effective sources.

(i) Caltech faculty will be used sparingly by JPL as consultants and the circumstances of their engagement will normally meet each of the conditions set forth below:

(A) The consultant(s) are especially qualified by education or by experience to perform some specialized service in a particular field.

(B) The specialized service to be performed is the provision of advice to JPL management, typically in a technical area.

(C) The consultant(s) contribute their knowledge but normally do not physically perform the work involved.

(D) The consultant(s) are retained as problem solvers since their expertise allows them to recommend solutions when it is not economical or prudent for JPL to work out the solutions.

(E) The consultant(s) do not supervise or perform operating functions.

(ii) Individual Caltech faculty may provide consulting services to JPL for a maximum of 48 workdays per Caltech fiscal year, in accordance with (i) above and Caltech policy, unless other arrangements are approved in advance by the Contracting Officer.

(iii) Caltech faculty engaged by JPL as consultants shall be compensated for such services on a daily basis at a rate equal to 100 percent of their daily campus salary unless a greater amount is approved in advance by the NMO Procurement Officer. In addition to their compensation, Caltech faculty engaged by JPL as consultants will be reimbursed for allowable transportation, subsistence and other costs necessary for performing the consulting assignment. Transportation between the Campus and JPL will not be reimbursed.

(iv) To the extent that foreign travel is involved, approval is required in accordance with Attachment A.

(9) Litigation Costs. This advance agreement only applies to certain litigation costs the Contractor incurs when it fails to prevail in court or at an administrative board. Specifically, the parties agree that when the Contractor litigates a third party suit and a court or an administrative board finds that the Contractor violated Federal law, the Contractor's legal cost and judgment costs will be allowable only when the Contractor can demonstrate it had a reasonable expectation of prevailing on the merits. The test regarding "reasonable expectation of prevailing" is whether (1) there was a reasonable basis for the facts asserted; (2) there was a reasonable basis for the theory of law advanced; and (3) there was factual support for the legal theory. Additionally, this advance agreement does not alter the requirement that costs also must be reasonable and allocable.

(10) Other Cost Agreements. The NMO Procurement Officer may also approve other advance agreements with the Contractor regarding the allowability of particular types of cost.

(11) Intergovernmental Personnel Act (IPA).

(i) With prior written approval, the Contractor's personnel may be assigned temporary duties in accordance with the Intergovernmental Personnel Act (IPA). When the IPA assignment is to a NASA organization, the Contractor shall support its request for approval with a written endorsement from the applicable NASA proponent organization. When the IPA assignment is to a non-NASA sponsor, the Contractor shall, at a minimum, also support its request for approval by specifically (i) referencing to one or more appropriate subparagraphs of C-1(a) or the special competency of JPL and (ii) demonstrating the anticipated benefits to be gained from participating in the IPA assignment with NASA's mission. Such temporary assignments shall be provided under separate IPA agreements rather than this contract. The negotiation of such IPA agreements will include the costs of Contractor employees direct labor cost, employee benefits and other direct costs (e.g., travel) while on temporary assignment. These costs shall be reimbursed under such IPA agreements and not this contract.

(ii) The costs associated with negotiating, managing and providing administrative support to such Contractor employees temporarily assigned under an IPA Agreement are not in the nature of personal services. These costs shall therefore

be reimbursed under the terms of this contract and not the individual IPA Agreements. Accounting review disclosed that IPA costs have a causal beneficial relationship with applicable allocated direct costs.

(iii) Pursuant to the concept of a single cost objective, the contracting parties have agreed to the exclusion of IPA costs from allocated direct costs. The parties have agreed to this cost accounting variance due to the immateriality of the IPA costs and the potential significant efforts associated with changing the existing cost accounting system. To allow for continuing cost monitoring, upon request by the NASA Management Office (NMO), the Contractor shall submit a cost report detailing incurred IPA costs, in order for the Government to reassess the materiality of the costs.

(12) Regarding the allowability of interest payments by the Contractor to its subcontractor, Honeywell Building Solutions -SES, under subcontract number 1273095 and any follow-on subcontract for the same work, the Government has properly executed an approval to deviate from Federal Acquisition Regulation (FAR) 31.205-20, Interest and Other Financial Costs, and 31.109(c), Advance Agreements.

(13) Regarding all payments (including but not limited to advance payments) to be made by the Contractor at the request of the Government, to the Government's energy conservation measures (e.g., HVAC and lighting upgrades) contractor(s), with which the Contractor has no privity of contract.

(i) A deviation from the allowability provisions of Federal Acquisition Regulation (FAR) Subpart 31.2, Contracts with Commercial Organizations, and FAR 31.109(c), Advance Agreements was properly executed under the Department of Energy's IDIQ contract DE-AM36-09G029031 which NASA has utilized, via task order issuance, for the performance of the energy conservation measures at JPL.

(ii) Any dispute by the Government's energy conservation measures (e.g., HVAC and lighting upgrades) contractor(s) regarding the payments made shall be the responsibility of and handled directly by the Government.

(iii) All requests to the Contractor to make payments to the Government's energy conservation measures (e.g., HVAC and lighting upgrades) contractor(s) shall be in writing, shall be issued by the NMO Contracting Officer, shall specify the amounts to be paid and by when (i.e., shall be a "payment schedule"), and shall include the name of the contractor(s) to be paid. Revisions to the payment schedule may be made by the NMO, in writing, at any time. The Contractor will draw the payments from an appropriate burden funded account.

(iv) The Contractor shall continue to provide technical management, general administrative and other support to NASA's energy conservation measures contracting effort as requested by NASA.

B-6 CONTRACTOR FINANCING BY LETTER OF CREDIT (LOC)

(a) Background. Payments to the Contractor shall be made upon the start of this Contract by the Letter of Credit (LOC) method through the Department of Health and Human Services—Payment Management System (DHHS/PMS) as set forth in NPR 9680.1A, NASA's Management of Grants and Cooperative Agreements, dated November 10, 2011, Appendix B, Letter of Credit Requirements for Recipients.

(b) Understandings. The Parties acknowledge:

(1) The Contractor shall submit requests for funds electronically through the DHHS/PMS system using the P account.

i. Authorizations and drawdowns under this contract will be made under the Contractor's current Entity ID Number (EIN) assigned P account number which includes prior activity from the predecessor contract NAS7-03001for the American Recovery and Reinvestment Act of 2009 (ARRA) task orders.

ii. LOC cash draws shall be processed at the NASA task order/DHHS /PMS subaccount level.

(2) The Contractor shall draw funds to meet current requirements.

(3) Cash draws shall be allocated across task orders based on a contract-to-date percentage of the current incurred cost records in the Contractor's Enterprise Business Systems, typically updated each business day (Mod 4). Cash draws for the predecessor contract NAS7-03001 ARRA task orders will continue using the predecessor contract's logic.

(4) The total value of draws against the subaccounts represents the Contractor's LOC claim.

(5) In support of NASA's fiscal month-end and year-end close process, the Contractor shall estimate its cash needs for the NASA defined LOC down time and draw as defined in (b) (1) and (b) (3) above. During such times it is recognized that disbursements may require up to ten working days. The Contractor will provide monthly reporting of the fiscal month-end estimated cash needs to the Goddard Space Flight Center Regional Finance Office (GSFC RFO) and year-end draw reporting of estimated cash needs to both the GSFC RFO and Contracting Officer.

(6) To expedite the flow of cash and in alignment with NPR 9680.1A, Section 1.2.4, the Contractor will notify the NASA Management Office (NMO) Procurement Office to promptly resolve funding variances between the Contractor's and NASA's financial systems;

(7) For funding variances resulting from cancelled funds withdrawals, the Contractor will work with the NMO Procurement Office to obtain a current year fund to cover allowable obligations incurred during the period of performance of the task order.

(8) The Contractor shall provide a monthly contract reconciliation of expenditures to LOC draws to the Contracting Officer and GSFC RFO.

(9) Separate reconciliations are required for predecessor contracts NAS7-1407and NAS7-03001.

(10) LOC certifications on Standard Forms SF 425, Federal Financial Report, SF 1034, Public Voucher for Purposes and Services Other Than Personal, and SF 1035, Public Voucher for Services Other Than Personal (Continuation Sheet), are based upon the total dollar amount drawn under the subaccounts. The Contractor will provide separate SF425 reports in PMS no later than 30 days following the end of each federal fiscal quarter for the open predecessor contracts NAS7-1260, NAS7-1407, NAS7-03001 and a consolidated reporting for the NAS7-03001ARRA task orders and new contract task order activity.

(11) The Contractor shall notify the GSFC RFO and NMO of pending actions for outstanding allowable Contractor costs within 90 days after task expiration.

(12) Specific processes that outline the procedures used to manage the LOC will be documented and provided to the Contracting Officer no later than sixty days after the Contract's effective date.

(c) Interest. All funds provided to the Contractor shall be maintained in interest bearing accounts. Interest earned shall be remitted monthly to DHHS with concurrent notice to the GSFC RFO.

B-7 FIXED FEE

In addition to allowable costs reimbursed per the provisions of the Contract, the Contractor shall be paid a fixed fee for its performance thereof in the amount of $21,000,000 annually. One-quarter of this amount, $5,250,000, shall be disbursed by NASA to the Contractor quarterly, through the end of the Contract. Each quarterly payment shall be made no later than 30 days after the end of each quarter. If the final Contract fee payment period is less than a full quarter, the $5,250,000 quarterly fixed fee amount shall be prorated and paid to the Contractor accordingly, no later than 30 days after the end of the Contract term.

B-8 CONTRACTOR EVALUATION

The Contractor shall submit a summary-level status on a mutually-determined set of Annual Performance Goals (APGs) for each fiscal year to support NASA's Fiscal Year Performance and Accountability Report reporting requirements. Reports in Contractor format shall be submitted semi-annually, at the mid-year point and at the end of each fiscal year.

[END OF SECTION]

SECTION C—DESCRIPTION/SPECIFICATION/WORK STATEMENT

C-1 DESCRIPTION OF WORK

(a) NASA—Sponsored Work. The Contractor's primary mission is to support the NASA Science Mission Directorate (SMD) in carrying out the specific objectives identified in the SMD Science Plan. The four broad scientific areas to be addressed, which coincide with the 2011 NASA Strategic Plan science sub-goals are: Earth Science, Planetary Science, Heliophysics, and Astrophysics. To achieve its primary mission, the Contractor must maintain its position as the unchallenged leader in deep-space and Earth-related scientific exploration by continually developing and maintaining the technical skills and infrastructure necessary to carry out such unprecedented scientific endeavors while making every effort to contain costs.

In the performance of this contract, the Contractor shall:

(1) Supply a broad base of scientific and technical capabilities relevant to NASA program and project responsibilities and assignments, and shall maintain professional staff capabilities at the highest level in order to derive as much technological and scientific data as possible from the actual performance of research and development work under this Contract.

(2) Foster its unique relationship with a top-tier university to facilitate the involvement of the premier scientists, engineers, and students from the university and research communities in NASA's mission and in supporting other government agencies' related projects.

(3) Support NASA in enabling program and institutional capabilities in accordance with NASA's 2011 Strategic Plan to conduct the Agency's aeronautic and space activities.

(4) Develop spacecraft and instruments that are sent to various destinations within our solar system, including Earth orbit, planets, planetary satellites, asteroids, and comets. These missions may be orbiters, landers, or rovers, and typically include cutting-edge technologies required to meet scientific requirements. Although instrument observations from and in space will be the primary tools for such explorations, investigations, and science programs, ground-based research and suborbital and laboratory experiments shall also be required for successful mission development and execution. A broad range of deep-space telecommunication capability, and management effort is also implicit in space mission assignments.

(5) The Contractor may perform project tasks involving: (i) autonomous deep-space, inner-space and earth-orbiting spacecraft or major subsystems, (ii) experiments, instruments, or other devices which may be carried as payload on spacecrafts in missions managed by others, an/or (iii) ground-based systems.

(6) Beyond its primary mission, the Contractor may perform work for other NASA Mission Directorates or offices. For example, the Contractor may propose or be assigned advanced technology research and development tasks that enable and enhance new space missions; shorten the mission development cycle; increase the effectiveness of land and spaced-based observation platforms; or provide improved modeling and research techniques that result in more effective planning of future missions and the operations of current missions and systems. Such tasks will support NASA's efforts to accelerate the pace of scientific discovery and may cover all areas described above, and may lead to additional NASA-required core competencies assigned to the Contractor.

(7) The Contractor may perform tasks which support NASA-sponsored Research and Analysis programs that carry out competed and peer-reviewed research, encompassing basic and applied research and technology development in space and Earth sciences. The Contractor may perform these tasks in both principal and supporting roles to enable effective project implementation and to further technological capabilities for future NASA requirements.

(8) The Contractor may support NASA's partnerships with other government agencies (Federal, State, or local), academia, and the private sector to leverage both NASA's and other Agency's investments in national objectives and to realize relevant societal benefits from NASA's research. Assigned tasks may include, but not be limited to, technology transfer, partnering, and commercialization activities that enhance the value and contribution of technology developed under the Contract resulting in the strengthening of the nation's technological competitiveness and prosperity, increasing the quality of life on this planet, and adding to the foundation of many other national priorities.

(9) The Contractor shall be responsible for the operation, research, technology insertion, and management of NASA's Deep Space Network to provide telecommunication and operation services, including data acquisition and data delivery required to meet established Agency objectives.

(10) The Contractor may assist NASA in the formulation and execution of programs and projects by providing technical advice, studies, and reports of investigations, compliant with the restriction cited in Article C-7 below.

(11) The Contractor shall maintain and conduct an education program in close coordination with the NASA Headquarters Education Office, the academic community at large, and in support to NASA's strategic objectives to improve student retention in the Science, Technology, Engineering, and Mathematics (STEM) disciplines and to promote STEM literacy through strategic partnerships with formal and informal organizations. The Contractor shall support NASA in accomplishing the Agency's Education Strategic Objectives and Annual Performance Goals.

(12) The Contractor shall maintain and conduct community outreach activities in close coordination with NASA Headquarters Office of Communications.

(13) The Contractor, when and as directed by the Contracting Officer consistent with NPR 2190.1B (effective date 12/27/11), Appendix E, NASA Fundamental Research Designation Guidelines , may perform fundamental research at JPL. "Fundamental Research" as used in this Contract is defined in Section E.2 of Appendix E of NPR 2190.1B. The Contractor may publish, release or otherwise disseminate data produced during the performance of task orders designated as fundamental research, including the final report, without prior review by NASA for export control or national security purposes. Notwithstanding the foregoing, the Contractor shall perform its responsibilities under Article F-5. Additionally, the Contractor is responsible for the reviewing of any publication, release or dissemination of the data for conformance with other restrictions expressly set forth in the Contract, and to the extent it receives or is given access to data necessary for the performance of the Contract which contains restrictive markings, for compliance with such restrictive markings. Nothing herein shall change the Contractor's obligations under Article H-36, SECURITY, including but not limited to restricting and monitoring access of foreign nationals to the JPL facility. Notwithstanding anything stated herein, and unless NASA otherwise specifies in the applicable task order, the Contractor is authorized (1) to perform work on the Caltech campus pursuant to Interdivisional Authorizations as Fundamental Research, and (2) to award subcontracts to perform Fundamental Research to subcontractors that are accredited institutions of higher learning in the United States. The Contractor may award subcontracts to perform Fundamental Research to other types of organizations only with the Contracting Officer's advance approval. Article C-1, paragraph (a) (13) does not create any vested rights in the Contractor to perform fundamental research at JPL. NASA may unilaterally rescind authorization for the Contractor to engage in fundamental research at JPL, at any time.

(b) Work for Non-NASA Sponsors. The Contractor may perform work for non-NASA sponsors, which falls within paragraphs (a)(1) through (a)(6) above, or which makes use of its special competencies. This work will be designated in task orders issued by the NASA Contracting Officers based on task plans initiated by the Contractor pursuant to Article G-5.

(1) Each new or amended task order will include a reference to one or more appropriate subparagraphs of (a) above or the special competency of the Contractor being utilized to perform the effort.

(2) The Contractor shall not seek to compete for or perform work for non-NASA sponsors unless the non-NASA sponsor is willing to accept proposals from FFRDC's.

(3) In no event will JPL compete with any non-FFRDC entity in response to a Federal Agency request for proposal for other than the operation of an FFRDC nor shall JPL submit unsolicited proposals for work which is otherwise available from the private sector or which would place JPL in direct competition with domestic private industry.

(4) NASA may enter into a Space Act Agreement with a non-NASA Sponsor and issue a Task Order to the Contractor to perform the work to support the Space Act Agreement. To facilitate technology transfer in support of individual Space Act Agreements, Contractor grants NASA the right to grant the non-NASA Sponsor a non-transferable,

royalty-free, non-exclusive, non-commercial, internal use license to data, software or patentable inventions developed by Contractor in performance of the NASA Task Order issued to support the Space Act Agreement. Such license should not be construed as a waiver of any rights afforded to Contractor under Contract, including rights granted under Articles G-12, H-37, H-38, FAR 52.227-11, 52.227-14, or 52.227-16. Should the non-NASA Sponsor request rights greater than those NASA may grant under this provision or should the non-NASA Sponsor require a license to use pre-existing Contractor data, software or inventions, NASA should direct the non-NASA Sponsor to the Contractor's Office of Technology Transfer.

(c) Related Facilities Work

(1) Task Order Funded Facilities Projects. The Contractor may be directed by task orders issued by the Contracting Officer and funded by special funds of the Government for such purposes and designated as Construction of Facilities (C of F) funds, to construct, restore, remove, relocate, maintain, install, or alter existing facilities provided by paragraph (b) of Article C-2 (Resources for Performance of the Contract), below. The Contractor is authorized with Contracting Officer approval, to construct and install, whether with Contractor's in-house staff or through subcontracts, certain other buildings, premises, and facilities for the Contractor's use in the performance of any work under this Contract. The Contractor may also obtain by subcontract or provide with its own personnel, design, architectural and engineering services for facilities to be furnished by the Government under this Contract.

(2) Related Facilities Acquisition and Management. For facilities acquisition and management work other than that authorized under subparagraph (c)(1) above, the Contractor shall, either with Contractor's in-house staff or through subcontracts, provide design, architectural and engineering services, and/or construct, acquire, restore, remove, relocate, maintain, install, or alter facilities furnished or acquired under this Contract, and may appropriately remove or dispose of, the equipment, facilities, buildings, premises, space and accommodations acquired, obtained, constructed, installed or held pursuant to paragraphs (1) or (2) of this Article C-1, paragraph (c) or pursuant to other provisions in this Contract.

(d) Safety, Health and Mission Success

NASA's policy is to protect the public, NASA workforce, high-value equipment and property and the environment from potential harm as a result of NASA activities and operations. To this end, in the performance of work at the Jet Propulsion Laboratory the Contractor is responsible for the safety and mission success of the JPL activities and operations and for compliance with Federal, State, and local safety and health requirements, regulations, and standards.

(e) Information Exchange with NMO.

In order to enable the NMO to interface more effectively with JPL program and institutional (e.g., Property, Facilities, Environmental, Energy Conservation) offices, the Director of the

NMO and the Contracting Officer shall be notified of, and invited to attend regular Program Management Reviews. In addition the Contractor shall present to the Director of the NMO and the Contracting Officer a semi-annual briefing on the status of major proposals (NASA and non-NASA) and planned new starts.

C-2 RESOURCES FOR PERFORMANCE OF THE CONTRACT

(a) The Contractor shall provide, either directly or through subcontract, the management, scientific, engineering, technical and other personnel, labor and services necessary to perform all work required under this Contract.

(b) Either directly or through acquisition by the Contractor as provided under this Contract, the Government shall provide, on a rent-free basis, all property as defined in FAR 52.245-1, Government Property (APR 2012), which is required for the performance of such work. The property which the Government will provide for the Contractor's use in the performance of the Contract work includes the Government-owned facilities, including, but not by way of limitation, the land, buildings and improvements located at 4800 Oak Grove Drive, Pasadena, California, which are generally referred to as the JPL Oak Grove Facility; the Government-owned facilities at Goldstone Deep Space Communications Complex; and Table Mountain; and all other facilities heretofore made available by the Government for use by the Contractor in the performance of this Contract (including overseas tracking and data acquisition facilities as allowed by the terms of the separate NASA international agreement(s) or contract(s) for which there is a current or anticipated use requirement under this Contract. Any resources no longer required by the Contractor will be identified to the Contracting Officer.

(c) Except as otherwise directed by the Contracting Officer or otherwise provided for under this Contract or otherwise required to be obtained by the Government, the Contractor shall procure all necessary permits or licenses required for the performance of work under this Contract. With regard to copyrighted material, the Contractor shall ensure that any copyright license required in order to perform work under this Contract shall provide that the license is freely transferable to any successor-in-interest of the Contractor, a successor Contractor to operate JPL, or the Government.

C-3 USE OF OTHER FACILITIES AND LOCATIONS

(a) The Contractor shall, to the maximum extent practicable, use the facilities provided to the Contractor under Article C-2, paragraph (b) in performing work under this Contract. The Contractor is not precluded, however, from:

(1) using other facilities or performing work at other locations when in its judgment such a course will be more practical or economical; or

(2) subcontracting work in accordance with the applicable provisions of this Contract.

(b) Prior to leasing facilities for use under this Contract, the Contractor shall obtain the Contracting Officer's approval.

(c) The Contractor shall not occupy space that is leased by a subcontractor, other than in exceptional circumstances approved by the Contracting Officer or in specific instances where a limited number of Contractor employees are authorized by the Contractor to occupy such space for the purpose of managing or monitoring the subcontracted effort of that subcontractor.

(d) Contractor shall submit to the Contracting Officer, on a quarterly basis, a report of facilities leased by the Contractor and of specific locations where Contractor employees are occupying space in subcontractor facilities pursuant to paragraph (c) above.

C-4 FACILITIES MANAGEMENT PROVISIONS

(a) Implementation of CoF Funded NASA Minor and Environmental Compliance and Restoration (ECR) Projects. General. In applying life cycle planning principles in managing facilities, the Contractor shall establish and maintain a procedure for coordinating with and in keeping the Contracting Officer informed about facility management matters, including acquisition of facilities planning process described in Article G-15 (Facilities). The following applies to the implementation of the Construction of Facilities (CoF) Minor Facility Projects designated as Minor Revitalization and Construction (MRC), and ECR Projects. Individual task orders shall be written to provide for each fiscal year's funding; with the exception of the Superfund Task Order that may include more than one (1) fiscal year's funds. ECR Projects will utilize the NASA Environmental Tracking System (NETS) for oversight and mandatory environmental reporting and metrics. (Note: Other specific submittals may be required based upon the specific language in the annual call for CoF projects (e.g., ECONPACK economic analyses).

(1) Application. Projects implemented under the authority of the Summary Brief Project Document (SBPD) shall conform to the intent and scope set forth in the Facility Project Brief Project Document (NASA Form 1509) as approved by the Director, Facilities Engineering Division or designee. ECR projects implemented under the authority of the ECR-SBPD shall conform with the intent and scope set forth in the project approval document, as approved by the Director, Environmental Management Division and placed on the task order by the Contracting Officer.

(2) Resources. The amount shown as the "Approved Program Plan" on the SBPD or ECR-SBPD indicates the total resources available for projects by related NASA Purchase Request (PR). At no time may fiscal obligations exceed this amount.

(3) Project Implementation. The Contractor may implement projects in any order after execution of a task order. The Approved Facility Project Cost Estimate as stated on the SBPD or ECR-SBPD may be increased by up to, but not to exceed, 25 percent for MCR Projects and 10 percent for Environmental Projects provided.

(i) Each of these increases in project cost estimates will be submitted by the Contractor for approval by the NASA Contracting Officer.

(ii) The total of the estimates of all work awarded and any to be awarded to complete an action under consideration does not exceed the amount of the "Approved Program Plan".

(iii) The Facility Project Cost Estimate of any individual Minor Revitalization and Construction Project does not exceed $10,000,000.

(iv) The intent and scope of the project remain as indicated on the approved NASA Form 1509.

(4) Project Changes Requiring Headquarters Approval. Any changes in intent or scope, or requiring an increase above the Approved Facility Project Cost Estimate and the introduction of a new, additional, or substitute project will require advance concurrence.

(i) For MCR Projects with a cost estimate increase of more than 25 percent, advance concurrence is required by the cognizant NASA Mission Directorate and approval by the Director, Facilities Engineering Division, by means of appropriate revised NASA Form 1509 or documents applicable.

(ii) For ECR Projects with a cost estimate increase of 10 percent, advance concurrence is required by the cognizant NASA Mission Directorate and approval by the Director, Environment Management Division by means of appropriate revised NASA Form 1509 or documents applicable.

(5) Reporting. As each project is implemented, commitments, obligations, schedule for completion etc., are to be reported against its assigned Project Number in a format similar to that contained in the Quarterly Report described in to NPR 8820.2F, Facility Project Requirements, dated January 28, 2008.

(6) Bid Notifications. The Contractor will provide NASA notification of bids received utilizing NASA Form 1579, Flash Bid Report, for those projects having been approved by NASA Headquarters. Said notice shall be made via facsimile or email within one working day of bid verification. Notification of bids received is required per NPR 8820.2F, Facility Project Requirements, dated January 28, 2008.

(7) The Contractor shall submit functional area performance metrics for CoF, Facilities Maintenance, Real Property, Space Utilization, and Environment to FED and the Environmental Management Division at Headquarters as requested each year.

The Contractor shall use the criteria, procedures and reporting requirements for "on-going" Construction of Facilities (CoF) projects as set forth in NPR 8820.2F, Facility Project Requirements, dated January 28, 2008.

(b) NASA Issuances Applicable to Facilities Work. The provisions of the NASA Issuances listed below shall be used for all work performed under Article C-1, paragraph (c). The issuances referenced in this paragraph apply to both Government-owned facilities and facilities leased by the Contractor. Deviations, variations, and exceptions to the documents

below can be accommodated and must be approved by the Director, Facilities Engineering Division, NASA Headquarters, through the Contracting Officer.

(1) NPD 8800.14D, Policy for Real Estate Management dated July 15, 2004, revalidated, October 14, 2009,

(2) NPR 8800.15B, Real Estate Management Program, dated June 21, 2010

(3) NPD 8810.2A, Master Planning for Real Property, dated December 9, 2009

(4) NPR 8810.1, Master Planning Procedural Requirements, dated April 28, 2005

(5) NPD 8820.2C, Design and Construction of Facilities, dated June 13, 2006

(6) NPR 8820.2F, Facility Project Requirements, dated January 28, 2008 is incorporated into the Contract with the following clarifications:

(a) 1.1.1 Discrete Projects are projects with an estimated construction cost of $10 million or more.

(b) 1.1.2 Minor Revitalization and Construction Projects (MRCs) are projects with an estimated construction cost of at least $1,000,000 and up to $10 million.

(c) 1.3.16.2. Each facility project estimated to cost $50,000 or more must have an approved NASA Form 1509, Facility Project-Brief Project Document, and NASA Form 1510, Facility Project Cost Estimate is required for each facility project estimated to cost $75,000 or more.

(7) NPD 8831.1E, Maintenance and Operations of Institutional and Program Facilities and Related Equipment, dated June 19, 2003, revalidated June 16, 2008

(8) NPR 8831.2E, Facilities Maintenance and Operations Management, dated November 18, 2008 is incorporated into the Contract with the following clarifications:

(a) 2.3.3 Funding Thresholds. Table 2-2, Facilities Maintenance Funding Thresholds, Note 2: (CoF) Program category (currently exceeding $1,000,000) must have Congressional approval.

(b) Appendix A, item A-70, Major Facility Work. Construction and revitalization work in excess of $10.0 million and Land Acquisition and emergency Repair approved under the provisions of Section 308(b) of the National Aeronautics and Space Act of 1958, as amended, at any cost.

(c) Task Orders shall reference the approved NASA Form 1509 or other applicable approved NASA Form (e.g., 799PD, 799EUL, etc.), to be observed by the Contractor in connection with the work to be performed under the task orders pursuant to Article C-1, paragraph (c) herein.

(d) This clause is intended to satisfy with the requirements of 1852.245-82, Occupancy Management Requirements (JAN 2011), and 1852.245-83, Real Property Management Requirements (JAN 2011).

C-5 EXCESS AND SURPLUS EQUIPMENT

The Contractor shall, except as otherwise provided for by the Contracting Officer or designee, use the Department of Defense Plant Clearance Automated Reutilization Screening System (PCARSS) for submitting inventory schedules of excess property both onsite and at subcontractor and alternate locations to the NASA NMO Plant Clearance Officer.

C-6 SPECIFIC AGREEMENT ON ORGANIZATIONAL AUTHORITY

(a) The following organizational responsibilities have been specifically agreed to by the parties:

(1) The Contractor's contracts administration function will be under the direction of its Vice President for Business and Finance, and no other Caltech organization unless agreed to pursuant to (c) of this Article.

(2) The JPL Director has full authority, without dollar limitation, to enter into contractual agreements on the behalf of the Contractor, including base operations and other competitive sourcing activities. The JPL Director also has full authority on behalf of Contractor for the acceptance and implementation by JPL of NASA and federal policies (e.g., NPDs and NPRs), release of data to NASA and outside organizations, and all technical and contractual issues associated with the issuance and administration of task orders under the Contract.

(b) The Parties acknowledge that the Contract for operation of JPL is between NASA and Caltech. The JPL Director is the Contractor's authorized representative for Contract implementation.

(c) Any changes to the organizational responsibilities set forth in this clause requires the mutual agreement of the parties.

C-7 AUTHORIZED WORK

(a) Authorized Core Competency Work. All work shall be within the scope of the core competences specified in Clause C-1, Description of Work, or efforts required to support those core competencies. This condition applies to both direct efforts and work that would be categorized as an allocated direct cost.

(b) Unauthorized Work.

(1) The Contractor shall promptly notify the Contracting Officer for clarification and guidance whenever a Contractor's employee in a supervisory position is informed that a NASA employee has requested JPL perform or the Contractor's employee has initiated work that the Contractor believes may be construed as outside the scope of the Contractor's core competencies. If the Contractor thereafter proceeds to perform work

without the Contracting Officer's authorization, then costs incurred for such work could be deemed unallowable by the Contracting Officer.

(2) The Contractor shall not knowingly propose, and the Government shall not knowingly request, any work that constitutes an inherently governmental function. Examples of typical inherently governmental functions can be found in Appendix A of the Office of Federal Procurement Policy (OFPP) Policy Letter 11-01, *Performance of Inherently Governmental and Critical Functions*, and FAR Subpart 7.5–Inherently Governmental Functions, Subsection 7.503(c). The listings are illustrative examples and are not all inclusive.

(c) Hosting Conferences and Meetings.

The Contractor, in carrying out its responsibilities under this Contract, may propose or be asked to host, organize, sponsor, or otherwise manage conferences, Agency or Government wide meetings, or other similar events. A conference is defined as a meeting, retreat, seminar, symposium or event that involves attendee travel. Indicia of a formal conference include (1) participants from multiple agencies or organizations, (2) discussions involving topical matters of interest to the participants, (3) scheduled speakers or discussion panels, (4) published substantive agenda, and (5) registration.

(1) Types of meetings or events that are not considered conferences:

a) Formal operational meeting: A meeting necessary to perform managerial or operational activities, as part of day-to-day operations. An operational meeting is required for program and project oversight, planning, review and approval. Examples of these include meetings of the oversight bodies and reviews as found in NASA's project management NPRs set forth in this Contract.

b) Other operational meeting: These are meetings other than formal operational meetings, held in furtherance of missions and operations, including meetings necessary for routine business. Included are activities such as project planning and prioritization, project development work or operations, property management reviews, audits, investigations, and inspections.

(2) The Contractor shall seek Contracting Officer approval prior to agreeing to host, organize, sponsor, co-sponsor, or otherwise manage conferences, or other similar events at the behest of NASA or another Government Agency.

(3) The Contractor shall notify the Contracting Officer as soon as practicable of conferences to be hosted, organized, sponsored, co-sponsored, or otherwise managed by JPL at its own behest in performance of the contract.

(d) Training. The Contractor will provide training to its workforce regarding both the scope of the Contract and inherently governmental functions.

[END OF SECTION]

SECTION D—PACKAGING AND MARKING

D-1 PACKAGING AND MARKING

Packing, packaging and marking requirements, if applicable, are included in task orders under this Contract.

[END OF SECTION]

SECTION E—INSPECTION AND ACCEPTANCE

E-1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

The following Contract clauses pertinent to this section are hereby incorporated by reference:

FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.246-9	Apr 1984	INSPECTION OF R&D (SHORT FORM)
52.246-11	Feb 1999	HIGHER-LEVEL CONTRACT QUALITY REQUIREMENTS

(a) The Contractor shall comply with the higher-level quality standard selected below.

Title	Number	Date	Tailoring
ISO	9001	2008	None

(b) The Contractor shall comply with the higher-level quality standard selected below by the end of calendar year 2014, in lieu of the quality standard described in paragraph (a).

Title	Number	Date	Tailoring
AS	9100C	2009	None

(c) The Contractor shall provide a detailed AS9100C transition plan, identifying implementation milestones and priorities, to the Contracting Officer no later than 90 days after the effective date of the Contract.

[END OF SECTION]

SECTION F—DELIVERIES OR PERFORMANCE

F-1 TERM OF THIS CONTRACT

The period of performance is from October 1, 2012, through September 30, 2017. The Contractor shall not perform work beyond the terminal date of this Contract, irrespective of the fact that the anticipated completion date of a task order may extend beyond such terminal date.

F-2 DELIVERIES

Delivery instructions shall be specified in each task order, as appropriate. Government Bills of Lading (GBL) may be used as requested by the Contractor and approved by the NASA Transportation Officer. All GBLs used for the purpose of satisfying the requirements of the International Traffic in Arms Regulations, 22 CFR 126.4, must be reviewed and approved by the Export Administrator in the NASA Management Office at JPL or the NASA Export Administrator in the Office of International and Interagency Relations at NASA Headquarters if needed.

F-3 STOP-WORK ORDER (FAR 52.242-15) (AUG 1989) (ALT I) (APR 1984) (DEVIATION)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this Contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either—

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Termination clause of this Contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule, the estimated cost, the fee, or a combination thereof, and in any other terms of the Contract that may be affected, and the Contract shall be modified, in writing, accordingly, if —

(1) The stop-work order results in an increase in the time required for, or in the Contractor’s cost properly allocable to, the performance of any part of this Contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided that, if the Contracting Officer decides the facts

justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this Contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

F-4 BILLS OF LADING (NFS 1852.247-73) (JUN 2002) (DEVIATION)

The purpose of this clause is to define when a commercial bill of lading or a government bill of lading is to be used when shipments of deliverable items under this Contract are f.o.b. destination.

(a) Commercial Bills of Lading. All domestic and domestic overseas shipments shall be made via commercial bills of lading (CBLs). As used in this clause, "domestic overseas" means non-continental United States (i.e., Hawaii, Commonwealth of Puerto Rico, and possessions of the United States). The Contractor shall prepay domestic transportation charges. The Government shall reimburse the Contractor for these charges if they are added to the invoice as a separate line item supported by the paid freight receipts. If paid receipts in support of the invoice are not obtainable, a statement as described below must be completed, signed by an authorized company representative, and attached to the invoice.

"I certify that the shipments identified below have been made, transportation charges have been paid by (company name), and paid freight or comparable receipts are not obtainable.

Contract or Order Number: [contract number]

Destination: TBD."

(b) Government Bills of Lading.

(1) International (export) overseas shipments of items deliverable under this contract shall be made by Government Bills of Lading (GBLs) only when ITAR exemption 126.4 is authorized for use by NASA. All international shipments of items deliverable under this contract that are not covered under ITAR exemption 126.4 shall be made by Commercial Bill of Lading.

(2) At least 15 days before shipment, the Contractor shall request in writing GBLs from: [Insert name, title, and mailing address of designated NASA transportation officer or other NASA official delegated responsibility for GBLs]. If time is limited, requests may be by telephone: [Insert appropriate telephone number]. In all instances, the use of ITAR exemption 126.4, is limited to "temporary" exports; i.e., exports of hardware that will, in general, be out of the U.S. for a maximum of four years, unless otherwise authorized by NASA. Requests for GBLs shall include the following information.

(i) Item identification/description.

(ii) Origin and destination.

(iii) Individual and total weights.

(iv) Dimensional Weight.

(v) Dimensions and total cubic footage.

(vi) Total number of pieces.

(vii) Total dollar value.

(viii) Other pertinent data, such as: name, date and number (if applicable) of the NASA international agreement or Caltech subcontract that requires the export, evidence that a NASA Export Administrator has authorized the use of the 126.4 exemption, destination control statement and/or shipment markings as required by the ITAR and/or the NASA international agreement.

F-5 GENERAL REPORTS AND PLANS

The Contractor shall furnish NASA such managerial, financial, technical, progress, and other reports as appropriate for the activities or class of mission carried out under this Contract.

(1) Scientific and Technical Reports. See Article H-31, Protection of Scientific and Technical Information of National Interest.

(2) Public Reports. Reports prepared primarily for members of the public generally, such as general educational and public information reports, shall be subject to the provisions of Article H-11, External Communications and Visitor Requests From Known Elected Officials and Those Known to Be Seeking Elected Office.

(3) Distribution Control. The Contracting Officer may require the Contractor to cease the external distribution under this Contract, of any reports within a regular or report series, or of any individual report, and any work in connection with such external distribution. However, in such event the Contractor shall remain free to publish, at the Contractor's own expense, any information or data contained in such report(s), subject to any limitations contained within this Contract, in bilaterally accepted task orders, or in the laws or regulations of the United States.

The term "external distribution", as used in this paragraph, means any distribution except distribution to the Contractor's own personnel, to present and prospective subcontractors of the Contractor, and to NASA personnel. The term "distributed externally" has a like meaning.

(4) NASA Publications. NASA may elect to publish in its own media and formats any of the information contained in reports prepared by the Contractor. When in the judgment of the program Associate Administrator or organizational Chief (e.g., Chief Technologist, Chief Engineer), or designee, information in any such reports should also be published in NASA media and format, the Contractor will make such revisions as are requested, to conform the reports to NASA requirements. Copies of all reports within paragraph (2) above, prepared

by the Contractor, shall be forwarded to the program Associate Administrator or organizational Chief (e.g., Chief Technologist, Chief Engineer), as soon as possible after preparation

(5) Contractor Distribution. Nothing herein shall be deemed to restrict the right of the Contractor to initiate, prepare and distribute to its own personnel, its present or potential subcontractors, and to NASA personnel such reports as it may deem necessary or desirable for the performance of work under this Contract, subject to Federal laws and regulations, including U.S. export laws and regulations.

(6) Overrun Reports. The Contractor shall submit electronically the status of task orders where expenditures exceed funds allotted by greater than $1,000 and the Contractor's plan of action on each such task order.

(7) Workforce Reports. The Contractor shall, by the 90th day after expiration of the yearly Affirmative Action Plan (AAP), provide to NASA Headquarters Office of Education, a copy of the new Affirmative Action Plan, prepared in accordance with the requirements of 41 CFR 60-2, Subpart B, including a copy of the Organizational Profile (41 CFR 60-2.11), and the section containing a review of the results of actions taken during the previous Affirmative Action Plan year.

(8) Caltech Transfers. The Contractor shall submit a quarterly report to the Contracting Officer describing the tasks being performed at JPL under Caltech Transfers, in a format to be approved by the Contracting Officer.

(9) New Technology Reporting. The requirements of the New Technology Reporting Clause of this Contract are further defined as follows:

(i) All New Technology Reports, inventions, disclosures, patent applications, requests for waivers, and intellectual property licenses year-end data shall be entered no later than 30 days following the end of the Fiscal Year.

(ii) NASA Technology Tracking System or (NTTS).

(A) The Contractor shall enter all available data on a monthly basis to the Technology Tracking System database (not later than the fifteenth of the month for which the data pertains) in support of Federal Agency reporting requirements under section 11 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended (15 U.S.C. 3710). These data shall include, but are not limited to, information regarding: subject inventions including software (FAR clause 52.227-11 as modified by NASA FAR Supplement clause 1852.227-11); decision on election of title to subject inventions; patent applications filed on subject inventions, patents issued on subject inventions, copyrights asserted on subject inventions (software); copyright and patent licenses executed and royalties received for subject inventions; subcontracts issued under this Contract; partnerships established; private entity contributions to each partnership (e.g., funds applied and/or dollar value of personnel, facilities or equipment, etc.); and success stories identified during the period.

(B) The Contractor shall ensure that data associated with each reportable item (e.g., NASA tracking number, innovator names, subject title, subsequent patent filing, and licensing information, subsequent copyright licensing information) is timely entered into the NASA Technology Tracking System database. The Contracting Officer may provide the Contractor additional guidance from time to time as necessary.

(C) Technology Transfer Policy Guidance: Will detail what activities the Contractor can engage in to encourage the transfer of technology to the private sector, and what resources the Contractor may apply to those activities

(D) Tech Transfer Annual Report: Summary of metrics derived from the data entered into the NTTS system.

(10) Safety, Health, and Mission Assurance Reports.

In accordance with Attachment E, the following will be submitted:

(i) Submit a safety and health plan per Article H-7(2) no later than 90 days prior to the effective date of the Contract that will be approved or disapproved by the Contracting Officer. The Contractor shall maintain updates to this plan and shall provide these updates. At the Contractor's discretion, the safety and health plan may incorporate elements of other required safety and mission assurance discipline plans.

(ii) Provide a list of the types of hazardous operations being performed under this Contract within 90 days after Contract award. The Contractor shall maintain updates to this list and shall provide, no less than semi-annually. Detailed documentation Operational Safety Reviews (OSRs) of potential hazardous operations shall be retained on file at JPL and shall be made available upon Contracting Officer request. The parties agree that the reporting requirements of paragraphs (i) and (ii) satisfy the Contractor's obligations under paragraph (j) of NFS 1852.223-70, Safety and Health.

(iii) The Contractor shall submit the Contractor's Safety and Mission Assurance (SMA) Technical Authority Implementation Plan per Article H-7 within 60 days after Contract award for approval by the Contracting Officer.

(iv) The contractor shall develop annually and submit a Safety and Mission Assurance Annual Operating Agreement that documents the agreement between the Contractor's Safety and Mission Assurance authority and the Director of JPL of the activities, processes, resources, and metrics to be applied for safety and mission assurance for the fiscal year. (Note as defined in this context safety and mission assurance includes all of the functions/activities under the purview of the NASA Chief, Safety and Mission Assurance regardless of how the contractor has organizational distributed these functions.) The Annual Operating Agreement shall be submitted no later than 31 October of each year and shall include:

(A) A summary of the results obtained for the previous fiscal year including an accounting of accomplishments versus the metrics established for the previous year.

(B) A summary of the mission, functions, and process descriptions for the safety and mission assurance activities performed under the contract.

(C) Metrics and planned goals for the year of submittal at a functional level, including at a minimum mishap data.

(D) Description of initiatives (either internal or externally directed) planned for the reporting period.

(E) Identification of the resources to be applied to the activities and processes for the reporting period.

(F) Identification of resource threats and associated risks for the reporting period.

(G) Assumptions used in the preparation of the agreement.

(H) Status of open corrective action plans from all safety and mission assurance sources, including, Mishap Investigations, audits, surveys, and reviews.

(I) Description of the process for obtaining customer feedback and a summary of the results of that feedback.

(J) Responses to endorsements provided on previous year agreements.

[END OF SECTION]

SECTION G—CONTRACT ADMINISTRATION DATA

G-1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

The following Contract clauses pertinent to this section are hereby incorporated by reference:

I. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.223-71	DEC 1988	FREQUENCY AUTHORIZATION
1852.227-11	MAY 2002	PATENT RIGHTS RETENTION BY THE CONTRACTOR (SHORT FORM)
1852.242-70	SEP 1993	TECHNICAL DIRECTION
1852.242-73	NOV 2004	NASA CONTRACTOR FINANCIAL MANAGEMENT REPORTING
1852.245-73	JAN 2011	FINANCIAL REPORTING OF NASA PROPERTY IN THE CUSTODY OF CONTRACTORS
1852.245-74	JAN 2011	IDENTIFICATION AND MARKING OF GOVERNMENT EQUIPMENT (JAN 2011)
1852.245-75	JAN 2011	PROPERTY MANAGEMENT CHANGES
1852.245-82	JAN 2011	OCCUPANCY MANAGEMENT REQUIREMENTS
1852.245-83	JAN 2011	REAL PROPERTY MANAGEMENT REQUIREMENTS

G-2 COST SEGREGATION AND REPORTING

(a) General. Costs under this Contract will be segregated and reported as set forth below. The Contractor shall transmit such reports electronically or by hard copy, as requested by the Government.

(1) Research and Development Work. The Contractor shall segregate, account, summarize, and report the accrued costs for each program Work Breakdown Structure (WBS) in accordance with NASA Procedural Requirements (NPR) 9501.2E, NASA Contractor Financial Management Reporting, as incorporated into this Contract pursuant to Article G-2, paragraph (a)(7), by each task order for all work performed pursuant to Article C-1 paragraphs (a) and (b) herein. The Contractor shall not transfer costs between task orders except:

(i) in those limited instances where the costs are found to have been originally charged to an incorrect JPL Project/Task Number due to a mistake or error, provided that sufficient documentation is maintained by the Contractor to demonstrate that the transfer was indeed required to correct a mistake or error, or

(ii) with prior written approval or at the written request of the Contracting Officer, or

(iii) to allow for the cost transfer of unused materials within the period of performance of the originating Task Order.

(2) Related Facilities Management/Maintenance. The Contractor shall segregate, account, summarize, and report the accrued costs for each task order and each program Work Breakdown Structure (WBS) in accordance with NASA Procedural Requirements (NPR) 9250.1B, Property, Plant and Equipment and Operating Materials and Supplies, as incorporated into this Contract pursuant to Article G-2, paragraph (a)(8) for all work performed pursuant to Article C-1, paragraph (c)(1) herein. Facilities maintenance costs shall be reported as requested by the Contracting Officer to assist NASA in complying with its CFO Act responsibilities.

(3) Closed Appropriations. Pursuant to the National Defense Authorization Act for Fiscal Year 1991, 104 Stat. 1485, P.L. 101-510, Nov. 5, 1990, all expired appropriation accounts at NASA Headquarters will be closed on September 30th of the fifth (5th) fiscal year after the end of the period of availability for obligation. The Contractor shall track closed appropriation accounts in the Contractor's accounting system in order to support the aforementioned closeout process.

(4) Uncosted Obligations. A phased costing plan will be provided for direct funded task orders at such times and in such formats as directed by NASA.

(5) Identification of Excess Funds on Inactive Task Orders. This report will identify excess funds greater than $1,000 on inactive task orders whose period of performance end dates are beyond 120 days past. It is due 30 days after the close of the previous quarter.

(6) NASA Contractor Financial Management Report. In complying with the reporting requirements of NFS 1852.242-73, the Contractor will submit NASA Contractor Financial Management Reports as follows:

(i) Monthly NF533 Reports will be submitted ten (10) work days after the end of the Contractor's fiscal month (the initial report will be submitted ten (10) work days following the end of the Contractor's fiscal month after the initial incurrence of cost). Each report will be comprised of a one page summary report at the total (prime) Contract level by major cost category (i.e., direct labor, travel, services, procurements, Caltech Interdivisional Authorizations, benefits and applied burden). The Contractor will also provide NF533M data for each task order on a task order basis.

(ii) Quarterly NF533 Reports will be submitted 15 calendar days prior to the beginning of the Contractor's fiscal quarter being reported (the initial report will

be submitted within 30 work days after award of the Contract). Each report will be comprised of a one page summary report at the total (prime) Contract level by major cost category (i.e., direct labor, travel, services, procurements, Caltech Interdivisional Authorizations, and benefits and applied burden), and NF533Q data for each task order on a task order basis.

(iii) The NF533 reports will not include narrative reporting, fee reporting at the task order level, or potential termination liability. Fee reporting may be required by the government when an incentive fee is applicable to a task order.

(iv) The NF533M will be submitted for three months after the period of performance of this Contract is completed. A significant amount of time may pass between the end of the Contract and final closeout. If no significant additional costs are being incurred or anticipated after the first quarter following the end of the Contract, the Contracting Officer may reduce or suspend NF533 reporting requirements. If the final cost of the Contract changes after the submission of the "final" report, the Contractor must submit a revised NF533 in the month the change is recognized.

(v) The NF533 will be submitted electronically. The electronic format will include cost and workforce data in a manner consistent with the current formats.

(vi) The NF533 reports are the official cost and workforce document for actual and estimated cost performance. Any financial data submitted to NASA in addition to the NF533 must be based upon data from the Contractor's financial system and reconcilable to that financial system as requested by the Contracting Officer.

(vii) The Contractor shall use the WBS breakout on the task orders as the lower level detail for the purposes for NFS 1852.242-73.

(viii) The requirement in NFS 1852.242-73 regarding subcontractor cost data is deemed to have been met by the Contractor accurately reflecting subcontractor NF533M and other cost data in the proper reporting categories on the Contractor's Form NF533 report.

(7) Financial Reporting. NPR 9501.2E, NASA Contractor Financial Management Reporting, dated May 27, 2011, is incorporated into this Contract with the following understandings:

(i) Regarding Sections 2.5.11 and 2.5.12, in lieu of the unique NASA WBS requirement, the Contractor will provide a monthly Capital Asset Report (CAR) which covers items that meet the definition of capital assets under NPR 9250.1B.

(ii) To satisfy the requirements of Section 3.6, Narrative Remarks, the Contractor shall provide narrative reporting following the submittal of NF 533 reports to the extent and in such formats as requested by NASA as part of its Continuous Monitoring Program.

(8) Property, Plant, and Equipment and Operating Materials and Supplies. NPR 9250.1B, Property, Plant, and Equipment and Operating Materials and Supplies, dated January 6, 2011, is incorporated into this Contract with the following understandings:

(i) NASA Form 1739, Alternative Future Use Questionnaire (AFUQ), is replaced by the similarly titled JPL Form 7121 wherever NASA Form 1739 is mentioned.

(ii) The existing language in the indicated NPR sections is deleted and replaced as follows:

P.2. (second paragraph) The Alternative Future Use Questionnaire (AFUQ), JPL Form 7121, is applicable to this Contract. Assets identified as capital on this form will be captured on the monthly Capital Asset Report (CAR).

1.3.6.1 Assets identified as capital on the AFUQ, JPL Form 7121, will be captured on the monthly Capital Asset Report (CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

1.3.6.2 Joint costs that are commonly used to support the production of multiple capital assets within a single project that cannot be directly traced to each final asset shall be directly traced to the Capital Asset Report (CAR). Joint or common project costs, as well as other costs that cannot be directly traced to the project or capital asset in an economically feasible manner, will be allocated to the final asset(s) based on a reasonably supportable allocation methodology. For example, inspection or survey costs that cannot be traced to a specific end item may be allocated to the final asset based on percentage of total inspections or surveys, square footage, or project size.

1.3.6.3 Reserved

1.4.2.1 Planning. Identifying planned acquisitions, fabrications, or modifications of NASA-owned PP&E shall be evaluated through the completion of the AFUQ, JPL Form 7121, by the JPL project manager. Those PP&E items that meet established capitalization criteria will be captured on the monthly Capital Asset Report (CAR).

1.4.2.1.1 Reserved

1.4.2.2.1 Costs incurred by the Contractor for an asset meeting the capitalization criteria shall be captured on the monthly Capital Asset Report (CAR).

1.4.2.2.2 Identified capital costs shall be accumulated as an Asset Under Construction (AUC) and recorded as WIP. For Construction of Facilities type work, those costs can be traced to a unique NASA WBS, within a Task Order, on the NF533 report. WIP (PP&E under construction), including Construction of Facilities type work, shall be reported in the monthly CHATS and annual NF1018 report.

1.6.1.c. Assets identified as capital on the AFUQ, JPL Form 7121, will be captured on the monthly Capital Asset Report (CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

1.6.1.d. Reserved

1.6.1.e. Create Purchase Requisitions (PRs) to fund the acquisition, fabrication, or modification of identified PP&E meeting the capitalization criteria ensuring that the PRs are funded by the unique WBS element for Construction of Facilities type work.

1.6.2.a. Reserved

1.6.3.d. Work with project managers, procurement officers, resource managers, real property officers, and logistics personnel to review project work that will procure, fabricate, construct, or improve capital assets to ensure all General PP&E is properly identified so that the assets can be accurately valued and reported.

1.6.3.e. Assets identified as capital on AFUQ, JPL Form 7121, will be captured on the monthly Capital Asset Report (CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

1.6.3.h. Reserved

1.6.3.k. Review subcontractor requests to purchase PP&E in order to ensure separate reporting of individual PP&E has been established.

1.6.4.a.(2) Reserved

1.6.4.b.(2) Assets identified as capital on the AFUQ, JPL Form 7121, will be captured on the monthly Capital Asset Report (CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

2.2.5.3.b. Facility modifications identified as capital on the AFUQ, JPL Form 7121, will be captured on the monthly Capital Asset Report (CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

2.3.7.2 WIP (Assets Under Construction) shall be reported in the monthly CHATS and annual NF1018 report. For Construction of Facilities type work, those costs can be traced to a unique NASA WBS, within a Task Order, on the NF533 report and shall be reported in the monthly CHATS and annual NF1018 report.

3.4.1.1 Costs of Construction of Facilities type work can be traced to a unique NASA WBS, within a Task Order, on the NF533 report.

4.4.3 Costs of personal property acquisitions and capital improvements meeting the capitalization criteria will be captured on the monthly Capital Asset Report

(CAR), which covers items that meet the definition of capital assets under NPR 9250.1B.

4.5.1.1 WIP (PP&E under construction) shall be reported in the monthly CHATS and annual NF1018 report.

(9) Capital Asset Identification and Treatment. NPD 9250.1A, Capital Asset Identification and Treatment, dated October 8, 2010, is incorporated into this Contract with the following understandings:

(i) NASA Form 1739, Alternative Future Use Questionnaire (AFUQ), is replaced by the similarly titled JPL Form 7121 wherever NASA Form 1739 is mentioned.

(ii) Regarding Sections 1.a, 5.d and A.4, in lieu of the unique NASA WBS requirement, the Contractor will provide a monthly Capital Asset Report (CAR) which covers items that meet the definition of capital assets under NPR 9250.1B.

(iii) Regarding Section 5.b, the capitalization determination is delegated to the Contractor and becomes final upon review and approval of NASA Financial Office personnel.

G-3 PROPERTY REPORTING

The Contractor will furnish a current itemized listing of all NASA-owned property accountable under this Contract, including subcontractors and a separate current listing of NASA property in the possession of Instituto Nacional de Tecnica Aeroespacial (INTA) and the Commonwealth Scientific and Industrial Research Organization (CSIRO), annually, no later than October 30, in the format requested by the NMO Industrial Property Officer. This listing should include NASA-owned Construction in Progress at the project level, Contract Work in Progress at the project level and software as required by NFS 1845.7101-1.

G-4 LIST OF GOVERNMENT PROPERTY FURNISHED PURSUANT TO FAR 52.245–1 (NFS 1852.245-76) (JAN 2011) (DEVIATION) (MOD 6)

(a) For performance of work under this Contract, the Government will make available Government property in accordance with Article C-2, Resources for Performance of the Contract, of this Contract on a no-charge-for-use basis. The Contractor shall use this property in the performance of this Contract at the locations stated in Article C-2, paragraph (b) of this Contract, at the Contractor's campus facilities for on-campus research in accordance with paragraph (d) of FAR 52.245-1 and at other location(s) as may be approved by the Contracting Officer. Under the FAR 52.245-1 Government property clause of this Contract, the Contractor is accountable for the identified property.

(b) The Contractor is responsible and accountable for all Government personal property as identified in Article C-2, paragraph (b) in the Contract in accordance with FAR 52.245-1. For purposes of the tracking and data acquisition facilities located in Spain, Australia, and Goldstone, CA, the Contractor's property management system, in accordance with FAR 52.245-1, shall consist of the following actions: maintenance of all required records,

and annual on-site reviews of property, as directed by the Contracting Officer, but no more than annually. A listing of the property is required as requested per Article G-3 (Property Reporting).

(c) The Contractor is authorized to use Government-owned equipment, furnished or acquired for use in the performance of this Contract, in its on-campus research programs on a non-interference, no charge loan basis, under written procedures, including property and reporting procedures, that must be approved by the Contracting Officer. However, Government property that has no use under this Contract will not be retained solely for the Contractor's use, and will be dispositioned in accordance with the property terms of this Contract.

G-5 TASK ORDERING PROCEDURE (NFS 1852.216-80) (OCT 1996) (DEVIATION)

(a) General. Only the Contracting Officer may issue task orders to the Contractor, providing specific authorization or direction to perform work within the scope of the Contract. A task order shall be effective as provided therein. The Contractor shall proceed with performance of such task orders in accordance with their terms and the terms and conditions of this Contract.

(b) Statements of Work.

(1) NASA Sponsors. Statements of Work for task orders shall be in accordance with NASA requirements as denoted by approval letters or other documentation signed by NASA program personnel and directed to the Contracting Officer.

(2) Non-NASA Sponsors.

(i) Statements of Work with Non-NASA sponsors shall be in accordance with the Contractor's proposal as accepted by the non-NASA sponsor and the NASA Contracting Officer. The Contractor may procure computer hardware and software for a non-NASA sponsor for prototype units, software development and classified purposes only. All non-NASA sponsored work for or involving foreign entities must be reviewed through the NASA Export Administrator in the NASA Management Office at JPL or the NASA Export Administrator in the Office of International and Interagency Relations, if needed, prior to the approval by the NMO Contracting Officer.

(ii) Federal Acquisition Regulation (FAR) Part 35.017-1(c)(4) prohibits Federally Funded Research and Development Centers from competing with non-FFRDC entities in response to a Federal agency request for proposals. There are limited circumstances where the Contractor's support may be provided to non-FFRDC organizations responding to such requests for proposals. The Contracting Officer will provide a determination of the appropriateness of the Contractor's participation after pre-coordination activities with the Contractor and the non-NASA sponsor.

(c) Special Procedures for Tasks Designated by NASA. Task orders shall be in writing, be numbered in a succession of numbers; be dated; shall describe the work to be performed or

the services or supplies to be furnished; shall state both the estimated cost under this Contract, the amount allotted for performance thereunder, and the period of performance; shall set forth the appropriation and allotment chargeable and any other pertinent fiscal or administrative data; shall include delivery instructions if required and describe the applicability of the clauses from Article H-29 (Clauses Applicable on a Task Order Basis); may include performance standards and other requirements as appropriate; and shall be signed by the Contracting Officer.

(d) Special Procedures for Critical Flight Project Tasks.

In addition to other requirements set forth in this clause, NASA may determine that additional technical, cost, and schedule information be provided for task plans associated with critical flight projects, as designated by the cognizant NASA Office. The additional information will facilitate a tailored comprehensive review by NASA commensurate with procedures for evaluation of proposals received under Announcement of Opportunity requirements.

(e) Performance Incentives. NASA reserves the right to require performance incentives be incorporated for work performed under this Contract in accordance with Article B-3 (Cost and Performance Incentives for Tasks). Although performance incentives are primarily designed for critical flight projects, all NASA projects including, non-NASA sponsored projects may utilize the performance incentive option.

(f) Procedure. A task order may be issued by the Contracting Officer upon submission of a task plan pursuant to either (1) or (2) below.

(1) When the Contractor provides the Contracting Officer with a task plan in accordance with the agreed to task plan template and/or applicable sponsor guidelines.

(2) When NASA desires to issue a task order pursuant to Article C-1 (Description of Work) paragraphs (a),(b) and (c) and the Contractor has not yet provided a task plan pursuant to subparagraph (f)(1) above, the Contracting Officer shall provide the Contractor with the following data:

(i) A functional description of the work identifying the objectives or results desired from the contemplated task order.

(ii) Proposed performance standards, if any, to be used as criteria for determining whether the work requirements have been met.

(iii) A request for a task plan from the Contractor to include the technical approach, period of performance, appropriate cost information, and any other information required to determine the reasonableness of the Contractor’s task plan.

(iv) Within 60 calendar days after receipt of the Contracting Officer’s request, the Contractor shall submit a task plan conforming to the request. However, within 30 calendar days after receipt of the notice that funds have arrived for the proposed task, the Contractor shall submit a task plan conforming to the request.

(3) After review and necessary discussions, the Contracting Officer may issue a task order to the Contractor as set forth in (b) above.

(g) Acceptance. Upon receipt of a task order issued by the Contracting Officer pursuant to Article C-1 (Description of Work) paragraphs (a), (b) and (c), the Contractor shall promptly, and not later than ten days from such receipt, notify the Contracting Officer in writing, if, in its opinion, (1) the resources provided for performance of the work of the task order are inadequate; or (2) performance of the task is not technically feasible. Additionally, the Contractor shall notify the Contracting Officer of any other major problems that might, in the Contractor's opinion, threaten accomplishment of the work under the task order. Notwithstanding the foregoing, the Contractor shall proceed, to the best of its ability, with performance of the work of the task order in accordance with its terms pending a Contracting Officer's written direction within ten working days from receipt of the Contractor's initial notification.

(h) Modification Procedure. Any task order issued pursuant to Article C-1 (Description of Work) paragraphs (a), (b) and (c) may be amended by the Contracting Officer at any time. During the performance of the task order the Contractor may submit to the Contracting Officer a revision to the task plan and/or applicable sponsor guidelines for incorporation into a task order modification. Funds withdrawal from any task order shall be coordinated with the Contractor to ensure the funds decrease does not reduce the amount allotted to the task order below that amount estimated by the Contractor to be necessary to cover (i) all expenditures and other amounts accrued against the task order, (ii) all outstanding obligations and commitments against the task order to the extent they cannot be withdrawn. The Contractor will identify all funds available for withdrawal upon completion of the task order's period of performance. Subject to the provisions of Article I-12 Limitation of Cost (FAR 52.232-20); Limitation of Funds (FAR 52.232-22) (Deviation), the Contractor shall not terminate work on any task order, unless so directed by the Contracting Officer.

(i) The Contractor shall notify the Contracting Officer whenever, in its opinion, the funds made available to the Contractor by any task order are insufficient to permit continuance of the performance of work under that task order for more than fifteen (15) days after the date of the notification.

(j) In the event of a conflict between the requirements of the task order and the Contractor's approved task plan, the task order shall prevail

(End of Clause)

G-6 TRANSFERS OF FUNDS BETWEEN TASK ORDERS

(a) General. Funds may not be transferred from one task order to another task order unless specifically authorized by the Contracting Officer.

(b) When funds are transferred to any task order in accordance with paragraph (c) below, the sum allotted for the performance of work under that task order shall be deemed to be

increased in the amount so transferred. In the event the sum previously allotted for the performance of such work plus the sum so transferred exceeds the estimated cost of the performance of such work, such estimated cost shall be deemed to be increased in the amount of such excess. The sum allotted for the performance of work under any task order from which such transfer of funds is made shall be deemed to be decreased in the amount of the transfer. Additionally, the statements of work of all affected task orders shall be modified if necessary to include resultant changes in scope of work if any. Such modification shall be in conformance with this provision.

(c) Procedure. The Contractor may request funds which have previously been allotted to another task order or task orders be transferred to the task order requiring additional funds, provided prior approval has been received from the authorizing NASA Mission Directorate. The request shall state the amount which the Contractor desires to have transferred, the task order or task orders from which this amount is to be transferred, and the justification supporting the transfer request. If the Contractor's request is approved by NASA, the Contracting Officer will timely issue the appropriate task order modification to confirm the transfers of funds.

G-7 FUNDS PROCEDURE FOR TERMINATION OF TASK ORDERS

(a) In the event the Government terminates a task order and the funds allotted thereto are insufficient to cover termination costs, the Contractor shall notify the Contracting Officer of its estimate of the additional funds that it believes to be necessary to cover reasonable, allocable, and allowable task order termination costs as follows:

(1) Within 60 days of the notice of termination the Contractor shall provide an initial estimate of the total amount of such funds required, and shall also identify those funds legally available for removal from other task orders which the Contractor recommends be used to cover such estimated total termination costs; and

(2) Within 180 days of the notice of termination, the Contractor shall supplement the initial estimate by providing a funds requirement proposal, with supporting detail for each cost element, and with any further recommendations regarding a source of funds.

(b) Upon receipt of the initial estimate described in (a)(1) above the Contracting Officer will proceed with the actions necessary to support obtaining the requested funds.

(c) Upon receipt of the funds requirement proposal described under (a)(2) above, the Contracting Officer will perform an analysis of such proposal, and the parties will promptly pursue agreement as to the amount of funds mutually determined to be necessary to cover the termination costs.

(d) Within 90 days of receipt of the Contractor's funds requirement proposal described under (a)(2) above, the Contracting Officer will provide the Contractor direction on the source of funds to cover task order termination costs. In the event that the Contracting Officer does not provide such specific redirection of task order funds or provide other unobligated funds within the above-noted 90-day period, the Contracting Officer shall be deemed to have authorized the redirection of the funds as proposed by the Contractor in its notification.

(e) The Contracting Officer will document the transfer of funds by the subsequent issuance of a task order amendment.

(f) Nothing in this Article G-7 shall be deemed to limit or otherwise affect the rights of the Contractor under paragraph (k) of Clause I-12, Limitation of Cost (FAR 52.232-20); Limitation of Funds (FAR 52.232-22) (Deviation).

(g) In no event shall Construction of Facilities appropriated funds be used for termination costs other than for the authorized CoF project(s).

G-8 IDENTIFICATION AND MARKING OF GOVERNMENT EQUIPMENT

NFS 1852.245-74, "Identification and Marking of Government Equipment," dated January 2011, is incorporated into this Contract with the understanding that the Contractor's established practice, methods and procedures are deemed to satisfy paragraphs (a)–(f) for identifying, marking, reporting, procuring, addressing, and delivering Government equipment.

G-9 SMALL BUSINESS SUBCONTRACTING PLAN

(a) Attachment D sets forth the Contractor's Small Business Subcontracting Plan as agreed to by the Parties.

(b) In applying paragraph (d)(9) of FAR 52.219-9, Small Business Subcontracting Plan (JAN 2011), it is understood and agreed that the requirement that the Contractor require subcontractors (except small business concerns) who receive subcontracts in excess of $650,000 ($1,500,000 for construction of any public facility) to adopt a similar plan only applies to subcontracts which have subcontracting possibilities. In those cases where the subcontract meets the thresholds but no plan is adopted, the subcontract file shall document why that is the case.

(c) The standards set forth in paragraph (b) above shall also apply to letter subcontracts. However, in acknowledgment of the urgency associated with letter-contract procurements, the small business subcontracting plans included in letter contract files may be preliminary in nature. Furthermore, in limited cases of extreme urgency, development of such preliminary plans for letter contracts may take place after letter-contract award, but in such instances the Contractor shall ensure that the plans are established as soon as possible in order to maximize achievement of Small Business procurement goals.

(d) In applying paragraph (k) of said FAR 52.219-9, Small Business Subcontracting Plan, it is understood and agreed that the failure of a subcontractor to comply in good faith with the clause of its subcontract entitled "Utilization of Small Business Concerns", or with any plan required to be included in its subcontract, shall be a material breach of such subcontract, but that such failure on the part of the subcontractor shall not itself constitute a breach of this prime Contract. However, a failure of the Contractor to comply in good faith with such clause in this Contract, or with any plan required to be included in this Contract, shall be a material breach of this Contract.

(e) The Contractor shall as soon as practicable notify the Contracting Officer of any material breach, known to the Contractor, of a subcontract caused by failure of a subcontractor to comply in good faith with its Small Business Subcontracting Plan.

G-10 PROGRAM/PROJECT MANAGEMENT

(a) Task orders for programs and projects issued under this Contract shall be managed by the Contractor in accordance with the following:

(1) NPD 7120.4D, NASA Engineering and Program/Project Management Policy, dated March 16, 2010.

(2) NPR 7120.6, Lessons Learned Process, dated March 22, 2005 (Revalidated w/change 1, January 22, 2010).

(3) Unless otherwise specified within this contract, NPR 7120.10, Technical Standards Products for NASA Programs and Projects, dated April 22, 2011, is incorporated, with the understanding that the Contractor's internal processes and procedures satisfy Section P.5, Measurement/Verification, for the documentation of technical standards followed by non-space flight programs and projects.

(b) Task orders for space flight programs/projects issued under this Contract shall be managed by the Contractor in accordance with the following:

(1) It is the understanding of the parties that the Government is in the process of updating the requirements of NPR 7120.5, NASA Space Flight Program and Project Management Requirements. As an interim requirement the Contractor shall:

(i) Begin to develop procedures and processes and/or employ practices consistent with the applicable portions of Draft NPR 7120.5E dated January 31, 2012;

(ii) Complete by April 30, 2012, the analysis of requirements found in Draft NPR 7120.5E dated January 31, 2012;

(iii) Complete within 60 days of NASA's written notice to JPL of the final NPR 7120.5E release in NODIS the analysis of the requirements contained therein, focusing primarily on the changes from Draft NPR 7120.5E ;

(iv) Collaboratively work with NASA to incorporate applicable portions of Final NPR 7120.5E into the Contract via bilateral modification; and

(v) Fully implement the bilateral modification incorporating applicable portions of final NPR 7120.5E by the latter of April 1, 2013, or 6 months after the execution date of the subject bilateral modification.

(2) Program/Project Management Certification

(i) The Contractor shall ensure that individuals functioning as NASA Program/ project managers at JPL possess and demonstrate levels of proficiency and competency appropriate to their positions. Consequently, the Contractor shall create, implement and maintain a "JPL Certification Program" using NASA's Program/Project Management Certification Program as a guideline.

NASA will designate which Programs/Projects are subject to this requirement. The Contractor shall then have 12 months to certify the individual appointed to the position in accordance with the JPL Certification Program. Individuals functioning in such positions for Programs/projects designated by NASA shall:

(a) Have levels of proficiency and competency commensurate with the requirements identified in the JPL Certification Program;

(b) Maintain skills currency through continuing education, professional development, training, assignments and job-related experiences.

(ii) The Contractor shall document, maintain and make available the following documents to NASA for review upon request:

(a) The requirements for individuals to be certified under the JPL Certification Program;

(b) The established procedure for certification of individuals under the JPL Certification Program;

(c) An assessment demonstrating how the JPL Certification Program aligns with NASA's Program/project Management Certification Program resulting in JPL's program being functionally equivalent;

(d) The Program/projects that NASA has designated requiring JPL Certification;

(e) The names of the individuals that have been certified using the JPL Certification Program.

(c) Task orders for research and technology programs/projects issued under this Contract shall be managed by the Contractor in accordance with the following:

(1) NPR 7120.8, NASA Research and Technology Program and Project Management Requirements, dated February 5, 2008 (w/change 1 dated November 24, 2010). NPR 7120.8 will be implemented predicated on the following conditions:

Within Section P.2., Applicability, paragraph b., add new subparagraph 1. as follows: The NPR may either be implemented at the program level or at the project level and will apply to programs, individual research tasks, or individual research projects awarded or directed to the Contractor as designated in the task order. The Contractor will comply with the R&T enabling technology program management requirements set forth in annual calls such as, but not limited to, ROSES or other NASA-directed R&T

projects. Research portfolios initiated by the Contractor that are carried out under the Contractor's Research and Technology Development (R&TD) projects are excluded from this requirement.

(d) Task orders for Information Technology projects directly funded by NASA issued under this Contract shall be managed by the Contractor in accordance with the following:

(1) NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements, dated November 3, 2008.

G-11 USE OF DEPARTMENT OF DEFENSE SERVICES

The Contractor shall, to the extent required by the Contracting Officer, utilize Department of Defense audit, source inspection and property administration services. Other administrative services of the Department of Defense, which may be available to the Contractor, shall be utilized to the extent deemed practicable by the Contractor.

G-12 REFERENCES TO FAR "RIGHTS IN DATA" CLAUSE

References in FAR 52.227-16, Additional Data Requirements (JUN 1987), to the FAR Clause at 52.227-14, Rights in Data (DEC 2007), shall be deemed to refer to FAR 52.227-14, Rights in Data—General (DEC 2007)(ALT II, III, V)(DEC 2007), of this Contract.

G-13 NASA ISSUANCE SYSTEM AND GOVERNMENT POLICIES

(a) For purposes of this Clause, Government Policies includes the NASA Management Directives System publications ("NASA Issuances"); certain other Government orders, regulations, procedures, manuals, or advisories (e.g., Federal Aviation Administration Advisory Circulars; National Industrial Security Program Operating Manual) that NASA actively determines applicable to the Contractor's performance under the Contract; and Executive Orders of the President.

(b) In performing work under this Contract, the Contractor shall comply with the requirements of the Government Policies, or parts thereof, so identified in Sections A through J of the Contract.

(1) Except as provided for in paragraph (c) of this clause, the Contracting Officer, by unilateral modification to the Contract, may add, modify, or delete the requirements of Government Policies, or parts thereof, in accordance with FAR 52.243-2, Changes–Cost Reimbursement (AUG 1987) Alt V (APR 1984).

(2) Attachment C to the Contract is a quick reference of the Government Policies that are applicable to the Contractor's performance under this Contract. Attachment C will be timely updated by the Contracting Officer whenever Government Policies have been added or deleted.

(3) Where the Government Policy prescribes a responsibility to a specific government organization or any subdivision thereof or to a specific government official or position

up to the level of a NASA Center Director, it is the presumption of the parties that the Contractor shall comply with the requirements of the Government Policy with the functional or managerial equivalent within its own organizational structure, unless otherwise directed by the Contracting Officer. To the extent the Contractor believes it cannot comply with the requirements of the Government Policy with its own functional or managerial equivalent, the Contractor shall so inform the Contracting Officer in accordance with (c)(1) of this Article.

(c) Non-exigent circumstances. Except as provided for in paragraph (d) of this Article, the Contracting Officer shall notify the Contractor in writing of NASA's intent to add, modify, or delete a Government Policy.

(1) Within 30 working days after receipt of the Contracting Officer's notice, the Contractor shall provide a written assessment of the impact of the Contractor's compliance with the Government Policy being proposed for addition, modification, or deletion. This assessment shall address the impact on Contract cost and funding, technical performance, and schedule and identify any potential inconsistencies between this Government Policy and other terms and conditions of the Contract. The Contractor, as part of this assessment, may also advise the Contracting Officer of other potential impacts to the Contractor's performance under this Contract by providing a written rationale as to why the additional or modified Government Policy is not appropriate for incorporation into the Contract. Further, to the extent the Contractor believes its own policy or procedure is the functional equivalent or is more appropriate for application at JPL than the Government Policy being proposed for addition or modification, the Contractor may so advise the Contracting Officer by providing a written rationale as to why the Contractor's policy or procedure should be applicable under this Contract instead of the Government Policy. In addition, the Contractor may propose to satisfy the requirements of the Government Policies through the use of existing Contractor policies and procedures. NASA will have the unilateral right to determine whether the Contractor policies and procedures meet the outcome of the particular Government Policy. In the case of a Government Policy being proposed for deletion, the Contractor may similarly advise the Contracting Officer with a written rationale as to why the Government Policy should not be deleted.

(2) In the event that Contractor objects to the Government Policy being proposed for addition, modification, or deletion, the JPL Director may, within the 30 working day period in (1) of this paragraph, request, and schedule consultation with Associate Administrator, Mission Support Directorate or one of his or her Deputies regarding any such objection.

(3) The Contractor may, in those situations where NASA has given notice of its intent to add, modify, or delete more than several Government Policies, request an extension in time at any time prior to the expiration of the 30 working days provided in (1) of this paragraph. Such a request shall be made in writing to the Contracting Officer. Any period of extension granted to the Contractor under this paragraph by the Contracting Officer shall be added to the time in which the JPL Director has under (2) of this paragraph.

(4) The parties acknowledge that funding of additional or modified Government Policies may be done through one of several methods, including, but not limited to: (i) adjustment to the Contractor's burden rate; (ii) absorbing cost through the re-scoping of tasks performed under the Contract, or (iii) providing discretely funded task orders for the initiative. The actual funding mechanism shall be at the final discretion of the Associate Administrator, Mission Support Directorate.

(5) If, at the completion of the 30 working day review period, or any agreed upon extension thereof, and after considering the information provided by the Contractor in (1) and (2) of this paragraph and any other information, NASA decides to add, modify, or delete a Government Policy (the "Final Requirements"), it shall do so pursuant to the FAR 52.243-2, Changes – Cost Reimbursement (AUG 1987) (Alt V)(APR 1984) and the Contractor so notified in writing. The Contractor shall immediately comply with the Final Requirements. It is understood that NASA must identify the funding mechanism prior to JPL incurring actual costs associated with the Final Requirements.

(d) Exigent Circumstances. The Contracting Officer may, in those situations where the Government believes there are exigent circumstances, unilaterally modify the Contract to add, modify, or delete a Government Policy notwithstanding paragraph (c) of this clause. The Contractor shall immediately comply with the added, modified, or deleted requirements. The Contract modification shall be made pursuant to FAR 52.243-2, Changes–Cost Reimbursement (AUG 1987) (Alt V)(APR 1984) and the Contractor so notified in writing as soon as practical.

(e) Regardless of the performer of the work, the Contractor is responsible for complying with the requirements of this Article. The Contractor is responsible for flowing down the requirements of this Article to subcontracts at any tier to the extent necessary to ensure the Contractor's compliance with the requirement of this Article.

G-14 EXPORT CONTROL REGULATIONS

(a) General. In the performance of this Contract, the Contractor will from time-to-time be required to handle, process, store, or transmit electronically technical data, software or equipment which may be subject to the export laws and regulations of the United States. The Contractor shall control access to scientific and technical information of national interest, which it handles, processes, stores or transmits electronically or manually consistent with NPD 2190.1A, NASA Export Control Program, dated May 24, 2001 (Revalidated May 5, 2006). The Contractor shall control access to these assets and maintain appropriate records as required by law. The Contractor will from time-to-time be required to deliver, disclose, or transfer (export) to foreign entities, (including foreign nationals that are Contractor employees) technical data, software or equipment which may be subject to the export laws and regulations of the United States and which may require an export license (or other regulatory agency approval) or the use of a license exemption/exception. Such exports, which would include, but not be limited to, export of technical data as defined at 22 CFR 120.10, will from time-to-time be required for, and be in furtherance of, the performance of this Contract. The Contractor shall comply with Federal export laws and regulations in the performance of this Contract and shall include appropriate provisions in

its subcontracts directing its subcontractors to comply with applicable export laws and regulations in the performance of their subcontracts.

(b) NASA-Sponsored Work.

(1) In the performance of NASA-sponsored work pursuant to Article G-5 (Task Ordering Procedure) of this Contract where such work is in furtherance of planned or in-place international agreements between NASA and a foreign partner, the Contractor will identify to NASA that such work requires the transfer to foreign entities of equipment, software or technical data controlled under the International Traffic In Arms Regulations (ITAR) or the Export Administration Regulations (EAR). In each such instance, language will be included in the task plan indicating that the Contractor is required under the terms of this Contract and the task order to deliver, disclose, or transfer (export) technical data, software or equipment to a specific foreign entity, including appropriate limitations, provisos and instructions applicable to the specific transfers. Any and all exports in support of such task plans which do not fall within either generally available license exceptions/exemptions, including but not limited to the ITAR exemption available under 22 CFR 125.4 (b)(3), shall be exported under Contractor obtained licenses, unless NASA and the Contractor determine that the export is unnecessary for performance of the applicable task plan. To the extent that the Government agrees to the use of a Government Bill of Lading to satisfy the requirements of ITAR exemption 22 CFR 126.4, the Contractor shall provide all documentation required for NASA to issue such GBLs.

(2) In the event the Contractor determines that in performance of NASA-sponsored work pursuant to Article G-5 (Task Ordering Procedure) of this Contract it would be appropriate to deliver, disclose or transfer (export) technical data, software or equipment to a foreign entity and such work is not in furtherance of a planned or in-place international agreement between NASA and a foreign partner, the Contractor may request NASA to obtain export authorization for such export. If NASA concurs that such export is necessary, NASA may authorize the use of exemptions uniquely available to the U.S. Government or seek to obtain a license. The Contractor shall provide all documentation required for NASA to issue Government Bills of Lading (GBLs) or to obtain a license. From time-to-time other forms of authorization to the Contractor may be used by NASA (e.g., a letter from the Contracting Officer).

(c) Work for Other U.S. Government Sponsors. In the performance of non-NASA-sponsored work for other U.S. Government sponsors pursuant to Article G-5 (Task Ordering Procedure) of this Contract, the Contractor will identify to NASA that such work requires the transfer to foreign entities of equipment, software or technical data controlled under the ITAR or EAR. In each such instance, subject to NASA confirmation with the U.S. Government sponsor that such export is required, language will be included in the task order indicating that the Contractor is required under the terms of this Contract and the task order to deliver, disclose, or transfer (export) technical data, software or equipment to a specific foreign entity. Any and all exports in support of such task orders which do not fall within either generally available license exceptions/exemptions or the 22 CFR 125.4(b)(3) exemption shall be exported, as specified by the other U.S. Government sponsor, using

exemptions available to that sponsor or using a license obtained by that sponsor or by the Contractor.

(d) Work for Non-U.S. Government Sponsors. Any and all exports in support of task orders for non-U.S. Government sponsored work that does not fall within generally available license exceptions/ exemptions shall be exported pursuant to a license obtained by the Contractor or the non-U.S. Government sponsor. The Contractor shall not utilize the 22 CFR 125.4(b)(3) or other exemptions uniquely available to the U.S. Government for such exports.

(e) Limitations. In no instance will NASA apply for a Technical Assistance Agreement or a Manufacturing License Agreement as defined in the ITAR on behalf of the Contractor. In no instance will NASA apply for an export license on behalf of a subcontractor. In all cases not covered by relevant license exemptions as discussed above or licenses applied for by NASA for NASA-sponsored work as agreed with the Contractor, the Contractor shall be responsible for obtaining required export licenses or other approvals for performance of work under this Contract.

(f) Notification. In all instances wherein the Contractor applies for an export license, other prior approval, commodity jurisdiction, classification request or advisory opinion, in furtherance of work under this Contract, a copy of the Contractor's application package or other request as submitted to the U.S. government regulatory agency shall be provided to the NMO at JPL and The Export Control and Interagency Liaison Division, NASA Headquarters, HQ-TH000, Washington, DC 20546 (Attn: Manager, International Technology Transfer Policy and NASA Export Administrator).

(g) Record keeping. The Contractor shall be responsible for all regulatory record keeping requirements associated with the use of license exemptions/exceptions and licenses.

(h) Annual Self-Assessment. For purposes of ensuring adequacy and compliance, the Contractor shall conduct an annual self-assessment consistent with the Export Control Program Audit per NPR 2190.1B (effective 12/27/2011), Chapter 7, but not including the NPR's Section 7.3.1(i) or 7.4. The annual self-assessment, to be conducted by a JPL organization, shall verify, via sampling that required screening and licensing procedures are regularly followed and that required documents are maintained in compliance with the requirements of the EAR and the ITAR. This includes a review to ensure that appropriate records of all exports or transfers affected in support of NASA cooperative international programs are maintained in accordance with relevant regulations. The Contractor will brief the Headquarters Export Administrator on actions taken and intended to be taken as a result of such self-assessment by March 31 of each year.

G-15 FACILITIES

(a) Authorizations. Authorizations for acquisition of facilities will be provided as follows:

(1) Authorizations for the acquisition of facilities involving the use of funds appropriated for construction of facilities, or involving construction of any facility requiring more than $500,000 of funds from other sources, will be provided pursuant to the terms of Article C-1 subparagraph (c)(1) of this Contract.

(2) In accordance with the facilities terms and conditions of this Contract acquisition of other facilities will be made by the Contractor for the performance of work under Article C-1 paragraph (a), or Article C-1 paragraph (b), provided, however, that nothing shall preclude the issuance of a task order, pursuant to Article C-1 subparagraph (c)(1) for the acquisition of any such other item of facilities, and provided further, that nothing herein shall preclude the Government from furnishing any item of facilities in lieu of authorizing the Contractor to acquire such item, and

(3) The Contractor shall manage all facility projects funded from NASA appropriations, inclusive of projects involving funds for which NASA will be reimbursed by other federal agencies, estimated to cost $50,000 or less. Any facility project in excess of $50,000 must be approved in writing by the NMO Facility Manager prior to the obligation of any funds for the proposed project. The requirements of this paragraph are in addition to, and not in lieu of, the requirements of Article I-5, Subcontracts (FAR 52.244-2) (OCT 2010) (Alt I) (JUN 2007) (Deviation). NASA Form 1509s with a value of $500,000 and below shall be submitted to the NMO Facility Manager for approval and NASA Form 1509s valued greater than $500,000, must be submitted to NASA Headquarters Facilities Engineering Division, Code LD030 for approval. A copy of the NASA Headquarters' approved 1509 will be forwarded to the Contracting Officer and NMO Facility Manager. NPR 8820.2F, Facility Project Requirements, dated January 28, 2008, shall be utilized by the Contractor in preparing facility approval and implementation documents respectively. This applies to both Government-owned facilities and facilities leased by the Contractor. The definition of words utilized in facility approval documents (e.g., "construction", "repair", "rehabilitation", and "facility") shall have the meanings set forth in Appendix A to NPR 8820.2F, Facility Project Requirements, dated January 28, 2008.

G-16 DESIGNATION OF NEW TECHNOLOGY REPRESENTATIVE AND PATENT REPRESENTATIVE (NFS 1852.227-72) (JUL 1997)

(a) For purposes of administration of the clause of this Contract entitled "New Technology" or "Patent Rights—Retention by the Contractor (Short Form)", whichever is included, the following named representatives are hereby designated by the Contracting Officer to administer such clause:

New Technology Representative
Office Code: MS/180-801
Address: NASA Management Office at JPL
4800 Oak Grove Dr.
Pasadena, CA 91109

Patent Representative
Office Code: MS/180-802
Address: NASA Management Office at JPL
4800 Oak Grove Dr.
Pasadena, CA 91109

(b) Reports of reportable items, and disclosure of subject inventions, interim reports, final reports, utilization reports, and other reports required by the clause, as well as any correspondence with respect to such matters, should be directed to the New Technology Representative unless transmitted in response to correspondence or request from the Patent Representative. Inquires or requests regarding disposition of rights, election of rights, or related matters should be directed to the Patent Representative. This clause shall be included in any subcontract hereunder requiring a "New Technology" clause or "Patent Rights--Retention by the Contractor (Short Form)" clause, unless otherwise authorized or directed by the Contracting Officer. The respective responsibilities and authorities of the above-named representatives are set forth in 1827.305-370 of the NASA FAR Supplement.

(End of Clause)

G-17 MANAGEMENT AND OVERSIGHT OF PROPERTY AT OVERSEAS TRACKING STATIONS

The Contractor shall provide technical surveillance and guidance at Government facilities at foreign locations in support of NASA work, covered by this Contract, including Deep Space Network Sites in Spain and Australia. Such oversight shall include an annual site visit for the purpose of conducting a property management system audit. The results of such audits shall be disclosed to the NASA Industrial Property Officer (IPO).

G-18 ALLOCATED DIRECT COST REPORTING

The Contractor will provide financial reports in sufficient detail to enable the Contracting Officer to assess the effectiveness of Contractor's planning, monitoring and control of Allocated Direct Costs. These reports will include:

(a) An annual report which shall include

(1) An overview of the contents of the budget together with the significant factors, requirements and assumptions that influenced the development of the allocated direct cost budget for the current fiscal year,

(2) The results of the prior fiscal year baseline allocated direct cost budget and actuals, including

(A) Summary of all allocated direct cost rates, including pool and base.

(B) Allocated Direct Cost Expenses (final allocated direct cost pools). Schedule of claimed allocated direct cost expenses by pool and element of cost as identified in the accounting records.

(C) Claimed allocation bases, by element of cost, used to distribute allocated direct costs.

(D) Reconciliation of books of account (i.e., General Ledger) and claimed direct costs.

(E) Schedule of costs by task order and project.

(F) Schedule of cumulative costs claimed by subcontract.

(G) Subcontract information. Listing of subcontracts awarded to companies for which the contractor is the prime or upper-tier contractor (include prime and subcontract numbers; subcontract value and award type; amount claimed during the fiscal year; and the subcontractor name, address, and point of contract information).

(H) Reconciliation of total payroll per IRS form 941 to total labor costs distribution.

(I) Listing of decisions/agreements/approvals and description of accounting/ organizational changes.

(3) The following supplemental JPL information is not required to determine if the annual Allocated Direct Cost report is adequate, but may be required during the audit process:

(A) Cost data for comparative analysis of allocated direct costs detailed by account to prior fiscal year.

(B) General Organizational information and Executive compensation for the five most highly compensated executives at JPL. See 31.205-6(p). Additional salary reference information is available at the http://www.whitehouse.gov/omb/procurement_index_exec_comp/.

(C) Identification of prime contracts under which JPL performs as a subcontractor.

(D) Procedures for identifying and excluding unallowable costs from the costs claimed and billed (excludes contractors where the procedures have not changes from the previous year’s submission).

(E) Audited financial statements and other financial data for JPL (e.g., trial balance, compilation, review, etc.).

(F) Management letter from outside CPAs issued in conjunction with the JPL A-133 concerning any internal control weaknesses at JPL.

(G) Actions that have been and/or will be implemented to correct the weaknesses described in the management letter from subparagraph (F) of this section.

(H) List of all planned internal audit reports related to JPL that have been completed and issued since the last disclosure of internal audit reports to the Government.

(I) Annual internal audit plan of scheduled audits to be performed at JPL in the fiscal year when the final allocated direct cost rate submission is made.

(J) Minutes of the Meeting of the Board of Directors related to JPL.

(K) Listing of delay claims and termination claims applicable to JPL submitted which contain costs relating to the subject fiscal year.

(L) Access to JPL Task Orders, which generally include a synopsis of all pertinent contract provisions, such as: Contract type, contract amount, product or service(s) to be provided, contract performance period, rate ceilings, advance approval requirements, pre-contract cost allowability limitations, and billing limitations.

(4) Projections of estimated allocated direct costs and business-base assumptions for the subsequent five years;

(b) Monthly reports which shall include

(1) A comparison of baseline budget and allocated direct cost actuals by budget category,

(2) A variance report of the allocated direct costs actually incurred compared to the applied allocated direct costs and associated distribution bases, and

(3) Report any significant changes to the baseline allocated direct cost budget, actuals or business base;

(c) And such other special reports as the Contracting Officer may request.

G-19 WHOLE AGREEMENT

(a) This Contract, NNN12AA01C, contains the whole agreement between the Parties.

(b) Appendices to this Contract are separate and non-binding documents appended for information only. Appendices do not constitute a part of this Contract.

G-20 NFS 1852.245-70, CONTRACTOR REQUESTS FOR GOVERNMENT-PROVIDED EQUIPMENT (JAN 2011)(ALT I)(JAN 2011)

(a) "Equipment," as used in this clause, is defined by FAR 52.245-1.

(b) (1) Upon determination of need by JPL or its subcontractors for any Government-owned equipment with an item value over $75,000 for performance of this Contract, the Contractor shall provide to the Contracting Officer, in accordance with the consent to subcontract provisions set forth in Article I-5, Subcontracts (FAR 52.244-2) (OCT 2010), (Alternate I) (JUN 2007) (Deviation), a written request justifying the need for the equipment and citing the applicable FAR or contract authority for use of Government-provided equipment. This requirement is only applicable to property purchased for use at the JPL facility, or on other NASA real property. If the Contractor plans to acquire property for other non-NASA places of performance, the Contractor shall request Contracting Officer approval. Equipment being acquired as a deliverable end item

listed in the Contract or as a component for incorporation into a deliverable end item listed in the Contract is exempt from this requirement.

(2) Notwithstanding the Contractor's ability to provide Government property (other than Equipment as defined in this provision) to its subcontractors in the performance of subcontracts under this Contract, the Contractor shall be authorized to permit its subcontractors to use Government- provided equipment only under the circumstances specified below. Upon determination by a subcontractor of need for any Government-provided equipment item for performance of a subcontract under this Contract, the subcontractor shall provide to the Contractor a written request justifying the need for the equipment and the reasons why subcontractor- owned property cannot be used, citing the applicable FAR or subcontract authority for use of the Government- provided equipment. Before authorizing the use of the requested Government- provided equipment, the Contractor shall review the subcontractor's written request and such other information as it deems relevant and shall conclude whether the need is justified. Equipment being acquired as a deliverable end item listed in the subcontract or as a component for incorporation into a deliverable end item listed in the subcontract is exempt from this requirement.

(c) In the event the Contracting Officer issues written authorization to provide property, the Contractor shall screen Government sources to determine the availability of property from Government inventory or excess property.

(1) The Contractor shall review NASA inventories and other authorized Federal excess sources for availability of items that meet the performance requirements of the requested property.

(i) If the Contractor determines that a suitable item is available from NASA supply inventory, it shall request the item using applicable Center procedures.

(ii) If the Contractor determines that an item within NASA or Federal excess is suitable, it shall contact the NMO Industrial Property Officer to arrange for transfer of the item from the identified source to the Contractor.

(2) If the Contractor determines that the required property is not available from inventory or excess sources, the Contractor shall note the acquisition file with a list of sources reviewed and the findings regarding the lack of availability. If the required property is available, but unsuitable for use, the contractor shall document the rationale for rejection of available property. The Contractor shall retain appropriate cross-referenced documentary evidence of the outcome of those screening efforts as part of its property records system.

(End of Clause)

G-21 FINANCIAL MANAGEMENT

(a) General. The Contractor shall maintain financial management operating procedures and engage in continuous monitoring activities to enable the review and analysis of financial data to identify inaccurate data, abnormal balances, accounting relationship differences and other financial reporting anomalies resulting in reporting discrepancies. The Contractor shall ensure that various tools and methods are used to thoroughly analyze and review the financial data reported both internally and externally.

(b) Operating Procedures. To ensure the most accurate financial data, the Contractor's financial management operating procedures shall provide guidance relative to executing project business activities as well as the framework for performing institutional financial activities for program/project managers, line managers, business managers and technical and business staff. The Contractor's procedures shall be designed to ensure the use of standard and consistent methods of processing, reporting and reviewing financial data. The Contractor's procedures shall serve as a resource to assist financial management personnel with their day-to-day operations.

(c) Monitoring. Continuous monitoring shall be performed to assess and evaluate (a) internal controls, (b) compliance with Generally Accepted Accounting Principles (GAAP) and the financial requirements of this Contract and (c) evidence that balances and activity reported in the Contractor's financial statements are accurate and complete. The monitoring shall ensure that errors and/or discrepancies are identified and corrected in a timely manner and that there are ongoing management reviews and validations of financial data and internal controls. This would also include providing information/documentation necessary to assist NASA with the monthly Continuous Monitoring Program (CMP) CFO Certification requirements.

G-22 COST ACCRUALS

(a) The Contractor's accounting records shall be maintained on a modified accrual basis. Every practicable effort shall be made to ensure cost accruals are as accurate as possible. Generally accepted accounting methods shall be used in developing accruals. Simplified methods for monthly accruals such as estimates based on prior month reporting may be used when demonstrated to be reasonably reliable. Accruals shall be recorded in the appropriate accounts as defined by the fiscal period.

(b) The Contractor shall incorporate accruals into the Monthly Contractor Financial Management Report, NF 533M, that is delivered to NASA.

(c) It is recognized that the Contractor's accounting periods differ from the calendar month basis used for NASA accounting. The Contractor's cost accruals, however, need not include an estimate for the costs to be incurred during the period from the end of the Contractor's accounting period to the end of the calendar month, quarter or fiscal year.

G-23 TRAVEL

(a) The Contractor shall maintain comprehensive travel management policies and procedures to enable efficient travel. The Contractor shall continuously evaluate travel and relocation programs and policies, examine new technologies and automated systems, and educate and train travel personnel. The Contractor shall ensure that travel is conducted in a responsible manner, with the need to minimize costs, and that policies and procedures are communicated in a clear manner to personnel. It is incumbent upon travelers, authorizing and approving personnel and financial management personnel to be familiar with the Contractor's policies, procedures and requirements in relation to their specific roles in the travel process. Quality assurance reviews shall be conducted by the Contractor to ensure that travel costs claimed under this Contract comply with the Contractor's policies and procedures.

(b) The Federal Travel Regulation (FTR), Joint Travel Regulation (JTR) and Standardized Regulations (SR) are applicable to the Contractor to the extent invoked by FAR Subpart 31.2, Contracts with Commercial Organizations, consistent with Article B-5, Allowable Costs, of this Contract.

G-24 NFS 1852.245-78, PHYSICAL INVENTORY OF CAPITAL PERSONAL PROPERTY (JAN 2011)

The parties agree that:

(a) The Contractor's annual property inventory, and its associated processes and procedures, satisfy paragraphs (a)(1)-(2) inventory requirements.

(b) The NASA Industrial Property Officer's annual validation of the Contractor's property system satisfies the paragraph (b) written authorization and is considered the approved waiver.

(c) The Contractor's monthly Contractor Held Assets Tracking System (CHATS) and NASA Form 1018 (NF 1018) reports satisfy the reporting requirement in paragraphs (c)(1)-(2).

[END OF SECTION]

SECTION H—SPECIAL CONTRACT REQUIREMENTS

H-1 LISTING OF CLAUSES INCORPORATED BY REFERENCE

The following Contract clauses pertinent to this section are hereby incorporated by reference:

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.223-2	DEC 2007	AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS
52.223-5	MAY 2011	POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION (with ALT 1) (MAY 2011) and ALTERNATE 2 (MAY 2011)
52.223-15	DEC 2007	ENERGY EFFICIENCY IN ENERGY- CONSUMING PRODUCTS
52.223-16	DEC 2007	IEEE 1680 STANDARD FOR THE ENVIRONMENTAL ASSESSMENT OF PERSONAL COMPUTER PRODUCTS
52.223-17	MAY 2008	AFFIRMATIVE PROCUREMENT OF EPA-DESIGNATED ITEMS IN SERVICE AND CONSTRUCTION CONTRACTS

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.208-81	NOV 2004	RESTRICTIONS ON PRINTING AND DUPLICATING
1852.223-70	APR 2002	SAFETY AND HEALTH
1852.223-75	FEB 2002	MAJOR BREACH OF SAFETY OR SECURITY (ALT I) (FEB 2006)
1852.223-76	JULY 2003	FEDERAL AUTOMOTIVE STATISTICAL TOOL REPORTING
1852.228-72	SEP 1993	CROSS-WAIVER OF LIABILITY FOR SPACE SHUTTLE SERVICES

CLAUSE NUMBER	DATE	TITLE
1852.228-76	DEC 1994	CROSS-WAIVER OF LIABILITY FOR SPACE STATION ACTIVITIES
1852.228-78	SEP 1993	CROSS-WAIVER OF LIABILITY FOR NASA EXPENDABLE LAUNCH VEHICLE (ELV) LAUNCHES
1852.235-73	DEC 2006	FINAL SCIENTIFIC AND TECHNICAL REPORTS
1852.242-72	AUG 1992	OBSERVANCE OF LEGAL HOLIDAYS (ALT II) (OCT 2000)
1852.244-70	APR 1985	GEOGRAPHIC PARTICIPATION IN THE AEROSPACE PROGRAM
1852.225-70	FEB 2000	EXPORT LICENSES AND ALT I (FEB 2000) Insert JPL in paragraph B

H-2 REPRESENTATIONS AND CERTIFICATIONS

The representations and certifications completed by the Contractor online via ORCA (52.204-8) are incorporated herein by reference.

H-3 KEY PERSONNEL AND FACILITIES

(a) The personnel listed in (c) below, or specifically detailed in an AO or task plan as key personnel are considered essential to the work being performed under this Contract. Before removing, replacing, or diverting any of the listed or specified personnel, the Contractor shall:

(1) notify the NASA Program Director or cognizant Division Director reasonably in advance and

(2) discuss with that individual the justification for the removal, replacement or diversion (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the effort being performed.

(b) The Contractor shall make no diversion without the cognizant NASA Associate Administrator's consent.

(c) The list of personnel shown below may, with the consent of the Associate Administrator for the Science Mission Directorate and the JPL Director be amended from time to time during the course of the Contract to add or delete personnel:

(1) "Director For" a JPL directorate or an equivalent position and above.

(2) JPL Project Managers and Project Scientists assigned full time to perform for a “flight project”, including AO projects. The term “flight project” is a project which has as one of its principle purpose the construction and operation of one or more aeronautic or space vehicles and necessary ground support.

(d) The Contracting Officer will be notified in writing of changes at the “JPL Director For” or an equivalent position and above.

H-4 MANAGEMENT CONTROLS

(a) The Contractor shall be responsible for maintaining, as an integral part of its organization, effective systems of management controls for both administrative and programmatic functions. Management controls comprise the plan of organization, methods, and procedures adopted by management to reasonably ensure that: the mission and functions assigned to the Contractor are properly executed; efficient and effective operations are promoted; computational, infrastructure, and data resources’ confidentiality, integrity, and availability are maintained; resources are safeguarded against waste, loss, mismanagement, unauthorized use, or misappropriation; all encumbrances and costs that are incurred under the Contract and fees that are earned are in compliance with applicable clauses and other current terms, conditions, and intended purposes; all collections accruing to the Contractor in connection with the work under this Contract, expenditures, and all other transactions and assets are properly recorded, managed, and reported; and financial, statistical, and other reports necessary to maintain accountability and managerial control are accurate, reliable, and timely. The systems of controls employed by the Contractor shall be documented and satisfactory to NASA. Such systems shall be an integral part of the Contractor’s management functions, including defining specific roles and responsibilities for each level of management, and holding employees accountable for the adequacy of the management systems and controls in their areas of assigned responsibility. The Contractor shall institute a program to periodically review the management systems and controls employed in its programmatic and administrative operations to ensure that they are adequate to provide reasonable assurance that the objectives of the systems are being accomplished and that these systems and controls are working effectively. All aspects of the contractor’s systems of management controls for JPL are subject to review and audit by NASA. The Contractor will provide NMO with a copy of the annual plan for JPL internal audits and be opened to suggestions by NMO regarding scope or focus of any scheduled internal audits. Upon request, the Contractor will provide NMO with copies of any of these internal audit reports once published.

(b) The Contractor shall be responsible for maintaining, as a part of its operational responsibilities, a baseline quality assurance program that implements documented performance, quality standards, and control and assessment techniques. The Contractor shall institute a program to periodically review its quality assurance program to ensure that it is adequate to provide reasonable assurance that the objectives of the program are being accomplished and that the quality assurance program is working effectively. All aspects of the Contractor’s quality assurance program for JPL are subject to review and audit by NASA.

H-5 EXECUTIVE ORDERS

Executive Orders are legally binding orders given by the President of the United States, acting as the head of the Executive Branch, to federal administrative agencies such as NASA. Executive Orders are used to direct federal agencies or federal officials in the execution of their legal, statutory, regulatory, or policy duties, including the operations affecting federally owned facilities such a JPL. In the planning and execution of government funded programs/projects, as well as the operation of government facilities, the contractor shall, within the scope of the contract, perform in such a manner so as to support NASA meeting its obligations under Executive Orders, including the provision of any such data necessary for NASA to meet its reporting obligations. While Executive Orders may only apply to NASA on its face, the Contractor will provide technical, logistical, and other services as may be necessary to NASA.

H-6 WAGES, SALARIES AND PERSONNEL DATA

(a) The Contractor agrees that all wages, salaries, and other compensation being paid, or to be paid, to the employees of JPL are being paid, and will be paid, in accordance with the Contractor's established wage and salary policy and practice and that such payments will be reasonable and consistent therewith. Further, upon written request from the Contracting Officer, the Contractor agrees to furnish the Contracting Officer its wage and salary schedules, its nonacademic personnel policies, and amendments thereto and modifications thereof, including job titles contained within such rate ranges and/or other descriptive information identifying the types of positions within fifteen calendar days from the date the written request is received.

(b) The Contractor shall provide the following aggregated data on its work force employed at JPL: occupational distribution, educational levels, and average age and rate ranges. Such data shall be submitted annually.

(c) To the extent that these materials contain personally identifiable information, such records will be handled in accordance with the provisions of Article H-16 (Property Rights in Records).

H-7 SAFETY, HEALTH, AND MISSION ASSURANCE

In performing work under this contract, the Contractor shall perform work safely, in a manner that reasonably ensures: adequate protection of the public, employees, the facility (plant) and product from damage; adequate protection of the environment; application of measures to obtain success of missions; and shall be accountable for the safe performance of work. The Contractor shall integrate environmental, safety, health, and mission assurance requirements into program missions and Center operations. Environment, safety, health, and mission assurance programs shall be operated as an integral and visible part of how the organization conducts both its mission and facility operational business, including the management of both routine and emergency operations. The Contractor shall exercise due care commensurate with the associated hazards of the work. The Contractor shall ensure the management of environment, safety, health and mission assurance functions and activities becomes an integral and visible part of the Contractor's work planning and execution process.

In accordance with Article C-1, paragraph (d), the Contractor shall:

(A) Maintain safe functioning of the JPL facilities and operations.

(B) Establish, document, and implement a closed loop process for making technical decisions dealing with residual safety and mission success risk to JPL operations and activities. Note: Residual risk is the remaining risk that exists after all mitigation actions have been implemented or exhausted in accordance with the risk management process.

(C) Establish, implement, and communicate to employees a graduated/stepped process where employees may express their dissatisfaction with a response to a reported health or safety concern.

(i) As a minimum the appeal reporting process shall provide access to the:

(a) JPL Safety/Health Official(s)

(b) Director of JPL

(c) NASA Designated Agency Safety and Health Official (for unhealthful conditions)/Chief Safety and Mission Assurance Officer (for unsafe conditions)

(d) NASA Safety Reporting System (NSRS)

(ii) Similarly the Contractor shall establish and implement a process that not only provides for dissenting or minority opinions to be expressed and elevated during decision making processes but solicits dissenting or minority opinions.

(iii) The Contractor shall assist in the investigation of NSRS Reports as requested by NASA.

(D) Establish and implement safety and mission assurance requirements, policies, plans, procedures, and methodologies for JPL activities and operations.

(E) Designate a functional manager for safety and mission assurance, independent from programs and projects, to serve as the leader and focal point for the Contractor’s safety and mission assurance activities. Safety and mission assurance line management, supporting this functional manager in implementation of the safety and mission assurance effort, shall also be afforded independence from programs and projects.

(F) Implement Technical Authority in accordance with the Contractor’s “Safety and Mission Assurance (SMA) Technical Authority Implementation Plan”. The Contractor shall designate personnel to serve as Safety and Mission Assurance Technical Authorities (SMA TAs). These technical authorities will be independent from programmatic authority. In the general NASA Governance Model the technical authority role is to determine which safety and mission assurance requirements are to be applied to programs and projects and to rule on requests for waiver to the safety and mission assurance requirements. The Contractor’s SMA TAs shall review and endorse/approve or reject all requests for waivers to NASA and

Contractor safety and mission assurance requirements. Waiver requests will be prepared and submitted in accordance with NASA-STD-8709.20 (August 6, 2010), "Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements", paragraph A.1 of Appendix A, "Waiver/ Deviations Form".

(G) Include safety and mission assurance in technical reviews of development activities and operations.

(H) Document, disseminate, and use NASA and Contractor lessons learned to improve operations and activities.

(I) Identify correct and control recurrence of undesired events and non-conformances through a closed-loop corrective action system.

(J) Establish and implement a program to identify, assess, analyze and develop controls for all hazardous operations. The Contractor shall ensure that personnel who perform or control hazardous operations or who use or transport hazardous material are trained and certified (including physical and medical considerations) to do the job safely.

(K) Perform safety and mission assurance surveillance, inspections, and audits to assure compliance with applicable Federal, State, and local laws, regulations, requirements, and standards and the requirements of this Contract. This is consistent with implementation of ISO 9001 and AS 9100C. With the exception of the Contractor self-assessments described within H-16(e)(2)(iii) the records of these inspections and audits shall be available to NASA.

i. The Contractor shall perform periodic audits of providers and suppliers to verify ongoing implementation of agreed-to or contractual safety and mission assurance and risk management requirements and processes.

(L) As defined in Section H-16, the Contractor is subject to safety and mission assurance audits by NASA. The Contractor shall document and track any corrective actions resulting from those safety and mission assurance audits within the Surveys, Audits, Assessments, and Review Information Systems (SAARIS).

(M) The Contractor is expected to participate in NASA safety and mission assurance audits and assessments of NASA facilities. In the performance of this function, the Contractor shall identify and provide subject matter experts to support NASA audits and assessments.

(N) Notwithstanding Article G-13, NASA Issuance System and Government Policies, the Parties recognize that certain requirements documents that are referenced within the NPRs and NPDs cited in this section ("referenced documents") may be appropriate for inclusion in the contract. The Parties agree that NASA will identify referenced documents or specific requirements therein for inclusion in the contract to the Contractor, within 30 days of the effective date of the contract. The Contractor will respond to NASA within 90 days after receipt of the requirements. Those referenced documents not added as requirements through a bilateral contract modification shall be used by the Contractor as guidance.

H-7(1). SAFETY AND MISSION ASSURANCE

(A) On Contractor-led spaceflight missions governed by draft NPR 7120.5E dated January 31, 2012, NASA Space Flight Program and Project Management Requirements, the Contractor shall prepare a Safety and Mission Assurance Plan that includes the following information:

(i) The life cycle safety and mission assurance relevant functions and activities.

(ii) A graphical representation of the project organizational relationships and assurance roles and responsibilities.

(iii) The life cycle safety and mission assurance processes implemented on the project that relate to disciplines such as: procurement, management, design and engineering, design verification and test, software design, software verification and test, manufacturing, manufacturing verification and test, operations, and preflight verification and test.

(iv) Definition of data and information in each area of safety and mission assurance for each milestone review, including preparation for and participation in the Safety and Mission Success Review (SMSR). This information may be documented in the project Review Plan and only referenced in the Safety and Mission Assurance Plan.

(v) Definition of metrics to be used to measure progress toward successful completion of the project and to measure risk levels.

(vi) At the Contractor's discretion, other safety and mission assurance discipline plans (e.g., System Safety Plan, Software Assurance Plan, and Quality Assurance Plan) may be integrated into the project Safety and Mission Assurance Plan.

The Safety and Mission Assurance Plan will be approved by the Contractor's Safety and Mission Assurance Technical Authority.

(B) Additionally the Contractor shall assess and tailor the level of safety and mission assurance work (both hardware and software) needed to be performed commensurate with each lifecycle phase of the project, cost, schedule, risk and technical performance requirements. The parties agree that the content below does not necessarily apply to every task order**.** The list of exceptions will be documented and submitted to the Contracting Officer as early as practicable in formulation but not later than Preliminary Design Review with finalization and NASA approval of the exceptions to be completed no later than Key Decision Point-C (KDP-C). Changes to the list subsequent to KDP-C require NASA approval. Additionally, these requirements apply only to Contractor-led spaceflight missions which have not yet completed the KDP-B milestone on the effective date of the Contract.

(i) NPR 8715.6A, "NASA Procedural Requirement for Limiting Orbital Debris (w/Change 1 – 5/14/09)", dated May 14, 2009, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 1.3.10.1, 1.3.10.3, 1.3.13.2, 2.1.4, 2.2.1.7, 2.2.1.8, 2.2.1.9, 2.2.2.3, 2.2.2.5, 2.2.2.8, 2.2.2.9, 2.2.4.2.a, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 3.2.6, 3.2.7, 3.2.9, 3.2.10, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2.1, 3.3.2.2, 3.3.2.3, 3.3.2.4, 3.3.2.5, 3.3.3.1, 3.3.3.2, 3.3.3.3, 3.3.3.4, 3.4.1, 3.4.2, and 3.4.3 are applicable.

(c) Replace paragraph 1.3.10.2 with: "The Contractor SMA Director shall provide assistance to the program/project by reviewing and providing comments to ODARs and EOMPs to assist in determining compliance with this NPR and NSS 1740.14 or NASA-STD 8719.14."

(d) Replace paragraph 1.3.13.1 with: "The Contractor shall establish an orbital debris mitigation activity as a part of every Contractor-led spaceflight mission being funded, launched, operated, or managed by NASA."

(e) Replace paragraph 2.1.1 with: "The Contractor shall implement orbital debris requirements for the NASA portions of every Contractor-led spaceflight mission over which NASA has control (funds, launches, or manages)."

(f) Replace paragraph 2.1.2 with: "The Contractor shall include the applicable design requirements stated in NASA-STD 8719.14 or NSS 1740.14, in the program/ project requirements for any Contractor-led spaceflight mission being funded, launched, operated, or managed by NASA."

(g) Replace paragraph 2.1.7 with: "The Contractor shall include a review of the orbital debris requirements derived from this NPR and NSS 1740.14 or NASA-STD 8719.14, as applicable, as a part of the program/project System Requirements Review (or equivalent early review) for any Contractor-led spaceflight mission being funded, launched, operated, or managed by NASA."

(h) Replace paragraph 2.2.1.1 with: "The Contractor Program/Project Managers shall assess the mission for compliance with this NPR and NSS 1740.14 or NASA-STD 8719.14, for generation of orbital debris during all mission phases."

(i) Replace paragraph 2.2.1.2 with: "For any Contractor-led spaceflight mission being funded, launched, operated, or managed by NASA, the Contractor shall prepare and deliver the mission orbital debris assessments to the MDAA in an ODAR per the format and content defined in NSS 1740.14 or NASA-STD 8719.14."

(j) Replace paragraph 2.2.2.1 with: "Program/Project Managers shall assess the mission for compliance with this NPR and NSS 1740.14 or NASA-STD 8719.14, for proper disposal of the spacecraft for the portion of the program/project funded, managed, or operated by NASA."

(k) Replace paragraph 2.2.2.2 with: "For any Contractor-led spaceflight mission being funded, launched, operated, or managed by NASA, the Contractor shall prepare, update, and deliver an EOMP per the format and content defined in NSS

1740.14 or NASA-STD 8719.14, for the configuration of the space vehicles anticipated at EOM."

(l) Replace paragraph 3.1.2 with: "The Contractor shall track and monitor noncompliances (to NPR 8715.6A as tailored within the Contract, and NSS 1740.14 or NASA-STD-8719.14, as applicable) with the design and operations of the spacecraft and orbital launch vehicle stages beginning at PDR and shall have the tracking reviewed by the Contractor SMA organization prior to CDR and launch."

(m) Replace paragraph 3.1.3 with: "The Contractor shall ensure that all spacecraft and launch vehicles placed in orbit about the Earth or the Moon are designed to prevent/preclude, to the extent possible/feasible, a self-initiated unintentional on-orbit breakup from launch through reentry. Note: See the U.S. Space Policy Section 11 for direction to NASA on limiting orbital debris, NSS 1740.14, paragraph 4.4, or NASA-STD 8719.14, as applicable, for implementation of this requirement."

(n) Replace paragraph 3.3.1.5 with: "The systems defined in NPR 8715.6, paragraphs 3.3.1.5.a through d shall be analyzed when passivation is required (for further information on passivation, see NSS 1740.14 or NASA-STD 8719.14, as applicable): Note: NASA-STD 8719.14 and NHBK 8719.14 provide assistance with developing methods of passivation that are consistent with preventing premature passivation errors or malfunctions."

(ii) NASA-STD-8719.14, "Process for Limiting Orbital Debris (with Change 4)", dated September 14, 2009 is applicable.

(iii) NPR 8715.7, "Expendable Launch Vehicle Payload Safety Program", dated May 30, 2008, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 1.3.5 b and c, 1.3.6.c, 1.4.2, 1.4.3, 1.4.4, 1.4.5, 1.4.7 through 1.4.9, 1.5.2 , 1.5.3, 1.5.4.a through c, 1.5.6, 1.5.7, 2.3.1.c and d, 2.3.1.f, g, h, i, j, m, n, o, q, r, t, u; 2.3.2.a through g, 2.3.3.a, b, e, f, g, h; 2.3.4.a through p, 2.4.2 a, a.(1), a.(2), a.(3),a.(4), b, b.(1), b.(2), b.(3).(i), b.(3).(ii), b.(3).(iii), b.(4), b.(5), c, c.(1), c.(2), c.(3).(i), c.(3).(ii), c.(3).(iii), c.(4), d, e, e.(1), e.(2).(i), e.(2).(ii), e.(2).(iii), e.(3), e.(4), 2.4.3 a through c, 2.4.4, 2.5.1.a through c, 2.5.2.a through i, 2.5.3.a through p, 2.5.4.a.(1), a.(2), a.(3), a.(4), b, c, d.(1), d.(2), d.(3), d.(4), 2.5.5.a, b, c.(1), c.(2), c.(3), c.(4), c.(5), c.(6), 2.5.6.a through f, 2.5.7.a through h, 2.5.8.a through h, 2.5.9.a and b, 2.5.10.a and b, 2.6.1 through 2.6.4, 2.6.5.a and c, and 2.6.6.a through d are applicable.

(c) Replace paragraph 1.3.5.a with: "Establish the Center-level processes and associated requirements needed for each ELV payload project that uses the Center's resources."

(d) Replace paragraph 1.3.6.a with: “Ensure implementation of the applicable requirements for each ELV payload project that uses the Center’s resources.”

(e) Replace paragraph 1.3.6.b with: “Provide each payload project with safety engineering, safety analysis and other safety expertise needed to ensure the project successfully completes the safety review and approval process.”

(f) Replace paragraph 1.4.6 with: “The Payload Project Office shall ensure that the tailoring requirements document is completed and approved.”

(g) Replace paragraph 1.5.4 .d with: “Ensure appropriate signatures for approval, concurrence, and risk acceptance.”

(h) Replace paragraph 1.5.5 with: “The signatories of each waiver shall include the Payload Project Manager, responsible NASA Technical Authority(ies) (SMA, Engineering, and Health and Medical as applicable), and other authorities involved in the mission or having responsibility for issues addressed by the waiver.”

(i) Replace paragraph 2.3.1.a with: “Ensure that funding and other resources are allocated for payload projects to implement a System Safety Program and properly implements the applicable safety requirements and successfully completes the payload safety review and approval process.”

(j) Replace paragraph 2.3.1.b with: “Ensure that the project technical development, design, test, and review processes incorporate system safety engineering and the project’s Systems Safety Plan.”

(k) Replace paragraph 2.3.1.e with: “Coordinate with the local SMA organization to assign a Payload Organization Safety Engineer for the project.”

(l) Replace paragraph 2.3.1.k with: “Establish and implement any project-level processes and requirements needed to satisfy safety requirements and to ensure that the project fully participates in, and supports, the safety review and approval process activities.”

(m) Replace paragraph 2.3.1.l with: “Ensure that all requirements contained in the project’s tailored requirements document are implemented for its payload and associated GSE or that the project obtains an approval waiver for any requirement not satisfied.”

(n) Replace paragraph 2.3.1.p with: “Approve all safety review and approval process deliverables prior to submittal to the PSWG.”

(o) Replace paragraph 2.3.1.s with: “Ensure that the payload design process incorporates system safety engineering activities integral to identifying hazards, developing solutions to mitigate or eliminate the hazards, verifying the implementation of these solutions, and ensuring compliance with applicable requirements.”

(p) Replace paragraph 2.3.3.c with: “Review and provide comments to the project on all payload safety review deliverables and meeting minutes within 30 days after submittal.”

(q) Replace paragraph 2.3.3.d with: “Assess and concur (or obtain concurrence from their management as needed) on tailoring and any waiver to a safety requirement that is within their scope of responsibility.”

(iv) NPR 8715.3C, “NASA General Safety Program Requirements (w/ Change 7 dated 2/25/11)”, dated March 12, 2008, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 1.7.2.1.a through i, 1.7.2.2.a through c, 1.7.3.1.a through d, 3.15.7.1.a through h, 3.15.7.2, 3.15.7.3, 3.15.8.1.a and c, 6.1.3, 6.2.2.a, 6.2.2.b, 6.2.2.c, 6.2.2.e through g, 6.2.5.a, 6.3.3.1.a, 6.3.3.2, 6.3.4.1.a, 6.3.5.1.a, 6.3.5.1.b, 6.3.5.1.d through h, 6.3.6.1.a through j, 6.3.7.1.a through e, 6.3.8.1.a, 6.3.9.1.a, and 6.4.2.1.b are applicable.

(c) Replace paragraph 3.13.4.2 with: “Manned Space Flight Payloads. For payloads that will fly on, or interface with, a manned space launch vehicle, spacecraft, or entry vehicle controlled by NASA, Center Directors and program/project managers shall establish the processes and requirements to safeguard people and resources (including flight hardware and facilities) from hazards associated with payloads controlled by NASA and hazards associated with payload-related Ground Support Equipment (GSE) by eliminating the hazards or reducing the risk associated with the hazard to an acceptable level.”

(d) Replace paragraph 3.13.4.3 with: “Unmanned Suborbital Payloads. For a payload that will fly on an unmanned suborbital vehicle controlled by NASA (such as a sounding rocket, balloon, or experimental aeronautical vehicle), Center Directors and program/project managers shall establish the processes and requirements to safeguard people and resources (including flight hardware and facilities) from hazards associated with payloads controlled by NASA and hazards associated with payload-related Ground Support Equipment (GSE) by eliminating the hazards or reducing the risk associated with the hazard to an acceptable level.”

(e) Replace paragraph 3.13.4.4 with: “Return-to-Earth Payloads. For a payload that will be launched into space and will return to Earth for recovery or purposes other than disposal, Center Directors and program/project managers shall establish the processes and requirements for the recovery aspects of the mission to safeguard people and resources (including flight hardware and facilities) from hazards associated with payloads controlled by NASA and hazards associated with payload-related Ground Support Equipment (GSE) by eliminating the hazards or reducing the risk associated with the hazard to an acceptable level. Note: Disposal of space flight hardware is covered by the NASA Orbital Debris Program.”

(f) Replace paragraph 3.15.4.c with: “Laser operations during any open-air laser scenario conducted on DoD-controlled ranges or test facilities or by DoD personnel use the requirement in accordance with the site governing authority.”

(g) Replace paragraph 6.2.2.d with: “All space flight equipment (including medical and other experimental devices) that contain or use radioactive materials are identified and analyzed (per paragraph 6.3 of this NPR, as incorporated into this Contract) for radiological risk.”

(h) Replace paragraph 6.2.5.b with: “Coordinate with appropriate project office(s) to ensure radioactive material source reports that are submitted accurately reflect all known radioactive material sources intended for flight.”

(i) Replace paragraph 6.3.3.1.b with: “Submit the request to the NFSAM a minimum of 4 months prior to launch. Note: The request should be accompanied by the Radioactive Materials On-Board Report.”

(j) Replace paragraph 6.3.4.1.b with: “Submit the request to the NFSAM a minimum of 4 months prior to launch. Note: The request should be accompanied by the Radioactive Materials On-Board Report with a brief technical description of the radioactive material.”

(k) Replace paragraph 6.3.5.1.c with: “Ensure that the nuclear safety review contains a report.”

(l) Replace paragraph 6.3.8.1.b with: “Perform a safety analysis.”

(m) Replace paragraph 6.3.8.1.c with: “Meet the launch concurrence/approval requirements.”

(n) Replace paragraph 6.3.9.1.b with: “Perform a safety analysis.”

(o) Replace paragraph 6.3.9.1.c with: “Meet the launch concurrence/approval requirements.”

(p) Replace paragraph 6.4.2.1.a with: “Use the Radioactive Materials On-Board Report to report planned launches of radioactive materials and request for nuclear launch concurrence/approval.”

(v) NPR 8715.5A, “Range Flight Safety Program”, dated September 17, 2010, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Items (c) through (aa) below are applicable only when the Contractor is responsible for launching, flying, landing, and testing space and aeronautical vehicles (for example, re-entry missions).

(c) Paragraphs 1.3.3.2 b through e; 1.3.4 a through c, f, g, j; 1.3.6 b, e, f, g**,** g(1), g(2), g(3), j, k, l, m, n, o, p(1), p(2), p(3), p(4); 1.4.2 b**,** c; 1.4.3. 1.4.4, 1.4.5, 1.4.6, 1.4.7, 1.5.2, 1.5.3.1, 1.5.3.2, 1.5.4, 1.5.5, 1.6.2 a through d, 1.6.3, 1.6.4, 1.6.5 a through e, 1.6.6, 1.6.7,1.6.8, 3.2.1, 3.2.2, 3.2.3, 3.2.4.2, 3.2.4.3 a, b, d, e, f, g, h; 3.2.4.4, 3.2.4.5, 3.2.4.5 a(1)-(2), b, c(1)-(2); 3.2.5.1, 3.2.5.2, 3.2.5.3, 3.2.5.4, 3.2.5.5a through f, 3.2.5.6 a through h, and 3.2.5.7 a through b; 3.2.6.2 a through j; 3.2.6.3 a through h; 3.2.6.5, 3.2.7.1, 3.2.7.2. 3.2.7.3 a through f; 3.2.8.2, 3.2.8.2a. 3.2.8.2b(1) through (4), 3.2.8.3, 3.2.9.1, 3.2.9.2, 3.2.9.3, 3.2.10.1, 3.2.10.2, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.1.4 a through d, 3.3.3.2, 3.3.3.4, 3.3.4.1 a through b, 3.3.4.2, 3.3.5.1, 3.3.5.2, 3.3.5.3, 3.3.5.4, 3.3.6.1, 3.3.6.2, 3.3.6.3, 3.7.1.1, 3.7.1.2 b through f, 3.7.1.3, 3.7.2.1, 3.7.3.1, 3.7.3.2 a through d , 3.8.1a through d, 3.8.2 a through d are applicable.

(d) Replace paragraph 1.3.3.2a with: “Establish the processes and associated Center-level requirements needed to ensure the requirements of this NPR are satisfied.”

(e) Replace paragraph 1.3.3.2f with: “Approve each vehicle program’s range safety risk management process.”

(f) Replace paragraph 1.3.3.3 with: “When functioning as the safety authority for range operations, the Center Director or NASA designee shall designate a Center range safety organization.”

(g) Replace paragraph 1.3.4d with: “Ensure that personnel performing range safety functions have the qualifications and training appropriate to the types of vehicles and range operations.”

(h) Replace paragraph 1.3.4e with: “Ensure that operational performance requirements and standards for all range safety systems are satisfied.”

(i) Replace paragraph 1.3.4h with: “Evaluate tailoring and request for ELS determinations and Range Safety Waivers and coordinate these with the approval authorities.”

(j) Replace paragraph 1.3.4i with: “Evaluate each vehicle program’s range safety risk management process and coordinate this with approval authorities.”

(k) Replace paragraph 1.3.6a with: “Ensure the requirements of each range, launch site, or landing site that support the range operation are satisfied.”

(l) Replace paragraph 1.3.6c with: “Coordinate with all cognizant range safety organizations and Center/Program Range Safety Representative(s) to develop and implement operational range safety requirements, plans, procedures, and checklists, including mission rules and launch/flight commit criteria.”

(m) Replace paragraph 1.3.6d with: “Designate a Range Safety Representative for the vehicle program.”

(n) Replace paragraph 1.3.6h with: “Incorporate the applicable requirements in all contracts and agreements.”

(o) Replace paragraph 1.3.6i with: “Process tailoring, ELS determinations, and Range Safety Waivers in accordance with applicable paragraphs of 1.4, 1.5 and 1.6.”

(p) Replace paragraph 1.3.6p with: “Develop, document, and approve a range safety risk management process for vehicle program.”

(q) Replace paragraph 1.3.6q with: “Ensure that any vehicle program personnel who perform a range safety function are qualified and trained.”

(r) Replace paragraph 1.4.2a with: “Work with the cognizant Center range safety organization, Center Range Safety Representative, or the NASA Range Safety Manager and all other involved range safety authorities (such as Air Force) to identify and assess compliance with applicable requirements of this NPR and other applicable range safety requirements.”

(s) Replace paragraph 3.2.4.1 with: “A Center’s or vehicle program’s range safety risk management process shall include assessment of the risk to the public, workforce, and property.”

(t) Replace paragraph 3.2.4.3c with: “Perform and document the risk assessment.”

(u) Replace paragraph 3.2.6.1 with: “A range safety analysis shall assess any risk due to debris for input to the risk management process (Requirement). For a launch, these requirements apply to any debris that does not achieve orbital insertion. For an entry operation, these requirements apply to any debris that might be generated, intentionally or not, after the deorbit burn or sample return capsule release. Any orbital debris is subject to the requirements of NPR 8715.6A, NASA Procedural Requirements for Limiting Orbital Debris (with Change 1), dated May 14, 2009, as incorporated into this Contract.”

(v) Replace paragraph 3.2.6.4 with: “A range safety analysis shall establish launch/ flight commit criteria and operational constraints, such as hazard areas and impact limit lines, needed to control any risk due to debris impacts (Requirement).”

(w) Replace paragraph 3.2.8.1 with: “In the case of a catastrophic failure of a vehicle in flight, the fire, explosion, reactivity, and safety hazards of propulsion and power fluids (e.g., hydrazines, nitrogen tetroxide, solid rocket motors fuels, and their combustion or decomposition products) may be released. Under certain meteorological conditions, high concentrations of these materials may drift over populated areas at levels greater than emergency health standards permit. As a result, NASA shall protect the public and workforce from toxic hazards using either hazard containment or a risk mitigation approach (Requirement).”

(x) Replace paragraph 3.2.9.4 with: “Any residual risk due to any hazard not fully contained shall undergo the risk management process.”

(y) Replace paragraph 3.7.1.2a with: “Assurance that the collision avoidance requirements are satisfied for any launch or entry.”

(z) Replace paragraph 3.7.2.2 with: “The entry phase of a vehicle program’s risk management process, including the vehicle’s reliability to achieve controlled entry to the targeted landing site or debris footprint, shall be approved by the cognizant Center range safety organization or the NASA Range Safety Manager prior to launch (Requirement). Note: The intent is to provide assurance that the vehicle will be deorbited in a predictable manner that allows for appropriate risk management for the re-entry operation.”

(aa) Replace paragraph 3.8.3 with: “RSOs with real-time safety decision-making responsibility (including FTS command responsibility) shall meet the applicable safety certification requirements.”

(vi) NPD 8720.1C, “NASA Reliability and Maintainability (R&M) Program Policy”, dated April 18, 2008, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 5.c.(2) through (6), 5.d.(1) through (5), and 5.d.(7) through (11) are applicable.

(c) Replace paragraph 5.e.(1) with: “Ensure that failure history data is available for use as heritage data to support the formulation of R&M goals and requirements, quantitative and qualitative reliability analysis, and other R&M engineering activities as part of current, follow-on, or new programs and projects at the local Center.”

(d) The above-enumerated paragraphs are applicable only as follows: (a) post-launch maintainability design and operational requirements, including 5.d.(2) and 5.e.(1), are not applicable unless a spacecraft is required to be in operation maintainable, either robotically or by astronauts, and (b) reliability quantitative design and operational performance requirements are limited to those typically found in performance specifications and the mission assurance plans or are otherwise required to support PRA activities as negotiated. JPL does not impose failure rate, Mean-Time-Between-Failure (MTBF) or Probability of Success (Ps) quantitative requirements on its flight hardware or to validate compliance with a requirement.

(vii) NASA-STD-8739.8, “Software Assurance Standard with Change 1”, dated July 28, 2004, is incorporated into this Contract with the following understandings:

(a) Chapter 5 is not applicable.

(b) The Contractor’s established practices satisfy the requirements of Appendices A and B.

(viii) NPR 8705.5A, "Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects", dated June 07, 2010, is accepted for incorporation into this Contract with the following understanding:

(a) At the discretion of the Contractor, the implementation of these requirements may be documented in the Risk Management Plan, and referenced in the Safety and Mission Assurance Plan.

(b) Independent Peer Review (IPR) shall be the responsibility of the Center SMA Technical Authority (Section 5.2).

(ix) NPR 8705.6B, "Safety and Mission Assurance Audits, Reviews, and Assessments", dated May 24, 2011, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraph 3.2.3, 3.2.4.a, 3.2.4.d, 3.2.6.a and b, 3.2.6.d, 3.2.7.a through e, and 3.2.7.g are applicable.

(c) Replace paragraph 3.2.7 f with: "Participate in SMSR polling."

(x) NPD 8730.2C, "NASA Parts Policy", dated November 03, 2008, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 5.b (1), 5.f (1), 5.f (3), 5.f (4), and 5.f (6) are applicable.

(c) Replace paragraph 5.b (2) with: "Support program/project office implementation of this Contract's parts requirements."

(d) Replace paragraph 5.c (3) with: "Coordinate conformity assessment activities, including, but not limited to, the conduct of joint supplier audits and the sharing of conformity assessment information, with those of other NASA Centers, appropriate Government agencies, and the private sector to reduce unnecessary duplication."

(e) Replace paragraph 5.c (4) with: "Ensure that conformity assessment processes used by other Government agencies, third-party auditors, and the private sector, when utilized per paragraph 5.c. (3) above, provides satisfactory assurance of source capability and qualification."

(f) Replace paragraph 5.c (5) with: "Report nonconforming, defective, and/or suspected counterfeit parts to GIDEP Office in accordance with JPL's standard procedures, and for all cases involving counterfeit parts or other potential fraud, to the NASA Office of Inspector General and the NASA Acquisition Integrity Program (AIP)."

(g) Replace paragraph 5.d with: “NASA Center Engineering Offices, as assigned by the Center Director, shall support program/project offices in carrying out applicable requirements 5.f (1) through 5.f (6), as incorporated into this Contract.”

(h) Replace paragraph 5.f (2) with: “Select parts, materials, and packaging technology based on their intended use considering, but not limited to, performance, environment, criticality, and mission lifetime requirements”.

(i) Replace paragraph 5.f (5) with: “Mitigate risks associated with lead-free solder and surface finishes, in accordance with the Contractor’s established practices.”

(j) Replace paragraph 5.f (7) with: “The Contractor’s established practices satisfy the implementation of NASA-STD-6008 for control of fasteners. The Contractor will review the applicable chemistry, mechanical test, and processing reports received for each lot of bolts, screws, nuts, and inserts. If there are concerns associated with any of these items, additional testing shall be performed in accordance with the Contractor’s established practices.”

(xi) NPD 8730.5B, “NASA Quality Assurance Program Policy” NPD 8730.5B, “NASA Quality Assurance Program Policy (Revalidated 6/29/11)”, dated October 27, 2005, is incorporated into this Contract with the following understandings:

(a) Only the paragraphs below are applicable, with the limitations noted.

(b) Paragraphs 1.b (14), 5.c (1), are applicable as follows: when the references to Attachment A meet the following criteria: (a) Replace Attachment A, Item 1, with: “All work contracted by NASA shall be performed in accordance with this Contract” and; (b) Attachment A, Items 2.2.a, 2.a (1), 2.a (2), 2.b, 2.c, 2.d, 3, 3.a, 3.b, 3.c are not applicable.

(c) Replace paragraph 5.d (2) with: “Ensure program planning and acquisition documents incorporate applicable requirements, as determined by the Contractor, including specification of applicable quality system requirements.”

(xii) Workmanship Standards. The Contractor shall implement controls over workmanship processes including the selection and application of workmanship standards. The Contractor may select standards to be applied subject to the following condition. The Contractor shall obtain NASA’s approval to use alternates or equivalents to the following standards:

(a) NASA-STD-8739.1A, Workmanship Standard for Polymeric Application on Electronic Assemblies, dated March 4, 2008, with Change 2 dated March 29, 2011

(b) J-STD-001ES, Joint Industry Standard, Space Applications Electronic Hardware Addendum to J-STD-001 E Requirements for Soldered Electrical and Electronic Assemblies, dated December 2010 (Chapter 10 of IPC J-STD-001ES does not apply)

(c) NASA-STD-8739.4, Crimping, Interconnecting Cables, Harnesses, and Wiring, dated February 9, 1998, with Change 6, dated March 29, 2011

(d) NASA-STD-8739.5, Fiber Optic Terminations, Cable Assemblies, and Installation, dated February 9, 1998, with Change 2, dated March 29, 2011

(e) ANSI/ESD S.20.20, Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices), dated March 1, 2007

(xiii) The Contractor shall assess the requirements listed in section (B) above for applicability and describe within the list of exceptions how they will apply within the project. In the event the Contractor wants to deviate or use a substitute for any of the requirements contained above, the specific deviations or substitutions shall be documented, and waivers will be submitted to the Contracting Officer for any subsequent changes.

Additionally, the Contractor shall include in each Program/Project Plan a description of the risk management process as required by draft NPR 7120.5E dated January 31, 2012, NASA Space Flight Program and Project Management Requirements. The Project Plan containing such requirements will be referenced in the spaceflight project task order issued by the Contracting Officer and the Contractor shall comply with those requirements.

(C) To implement safety and mission assurance on this Contract, the Contractor shall establish discipline-specific subject matter experts that have sufficient expertise to prepare the Safety and Mission Assurance Plan and provide technical interchange with organizations that must interface with the spaceflight project. In implementing this requirement the Contractor shall:

(i) Designate a Range Safety Representative who shall coordinate the Contractor's range safety activities among the Contractor's organizations and with external organizations.

(ii) Designate a Probabilistic Risk Assessment (PRA) Point of Contact who shall coordinate JPL PRA and peer review activities related to spaceflight task orders**,** including review and concurrence on PRA plans**.**

(iii) Designate an Orbital Debris Representative who shall coordinate the Contractor's orbital debris activities among the Contractor's organizations and with external organizations.

(D) As a part of determining the scope of the safety and mission assurance for a project, the Contractor at a minimum shall:

(i) Recommend a risk classification level designation for the project in accordance with NPR 8705.4, Risk Classification for NASA Payloads (Revalidated July 9, 2008), dated June 14, 2004.

(ii) Recommend risk classification levels for lower levels of assembly, such as instruments, if different from mission classification levels.

(iii) Recommend a balanced development/acquisition approach for achieving the risk classification level recommended.

(iv) Consider and implement where appropriate any industry best practices related to Safety and Mission Assurance.

(E) On Contractor-led spaceflight mission task orders, the Contractor shall:

(i) Implement NASA-STD-8719.13B, "Software Safety Standard w/Change 1", dated July 8, 2004, with the following understandings:

(a) This standard applies to software created, acquired, or modified as Class A, B, and C as defined in Appendix E of NPR 7150.2A (Software Classifications). This standard also applies to Class D software to be used in space or to support operations of space assets. The standard applies to software created or acquired that poses a hazard or mitigates a hazard to humans, the environment, or external equipment. The standard also applies to software created or acquired that poses a hazard or mitigates a hazard to the flight system during development, integration, and testing.

(ii) Implement NPR 8000.4A, "Agency Risk Management Procedural Requirements", dated December 16, 2008, with the following understandings:

(a) This NPR applies to spaceflight programs/project, on a task order basis. The Contractor shall document how they intend to meet the requirements of NPR 8000.4A as part of the Project Implementation Plan or the Systems Engineering Management Plan.

(b) The Contractor will implement these requirements no later than one year from the effective date of this contract.

(iii) Identify and flow down requirements to successive levels of the supply chain.

(iv) Document and implement design and operational practices used to limit the generation of space debris during planned operations and anomalous events.

(v) Participate in the Government-Industry Data Exchange Program (GIDEP) Alert Program and the NASA Advisory Program.

(a) This participation shall be part of the implementation of the nonconforming product reporting requirements, pursuant to the terms of this contract.

(b) The Contractor reserves the discretion to require or request GIDEP reporting from subcontractors as the Contractor deems appropriate, and not subject to Contracting Officer approval.

(c) The Contractor shall designate an employee to represent JPL, excluding the NASA Management Office, as the GIDEP ALERT and NASA Advisory Coordinator. The person will serve as the primary focal point for JPL, excluding the NASA Management Office GIDEP ALERT and NASA Advisory activity and for coordination with the NASA GIDEP and NASA Advisory community.

(vi) The Contractor shall develop, document, and implement processes for:

(a) The exchange of significant problem and nonconforming data identified by the contractor with NASA Centers and with GIDEP. The Contractor shall conform with GIDEP processes and requirements for the release of GIDEP Alerts; if those criteria cannot be met the Contractor shall release the information via a NASA Advisory. Further the Contractor shall develop and implement process safeguards to preclude inadvertent release of GIDEP information to international partners and release of sensitive information in GIDEP Agency Action Notices or NASA Advisories.

(b) The evaluation and disposition of GIDEP ALERTS, GIDEP SAFE-ALERTS, GIDEP Problem Advisories, GIDEP Agency Action Notices, and NASA Advisories applicable to the Contractor's activities.

(vii) Establish and implement control of measurement processes to ensure the accuracy of measurement results affecting safety and mission success.

(viii) The Contractor shall establish and maintain traceability of measurement results by an unbroken chain of calibrations through the National Institute of Standards and Technology (NIST), or an institution recognized by NIST through international agreements, to the International System of Units (SI) when such units have been established.

(ix) The Contractor shall apply the processes to the functions and conditions identified in Attachment A to NPD 8730.1C (June 27, 2011) Metrology and Calibration.

(x) The Contractor shall control the accuracy, reliability, and use of Measuring and Test Equipment (M&TE) through the use of a calibration system compliant with the requirements of American National Standards Institute/National Conference of Standards Laboratories (ANSI/NCSL) Z540.3-2006 (August 3, 2006) Requirements for the Calibration of Measuring and Test Equipment as clarified in Attachment B to NPD 8730.1C (June 27, 2011) Metrology and Calibration, and incorporated into this Contract with the following understanding:

(a) Compliance with ANSI/NCSL Z540.3-2006 may be phased in over a period of time not to exceed 36 months from the effective date of this contract.

(b) Replace ANSI/NCSL Z540.3-2006, paragraphs 4.1.(c) with: "Customer requirements are met, in accordance with the Contractor's accepted practices."

(c) Replace ANSI/NCSL Z540.3-2006, paragraphs 5.4.1 with: "Measuring and test equipment (M&TE) requiring calibration shall be calibrated at periodic intervals

established and maintained to assure acceptable measurement uncertainty, traceability, and reliability.

The calibration interval process shall be free from conflicts of interest and systematically applied. The process shall be based on data resulting from the calibration of measuring and test equipment. The process shall also include stated measurement reliability or measurement uncertainty requirements and a method of verifying that the requirements are being attained. Calibration intervals shall be reviewed regularly and adjusted when necessary to assure continuous compliance of the specified measuring and test equipment performance requirements.

The Contractor's suppliers shall have a program to recall for calibration or verification, or remove from service, M&TE that has exceeded its calibration interval, has broken calibration seals, or is suspected to be malfunctioning because of mishandling, misuse, or unusual results. M&TE requiring calibration shall be calibrated or verified at periodic intervals established and maintained to assure acceptable reliability, where reliability is defined as the probability that M&TE will remain in-tolerance throughout the interval.

Intervals shall be established for all M&TE requiring calibration unless the equipment is regularly monitored through the use of check standards in a documented measurement assurance process. Check standards must closely represent the item parameters normally tested in the process and the check standard must be verified periodically. Where intervals are used to ensure reliability, the interval setting system must be systematically applied and shall have stated reliability goals and a method of verifying that the goals are being attained. Intervals may be based on usage or time since last calibration or verification. All exemptions from periodic calibration or verification shall be documented. The recall system may provide for the temporary extension of the calibration due date for limited periods of time under specified conditions that do not unreasonably impair the satisfaction of the customer's requirements."

H-7(2). SAFETY AND HEALTH

(A) This schedule provision supplements and implements NFS 1852.223-70 (April 2002), Safety and Health.

(B) General. The safety and health plan required to be submitted by the Contractor pursuant to F-5 shall implement the requirements of NFS 1852.223-70, "Safety and Health", dated April 2002, and the standards and specifications of paragraph (C) of this provision and shall describe the means to be employed by the Contractor to monitor and enforce said requirements. The plan shall include the Contractor's standards and criteria for imposing safety and health standards upon its subcontractors of any tier and its plans and procedures for monitoring compliance with such standards.

(C) Standards. The following safety and health standards, specifications, reporting requirements and provisions are prescribed pursuant to NFS 1852.223-70 (April 2002):

(i) General Standards and Specifications. The Contractor shall comply with applicable provisions of the Occupational Safety and Health Standards of the Occupational Safety and Health Act of 1970, Rules and Regulations of the Department of Labor issued pursuant thereto and applicable regulations of states provided for under the Act. The Contractor shall ensure that Contractor personnel are reasonably protected against occupational illness and injury on the job and on official travel overseas. The Government acknowledges the Contractor is required to comply with all applicable safety and health requirements established by the State of California.

(ii) The Contractor shall comply with all Federal, State, and local requirements applicable to motor vehicle safety.

(iii) The Contractor shall use MUTCD, Manual on Uniform Traffic Control Devices for Streets and Highways when establishing traffic control devices or marking roads for motor vehicle traffic on NASA property.

(iv) Reserved

(v) Nuclear Safety. Radioactive material will be handled in accordance with applicable Federal, State, and local regulations and requirements, to specifically include those of the State of California, Department of Energy and/or Nuclear Regulatory Commission. Launching of nuclear materials into space shall be done in accordance with National Security Council/Presidential Directive 25, as of May 8, 1996.

(vi) Fire Safety. The Contractor shall comply with all applicable Federal, State, and local requirements pertaining to Fire Protection and Life Safety. The Contractor shall implement a comprehensive fire safety program at the Jet Propulsion Laboratory in accordance with the specific requirements and procedures of NASA-STD-8719.11A, "NASA Safety Standard for Fire Protection", dated November 19, 2008. To effectively implement NASA-STD-8719.11A, the Contractor shall appoint in writing an Authority Having Jurisdiction for fire protection. Further the Contractor shall implement fire safety reviews for facility construction including review of contractual documents and facility design drawings.

(vii) Ammunition and Explosive Safety. The Contractor shall comply with all applicable Federal, State, and local requirements concerning ammunition and explosive safety. The requirements of NASA-STD-8719.12 Safety Standard for Explosives, Propellants, and Pyrotechnics, dated January 29, 2010 (Mod 6) shall be used to establish an ammunition and explosive safety program to be included in the safety and health plan to be submitted in accordance with paragraph (B) above. To effectively implement NASA-STD-8719.12, the Contractor shall appoint in writing an Explosive Safety Officer who shall manage the Contractor's Explosives, Propellants, and Pyrotechnic Safety Program and oversee the implementation of NASA-STD-8719.12 at JPL.

(viii) Facilities Safety. The Contractor shall establish a facilities safety program to assure that all new construction and facility modification activities do not impose unnecessary hazards to personnel and that such activities are reviewed for compliance with applicable building codes and fire and life safety requirements. As a part of this effort the Contractor as a minimum shall at least annually conduct facility inspections to ensure compliance with safety, fire protection, and building codes and standards. Additionally the Contractor shall ensure that occupational safety and health considerations such as ventilation, shower stalls, and eye wash stations are installed, maintained and remain accessible to users. Eye wash stations and shower equipment shall comply with ISEA Z358.1 2009, Emergency Eyewash and Shower Equipment. Facility design shall incorporate consideration for biohazards, toxic hazards, and as appropriate protection from and to physical samples returned from space.

(ix) Pressure Vessels and Pressurized Systems Safety.

(a) Ground-Based Pressure Vessels**:** The Contractor shall comply with all applicable Federal, State, and local requirements concerning ground-based pressure vessels and systems. The Contractor shall establish a ground-based pressure systems safety and recertification program to be included in the safety and health plan to be submitted in accordance with paragraph (B) above. To effectively implement the ground-based pressure systems safety program the Contractor shall appoint in writing a Ground Pressure Systems Manager who shall oversee the Contractor's ground-based pressure systems safety program (including NASA owned, Contractor owned, and transient items). The ground-based pressure systems safety program shall be in compliance with the following requirements:

(1) Establish and implement operating, maintenance, and inspection procedures to comply with requirements and work within established limits of the ground-based pressure vessels and systems (PVS).

(2) Design, acquire, fabricate, inspect, test, install, repair, alter, operate, and maintain all ground-based PVS items in accordance with the requirements of this contract and the design specifications.

(3) Ensure all ground-based PVS are certified in accordance with paragraph (5).

(4) Establish and implement procedures for the acquisition of ground-based PVS to include at a minimum establishment of requirements for the acquisition including application of national consensus standards and complete design review process.

(5) NASA-STD-8719.17A, "NASA Requirements for Ground-Based Pressure Vessels and Pressurized Systems (PVS)", dated November 6, 2009, with the following conditions:

It is understood that the requirements to certify all ground-based PVS prior to operation/use applies to newly acquired ground-based PVS and not to existing ground-based PVS. All ground-based PVS shall be evaluated for

safe operating condition by 30 September 2012. All ground-based PVS shall be certified (or a deviation or waiver shall be processed) by 01 October 2022. The Contractor shall provide a detailed certification plan, including the identification of safety milestones, to the Contracting Officer no later than 90 days after the effective date of the Contract.

(6) NPD 8710.5D, "Policy for Pressure Vessels and Pressurized Systems", dated March 12, 2008, is incorporated into this Contract with the following understandings:

a. Only the paragraphs below are applicable, with the limitations noted.

b. Paragraphs 1(h), 1(i), 1(j), and 1(k) are applicable

(b) Spaceflight Pressure Vessels. The Contractor's spaceflight pressure vessel systems shall be in compliance with the following requirements:

(1) NPD 8710.5D, "Policy for Pressure Vessels and Pressurized Systems", dated March 12, 2008, is incorporated into this Contract with the following understandings:

a. Only the paragraphs below are applicable, with the limitations noted.

b. Paragraph 1(c) with: "Qualify and accept spaceflight PVS, including qualification units, in accordance with ANSI/AIAA S-080, Space Systems Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, and ANSI/AIAA S-081, Space Systems Composite Over-wrapped Pressure Vessels (COPV), as incorporated into this Contract."

c. Paragraph 1(d) is applicable only if the Contractor is qualifying and accepting experiments containing PVS onboard atmospheric flight (nonspaceflight) in accordance with the Federal Aviation Administration regulations in Title 14 of the U.S. Code of Federal Regulations.

d. Paragraphs 1(f), 1(h), 1(i), 1(j), and 1(k) are applicable.

(2) ANSI/AIAA S-080-1998, "Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure Components", dated September 13, 1999, is incorporated into this Contract with the following understandings:

a. Sections 4.2.6 and 4.2.7 are applicable with the following provisions: that initial crack size be established by appropriate nondestructive evaluation (NDE) methods only. Proof test shall not be an acceptable method of establishing initial crack size.

b. Sections 5.1.1.1 and 4.4 are applicable with the following provisions: a life factor of four (4) be used for life analysis or test. Cycle tests shall be conducted for at least four (4) times the defined service life in sequence.

c. Section 4.4 is applicable with the following provisions: all regions of the pressure-containing wall including bosses and weld regions are shown to exhibit either leak-before-burst (LBB) or safe life. If LBB is used to demonstrate fracture control for the entire pressure vessel, the worst-case location (location having lowest propensity to leak rather than burst) shall be identified.

d. Section 5.1.1.7 shall not apply.

e. Figure 1 is applicable with the following provision: a burst factor of 2.5 or larger shall be demonstrated in Figure 1, approach B (DOT Title 49 vessel).

f. Table 1 shall exclude vessel #1.

(3) ANSI/AIAA S-081-2000, "Space Systems – Composite Overwrapped Pressure Vessels (COPVs)", dated December 19, 2000, is incorporated into this Contract with the following understandings:

a. Section 4.2.8 is applicable only as follows: The operating strain in the fiber shall be below 50 percent of the ultimate fiber strain at burst during ground pressurization, storage, integration, and flight operations. The Contractor's established practices for determination of fiber strain and strain ratio shall be followed

b. Section 4.2.11 is applicable with the following provision: applied stress level will be considered in evaluating potential for corrosion.

c. Section 5.1.3 is applicable with the following provision: during leak tests, the leak test chamber and dwell time at pressure will be validated with a calibrated leak source prior to pressure vessel testing.

d. Section 4.2 is applicable with the following provision: LBB or safe-life or a combination of these two approaches is acceptable for non-hazardous fluid applications

e. Table 1 is applicable with the following clarification: only strain cycles in excess of 0.25 at the strain value at maximum expected operating pressure (MEOP) or maximum design pressure (MDP) that occur after the initial flaw size is established with NDE shall be considered in the service life.

(x) Lifting Devices and Equipment Safety. The Contractor shall establish a lifting devices and equipment program for protecting persons and property during lifting operations. This program shall be described and included in the safety and health plan to be submitted in accordance with paragraph (B) above. JPL and Goldstone Deep Space Communications Complex (GDSCC) comply with the provisions of NASA-STD-8719.9, Standard for Lifting Devices and Equipment, dated May 9, 2002, with Change 1 dated

October 1, 2007 (Mod 6) with the exception of three specific paragraphs: (1) paragraph 4.2.6.b (5) Dual Holding Brakes; (2) paragraph k(2) Dual Upper Limit Switches; and (3) paragraph 4.2.7 f Control Stations: Positive Detent Buttons and Red Emergency Shop Buttons. JPL and GDSCC meet the intent of NASA-STD-8719.9 by implementing processes and procedures to mitigate risk and by providing substantial operating margins beyond the requirements of NASA-STD-8719.9. All critical lifting devices at JPL and GDSCC are fully Occupational Safety and Health Administration (OSHA) and California Occupational Safety and Health Administration (Cal/OSHA) compliant. New critical lift cranes will follow the NASA-STD-8719.9.

(xi) Electrical Systems Safety. The Contractor shall establish and implement an electrical systems safety program that establishes practices and procedures for the procurement, maintenance and operation of electrical systems and control of hazards associated with the systems. The Contractor shall ensure that electrical systems are designed in accordance with NFPA 70, National Electric Code, including Amendment 1 and Errata or as adopted by the California Electric Code (CEC), whichever is more stringent. The Contractor shall ensure that high voltage equipment (600+ volts) is protected to prevent unauthorized entrance including establishing grounded enclosures, locking access, establishing warning signage, and establishing and implementing protocols for access and work on the systems.

(xii) Hazardous Material Safety. The Contractor shall establish and implement processes for the procurement, storage, transport, use, and disposal of hazardous materials, including as a minimum: periodic inventory of the materials, contingency planning related to the materials, restrictions on procuring materials, and promulgation of hazardous material information to employees that use or may be in proximity to the material.

(xiii) Access to Equipment. The Contractor shall establish and implement processes to control access, especially unescorted access, to mission critical systems and areas.

(D) Illness, Incident, and Injury Experience Reports. The following illness, incident, and injury experience reports are prescribed pursuant to paragraph (d) of NFS 1852.223-70 (April 2002):

(i) Experience Reports. The Contractor shall prepare and submit to the Contracting Officer or his representative quarterly reports of occupational related illness, incidents, injury experience, worker's compensation costs; and government property damage due to mishaps or natural phenomena in such detail as prescribed in formats approved by the Contracting Officer or his representative.

(ii) Investigative Reports. The Contractor shall furnish reports of investigation of individual incidents or accidents or close calls in formats approved by the Contracting Officer or his representative, provided, however, that the Contractor shall not be required to furnish medical information, personal identifiers or any other private information concerning Contractor or subcontractor employees. The Contractor will identify type of body part and injury. Lessons learned from appropriate reports, excluding those related to close calls unless the Contractor believes material value

may be derived from such reporting, will be inputted into the NASA Lessons Learned Program.

(iii) Mishap Reporting. The contractor shall implement an effective mishap preparation, reporting and investigation program containing as a minimum the following:

(a) The Contractor shall within one hour of a mishap, report (and receive confirmation of the report) to the Contracting Officer, the NASA Management Office, and NASA Headquarters (Office of Safety and Mission Assurance who will concur in classification) when any Type A mishap, Type B mishap, or high visibility mishap or close call arises (or in the case of on-orbit anomalies within one hour of declaring a mishap) out of work performed under this contract or involving any area of NASA property. (Definitions of mishap types are contained within Section 1.2, "Description of NASA Mishaps and Close Calls" and Appendix A. "Terms and Definition" of NASA Procedural Requirements 8621.1B, NASA Procedural Requirement for Mishap and Close Call Reporting, Investigating, and Recordkeeping , dated May 23, 2006, with Change 5, dated March 15, 2010 and in the change table, dated March 11, 2010.) (Mod 6)

(b) Within 24 hours of a mishap or close call, the Contractor shall document that the incident occurred in the NASA Incident Reporting Information System. (The Contractor is not required to furnish medical information, personal identifiers or other private information concerning Contractor or subcontractor employees within the NASA Incident Reporting Information System.) The Contractor will identify type of body part and injury. NASA will establish appropriate access for the contractor to the NASA Incident Reporting Information System. The Contractor shall ensure that all material from the NASA Incident Reporting Information System, regardless of format, is kept secured when not in use. Unencrypted transmission of NASA Incident Reporting Information System data via e-mail is prohibited. NASA Centers will be permitted "read only" access to the Contractor's data in the NASA Incident Reporting Information System subject to the restrictions set forth in this Contract.

(c) The Contractor shall investigate all work-related mishaps and close calls arising out of work performed under this contract, to determine their proximate, intermediate and root causes. The parties recognize that where appropriate, an investigation may be undertaken at the direction of counsel and therefore subject to privilege**.** For NASA led investigations concurrence from the NASA Headquarters, Office of Safety and Mission Assurance and the Office of the Chief Engineer is required for the membership on Type A Mishaps, Type B Mishaps, and High Visibility Close Calls. NASA-led Types A, B investigations require formal appointment letters and shall be completed in accordance with these letters. NASA-led Types C, D, and close call investigations shall be completed with a target of 30 workdays or less. (Definitions of proximate, intermediate, and root cause are contained within Appendix A. "Terms and Definition" of NASA Procedural Requirements 8621.1B, NASA Procedural Requirement for Mishap and Close Call Reporting, Investigating, and Recordkeeping, dated May 23, 2006,

with Change 5, dated March 15, 2010 and in the change table, dated March 11, 2010.) (Mod 6) The Contractor shall establish and implement procedures for implementing investigation processes; including forming and implementing an Interim Response Team, consistent with the Contractor's established procedures which procedures will be available for review by NASA.

(d) When the Contractor's investigation lasts for more than 30 days, every 30 days the Contractor shall generate a status report of the investigation and place it in the NASA Incident Reporting Information System.

(e) Within 2 work days of completion of each Contractor-led investigation mishap or close call report, the Contractor shall upload a mishap report into the NASA Incident Reporting Information System using the formats identified for the system.

(f) Within 2 work days of documentation of a Corrective Action Plan(s) responding to a mishap investigation report, the Contractor shall upload the Corrective Action Plan(s) into the NASA Incident Reporting Information System using the formats identified for the system.

(g) Within 2 work days of completion of the mishap Corrective Action Plan(s), the Contractor shall upload the Corrective Action Plan(s) closure statement(s) into the NASA Incident Reporting Information System using the formats identified for the system.

(h) The Contractor shall cooperate with the Government safety mishap or close call investigation if conducted.

(E) The Contractor shall develop and implement a facility Mishap Preparedness and Contingency Plan within 30 work days of contract award.

(F) The Contractor shall develop and implement Flight Mishap Preparedness and Contingency Plans. These shall be delivered to NASA for review, comment, and approval. The Contractor will not provide a Mishap Preparedness and Contingency Plan for NASA-provided launch vehicles themselves but shall provide any interface information that NASA needs for inclusion in the NASA provide launch vehicles. These Mishap Preparedness and Contingency Plans shall include at a minimum the following:

(i) A description of the roles and responsibilities for Interim Response Team and Mishap Investigators, including discussion of coordination of rescue activities, hazard mitigation, site safing/securing, data collection.

(ii) A description of the training requirements required for personnel responding to, or investigating, mishaps and close calls and a description of the maintenance of the records related to the training.

(iii) A description of any special procedures for emergency response personnel that are not covered in the Contractor's emergency response plan (e.g., identification and handling of hazardous commodities specific to the facility or program/project).

(iv) A description of the procedures for impounding data, records, equipment, facilities, and property.

(v) A description or listing of existing agreements with national, state, local organizations or agencies that may be utilized during a mishap response or investigation.

(vi) A description of how debris (either on or off-site) is to be collected, transported, and stored.

(vii) A description of the investigation and debris collection process required for any mishap or close calls occurring in a foreign country.

(viii) A listing of the personnel who will assist in performing the procedures to impound data, records, equipment, facilities, and other property, depending on project.

(ix) Identification of the national, state, and local (and where applicable, international) organizations and agencies which are most likely to take part in debris collection; identifies the roles and responsibilities of each organization; and identifies a point of contact.

(x) Documents the responsibilities and procedures for mishap investigation in the bilateral or multilateral agreements when the flight program/project involves international partners, program managers, and project managers.

(xi) When applicable, describe the resources that may be needed from NASA or other government agencies (e.g., Federal Emergency Management Agency, National Transportation Safety Board, Department of Defense, Department of Justice) during a Type A mishap or Type B mishap investigation; identifies the point of contact and contact information for each of these agencies; describes the procedures to acquire their assistance; and identifies the potential roles and responsibilities of each agency.

(xii) Lists information such as databases, Web sites, documentation (including hardware history), drawings, basic system operation, and procedures and their associated points of contact for the information that may be scrutinized in a Type A mishap involving loss of a vehicle and/or major facility damage. Further, documents the processes and requirements to perform updates of the information.

(xiii) Documents the information technology plan to provide computer data retrieval and data archive support to the investigating authority.

(xiv) Documents the requisite security clearances, if any, for investigating authority members, chair, and ex officio participating in flight program/project investigations.

(xv) Documents the "chain of custody process" that will be used to secure and safeguard personal effects and sensitive information related to injured or deceased individuals.

(xvi) Identifies the key personnel both from the Contractor and from NASA to be notified for mishaps, particularly for Type A mishaps, Type B Mishaps, and high visibility close calls.

(xvii) Describes the steps to be taken in advance to ensure that assigned Interim Response Team and potential mishap investigation board members have authority and resources to expeditiously deploy to the mishap scene, effectively preserve mishap evidence, interview witnesses, and conduct an orderly investigation without administrative delay.

(xviii) Identifies the effective date of the plan and the required renewal/revision date for the plan.

(a) The Contractor shall create Flight Program/Project Mishap Preparedness and Contingency Plans during Phase B of the program and reviewed and updated on a yearly basis and prior to major test and launch events, as needed.

(G) Nothing herein shall be construed as diminishing the Contracting Officer's rights pursuant to F-5 paragraph (10) of this Contract.

H-8 ENVIRONMENTAL MATTERS

(a) Environmental Compliance. Environmental controls shall be in accordance with all applicable Federal, State and local regulatory requirements, and in accordance with other government policies as required in Article G-13 (NASA Issuance System and Government Policies).

(b) Environmental Compliance and Restoration (ECR) Program Provisions.

(1) General. This section pertains to ECR activities (e.g., environmental studies, designs, projects, etc.) included in the ECR Program. The ECR Program funding is part of the ECR budget. The Contractor, if requested to do so by the Contracting Officer, shall provide assistance to the Government concerning any matter arising under or relating to ECR activities. Accordingly the Contractor has entered or may enter into Agreements with local governments and other instrumentalities in order to assist the Government on certain ECR activities.

(2) Implementation of ECR Program Activities. ECR program activities shall conform to NPR 8590.1, NASA Environmental Compliance and Restoration (ECR) Program, dated June 14, 2007 with Change 1 dated June 2, 2010. For the Jet Propulsion Laboratory, the NASA Management Office (NMO) represents Headquarters as parent Center for satisfying the requirements of this NPR. As such, the NMO has the responsibilities of the Center Environmental Management Office.

(3) Environmental Project Support. NASA may require that certain environmental activities (studies, designs, and projects) be conducted by certain outside organizations or their contractors, including other Government agencies and other Centers. The Contractor shall provide access, facilities support, security, and other support services necessary for the outside organization to complete the environmental activity. The parties recognize that the Contractor is not responsible for the actions of any such outside organization doing business at the facility or at the facility and surrounding areas. In this regard, if third party claims are brought against the Contractor which are caused by or arise from the actions of such an outside organization doing business at the facility or at the facility and surrounding areas, those claims and any resulting liability there from to the extent attributable to such actions shall be deemed to "arise out of the performance of this contract" as that phrase is used in FAR 52.228-7—Insurance Liability to Third Persons, dated March 1996. This understanding, however, shall not alter any liability the Contractor would otherwise have as a Potentially Responsible Party under the Comprehensive Environmental Response, Compensation and Liability Act, 42 U.S.C. §9601.

(c) NASA Issuances Applicable to Environmental Matters. The provisions of the NASA Policy Directive (NPD) and NASA Procedural Requirements (NPR) documents below, shall be used for all work performed under this provision:

(1) NPD 8500.1B, 'NASA Environmental Management,' dated December 20, 2007, is incorporated with the following conditions:

(i) The functional reviews referenced throughout the NPD are those performed by NASA.

(ii) Information regarding environmental management activities, as referenced in Section 5, paragraph f.(6), and energy management activities will be reported to the Contractor's cognizant management official(s). These requirements are not to be construed to limit NASA's authority to request specific environmental or energy data or reports.

(2) NPR 8530.1A, 'Affirmative Procurement Program and Plan for Environmentally Preferable Products, dated June 4, 2004 (Revalidated April 3, 2009 with change 3) is incorporated into the Contract with the exception that the approval authority for waivers contemplated in the NPR is the Manager of the JPL Environmental Affairs Office.

(3) NPR 8580.1, 'Implementing the National Environmental Policy Act (NEPA) and Executive Order 12114', dated November 26, 2001. The Contractor recognizes that JPL is a Government-owned facility and the Government has certain responsibilities pursuant to NEPA for the conduct of all programs funded through the Contract. Therefore, the Contractor shall establish and maintain a procedure for assisting the Government with the Government's efforts to comply with NEPA on programs, missions, and facility operations funded through the Contract. It is recognized that the Government retains all responsibility for NEPA compliance for all Government programs, missions, operations

and tasks funded through the Contract and shall approve all documentation developed by the Contractor to assist the Government in accordance with this Article.

H-9 ENERGY MANAGEMENT

(a) Energy and Water Conservation. The Contractor shall comply with the energy reduction and water conservation goals set forth in this section. All Contractor operations shall support NASA's mission, as well as support NASA's need to meet federally mandated energy and water conservation requirements. The Contractor shall manage to the following goals:

(1) Appoint an Energy Manager to serve as the focal point for all energy matters and to manage and monitor energy consumption and conservation.

(2) Reduce Goal Subject building energy consumption per gross square foot relative to the FY 2003 baseline year by these specified percentages: 24% in FY 2013, 27% in FY 2014 and 30% in FY 2015. (Mod 6)

(3) Based on regulatory exclusion (goal exclusion) granted to NASA by DOE, Section H-9(a)(2) does not apply to Goldstone Deep Space Communication Complex (GDSCC) because energy needs of mission activities make it impractical for GDSCC to make energy reduction requirements per Article H-9, paragraph (a)(2). The following conditions apply:

(i) Conduct comprehensive evaluations per the National Energy Conservation Policy Act of 1978 (NECPA) and the Energy Independence And Security Act of 2007 (EISA) and implement cost-effective energy conservation measures identified in such evaluations within 180 days of audit completions to the extent that appropriated funds and/or alternative financing methods are available. (Mod 6)

(ii) Should regulatory exclusion granted to NASA be rescinded at a later date, Article H-9, paragraph (a)(2) shall apply to GDSCC 180 days from the rescission date unless otherwise provided in writing from the Contracting Officer.

(4) Increase the percentage of total electricity from renewable sources in accordance with the schedule of 5% (through FY 2012) and 7.5% (FY 2013 through the end of the Contract). Contractor shall meet renewable energy requirements through most cost effective methods such as:

(i) Purchase of Renewable Energy Credits

(ii) Self-Generated Renewable (SGR) energy

(iii) Purchase of renewable energy

(5) Reduce water consumption intensity (gallons per square foot) 2% annually through the end of the Contract from a FY 2007 baseline. Continue to pursue cost-effective water saving efficiencies, technologies, and methodologies.

(6) Prepare a 5-year Energy Efficiency and Water Conservation Plan and update on a maximum 3-year interval in accordance with DOE guidance. This plan shall detail the Contractor's strategy to ensure sustainable acquisition for energy and water-related products and services, and shall be submitted to the NMO Environmental and Facilities Manager for review and approval.

(7) Conduct comprehensive energy and water conservation evaluations of approximately 25% of facility gross square footage each year, such that all NASA-owned or leased facilities undergo evaluations on a recurring four-year cycle. Benchmark each metered building annually with a building energy use benchmarking system such as Portfolio Manager.

(8) To the extent that appropriated funds and alternative financing methods are available, begin implementing cost-effective energy and water conservation measures identified in facility evaluations within 180 days of audit completions.

(9) Implement awareness program (e.g., FEMP tools) to reduce waste in energy and water use by Federal and Contractor employees, which will include the NMO Environmental and Facilities Manager, consistent with Article F-5.

(10) Provide quarterly energy and water consumption reports, annual Office of Management and Budget Circular A-11 Energy and Transportation Efficiency Management budget exhibits, and an annual energy management progress assessment report through the NASA Environmental Tracking System (NETS).

(11) Minimize the life cycle cost of new and renovated facilities by utilizing sustainable design and construction methods. The Contractor is required to comply with either the current Federal Energy Efficiency Standards for design and construction (10 CFR 433) or the State of California Title 24 Building Energy Efficiency Standards, whichever is more stringent, for all facility design and construction work.

(12) Meter facility utilities and utilize consumption information in accordance with the requirements of NECPA, as modified by Energy Policy Act 2005 Section 103 and EISA Section 434(b).

(13) The Contractor shall submit to NASA on a semi-annual basis, a plan for the reinvestment of cost savings from realized energy and water conservation measures into additional energy conservation measures. This plan shall be deliverable to the NMO Environmental and Facilities Manager for review and approval.

(14) Development of Outdoor Environment Master Plan (OEMP). The Contractor shall, within 180 days of the effective date of this Contract, develop and submit to the NMO a draft Outdoor Environment Master Plan. The OEMP will include a baseline survey of the current outdoor environment including vegetation types and current irrigation and maintenance conduct. From this baseline, the OEMP will describe the vision for a 20-year planning period for the most appropriate outdoor environment.

(15) Should regulatory or statutory changes alter the externally imposed quantitative requirements of Article H-9(a)(2), (4), (5), and (7), those regulatory or statutory requirements shall immediately and automatically supersede the relevant quantities above.

(16) Ensure sustainable acquisition for energy- and water-related products and services as required in Article H-8(c)(3).

(17) For contract performance purposes, the metrics in Article H-9(a) will be considered on a "contract" basis, and not separately for Oak Grove and GDSCC; however, data will maintain the distinction between the two sites to support external reporting needs.

(b) Energy and Water Conservation Reports. The Contractor shall provide to NASA any reports required by Federal, State, and local regulation, Executive Orders, NPD's and NPR's within the timeframe established by the regulatory requirement or NASA.

H-10 OCCUPATIONAL HEALTH SERVICES

(a) The Contractor shall provide occupational health services of a scope that includes,

1. treatment of work-related injuries and illnesses;

2. medical examinations as specified in Occupational Safety and Health Administration (OSHA) standards;

3. other health examinations according to Contractor's established policies;

4. an employee assistance program for counseling regarding personal, work-related, mental health, and alcohol or substance dependency problems;

5. emergency medical assistance

(b) The Contractor will ensure that its operating policies and procedures for Occupational Health Services (OHS) and the Employee Assistance Program (EAP) are consistent with the intent of NASA Occupational Health Program Policy, but are adapted for the unique needs of the JPL.

(c) OHS policies and procedures will comply with applicable requirements of OSHA, American National Standards Institute and Nuclear Regulatory Commission. In the absence of a regulatory standard, OHS may utilize National Institute for Occupational Safety & Health Criteria Documents, Caltech/JPL policy or established occupational health best practices.

(d) In accordance with Article H-16, all medical records (both hard copy and electronic records) shall remain the property of Caltech and will be maintained in accordance with all applicable Federal, State and local laws.

Only redacted medical records (both hard copy and electronic) will be available for Agency medical quality control review.

(e) JPL OHS operating policies consist of the following:

1. Occupational Health Services Policies & Procedures Manual

2. JPL Medical Surveillance Manual

3. JPL Bloodborne Pathogens Manual

4. JPL AED Policy Manual

5. JPL Employee Assistance Program Guidelines and Procedures

Additionally, NPR 1800.1C, NASA Occupational Health Program Procedures dated October 6, 2009 with change 1 December 31, 2009 and NPD 1800.2C, NASA Occupational Health Program dated January 16, 2001, revalidated July 26, 2010, should be used as a best practice standard for services offered within the occupational health arena.

H-11 EXTERNAL COMMUNICATIONS AND VISITOR REQUESTS FROM ELECTED OFFICIALS AND THOSE KNOWN TO BE SEEKING ELECTED OFFICE

(a) General. The Contractor shall observe the policies and procedures agreed to by the Parties set forth in Attachment B hereto regarding the conduct of JPL's external communications programs, including public affairs programs, the release of information to the public relative to work performed under this Contract or matters relating to NASA programs, and communications with (i) Congress or other legislative bodies and (ii) elected officials and those seeking elected office.

(b) Consultation. The Contractor shall consult freely with the NASA Associate Administrator, Office of Communications and the NASA Associate Administrator, Office of Legislative and Intergovernmental Affairs, or the cognizant designees for guidance in applying these procedures.

(c) Visitor requests from elected officials. The Contractor shall coordinate visitor requests from elected officials and those seeking elected office to visit JPL or a JPL component facility (e.g., Table Mountain Facility; Goldstone Deep Space Communication Center) with the NMO Chief Counsel to assist NASA in complying the requirements of the U.S. Office of Special Counsel and the Hatch Act. The Contractor shall timely request the consent of the NMO Chief Counsel prior to granting a visit request from elected officials and those seeking elected office.

H-12 HANDLING, PROTECTION AND RELEASE OF RESTRICTED INFORMATION

1. Handling and Protection of Restricted Information

(a) Definition. “Restricted information,” as used in this clause, means recorded information, regardless of form or the media on which it may be recorded, the use and dissemination of which is restricted, and includes:

(1) Limited rights data;

(2) Restricted computer software;

(3) Information incidental to contract administration, such as financial, administrative, cost or pricing, or management information that embody trade secrets or are commercial or financial and confidential or privileged; and

(4) Information designated by the U.S. Government as Sensitive But Unclassified (SBU).

(b) Restrictions on use and disclosure of restricted information. With regard to any restricted information to which the Contractor is given access, by or on behalf of NASA, in performance of this contract that is either marked with a restrictive legend indicating that use and disclosure of the information is restricted or is specifically identified in this contract or in writing by the Contracting Officer as being subject to this clause, the Contractor agrees to:

(1) Use such restricted information only for the purposes of performing the services specified in this contract;

(2) Safeguard the restricted information from unauthorized use and disclosure;

(3) Allow access to the restricted information only to those employees and subcontractors that need it to perform services under this contract;

(4) Preclude access and disclosure of the restricted information to persons and entities outside of the Contractor’s or its subcontractor’s organization(s);

(5) Inform employees who may require access to the restricted information about obligations to use it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure;

(6) Require that each employee that has access to restricted information complies with the obligations regarding restricted information included in this clause; and

(7) Return or dispose of the restricted information, as NASA may direct, when the restricted information is no longer needed for performance of work under this contract.

(c) Exceptions

(1) The obligations and prohibitions of paragraph (b) do not apply to restricted information which the Contractor can demonstrate to the Contracting Officer—

(i) Was publicly available at the time of receipt by the Contractor or thereafter becomes publicly available without breach of this contract;

(ii) Was known to, in the possession of, or developed by or for the Contractor independently of the restricted information received from the Government and such knowledge, possession, or independent development can be shown;

(iii) Was received by the Contractor from a party other than the owner of the restricted information, who has the authority to release the restricted information and did not require the Contractor to hold it in confidence; or

(iv) Is released to or becomes available to a third party on an unrestricted basis from the owner of the restricted information, someone acting under the owner's control, or with the prior written approval of the owner.

(2) Under a valid order of a court or Government agency, the Contractor may release restricted information to which the Contractor is given access by or on behalf of NASA in performance of this contract, provided that the Contractor provides prior written notice to the owner of the restricted information of such obligation and the opportunity to oppose such disclosure. The Contractor shall provide a copy of the notice to the Contracting Officer.

(d) In the event that restricted information provided to the Contractor by or on behalf of NASA includes a restrictive legend that the Contractor deems to be ambiguous or unauthorized, the Contractor must notify the Contracting Officer of such condition. Notwithstanding such a notification, as long as the restrictive legend provides an indication that a restriction on use or disclosure was intended, the Contractor will treat the restricted information pursuant to the requirements of this clause unless otherwise directed in writing by the Contracting Officer or the owner of the restricted information.

(e) Other contractual restrictions on restricted information. This clause is subordinate to all other contract clauses or requirements that specifically address the access, use, handling, protection or disclosure of information. If any restrictions or authorizations in this clause are inconsistent with a requirement of any other clause of this contract, the requirement of the other clause shall take precedence over the requirement of this clause. Third party limited rights data and restricted computer software will be provided under this contract only as authorized by the clause at 52.227–14, Rights in Data—General, Alternates II and III (as modified by 1852.227–14, if applicable). If the Contractor believes there is a conflict between this clause and another clause in this contract regarding the access, use, handling, protection or disclosure of restricted information, the Contractor must consult with the Contracting Officer before taking subsequent actions under the other clause.

(f) The Contracting Officer may require the Contractor to demonstrate how it is complying with this Handling and Protection of Restricted Information clause.

(g) Remedies. Recognizing that this contract establishes a high standard of accountability and trust, the Contractor's breach of any of the conditions of this clause may provide grounds for the Government to pursue such remedies as may be permitted by law, regulation, or this contract.

2. Release of Restricted Information

(a) Definition. "Restricted information," as used in this clause, means recorded information, regardless of form or the media on which it may be recorded, the use and dissemination of which is restricted, and includes:

(1) Limited rights data;

(2) Restricted computer software;

(3) Information incidental to contract administration, such as financial, administrative, cost or pricing, or management information that embody trade secrets or are commercial or financial and confidential or privileged; and

(4) Information designated by the U.S. Government as Sensitive But Unclassified (SBU).

(b) In performance of NASA contracts, contractors, as well as their subcontractors and their individual employees, may require access to restricted information in the Government's possession. The Contractor agrees that, where needed for the performance of a NASA contract, NASA may release to its contractors, and their subcontractors, restricted information delivered during the course of this contract. Additionally, offerors agree that restricted information submitted with their proposals may be provided to NASA service contractors that assist NASA with contract closeout. If suitably marked with a legend indicating that use and disclosure of restricted information is restricted, such restricted information will be subject to the enumerated protections mandated by this clause. The Contractor's limited rights data and restricted computer software will be provided to other NASA contractors or subcontractors only as authorized by the clause at 52.227–14, Rights in Data-General, Alternates II and III (as modified by 1852–227–14, if applicable).

(c) For purposes of marking such restricted information, the Contractor may, in addition to any other notice or legend otherwise required (e.g., notices required under the clause at 52.227–14, Rights in Data—General, Alternates II and III), use a notice similar to the following:

Mark the title page with the following legend:

> This document was submitted by the California Institute of Technology in performance Contract No. NNN12AA01C. Submitter asserts that this document contains restricted information that embodies trade secrets or is commercial or financial and privileged or confidential. Such information shall not be disclosed outside of NASA except in accordance with NASA/Caltech Prime Contract No.

NNNAA1201C, clause H-12. This restriction does not limit the Government's right to use this restricted information if it is obtained from another source without restriction. The restricted information subject to this notice is contained in pages [insert page numbers or other identification of pages].

Mark each page containing restricted information the Contractor wishes to restrict with the following legend: This page contains restricted information and is subject to the restriction on the title page of this document.

(d) The Contracting Officer shall evaluate restricted information marked in accordance with paragraph (c) of this clause. Unless the Contracting Officer decides that reasonable grounds exist to challenge the markings, NASA and its contractors and subcontractors, shall comply with all of the safeguards contained in paragraph (2)(e) and paragraph 1 of this clause.

(e) To receive access to restricted information needed to assist NASA in accomplishing NASA mission activities and management and administrative functions, the Contractor or subcontractor must be operating under a contract that contains this clause, which obligates the Contractor or subcontractor, with respect to restricted information marked with a legend indicating that use and disclosure of the information is restricted, to do the following:

(1) Use such restricted information only for the purpose of performing the services specified in its contract;

(2) Safeguard such restricted information from unauthorized use and disclosure;

(3) Allow access to such restricted information only to those employees and subcontractors that need it to perform services under the contract;

(4) Preclude access and disclosure of such restricted information to persons and entities outside of the contractor's or its subcontractor's organization(s);

(5) Inform employees who may require access to such restricted information about obligations to use it only to perform the services specified in its contract and to safeguard it from unauthorized use and disclosure;

(6) Require that each employee that has access to restricted information complies with the obligations regarding restricted information included in this clause; and

(7) Return or dispose of such restricted information, as NASA may direct, when the restricted information is no longer needed for performance of work under the contract.

(f) Exceptions. The obligations and prohibitions of paragraph (e) of this clause do not apply to restricted information which the receiving contractor can demonstrate to the Contracting Officer -

(1) Was publicly available at the time of receipt by the receiving contractor or thereafter becomes publicly available without breach of the receiving contractor's contract;

(2) Was known to, in the possession of, or developed by or for the receiving contractor independently of the restricted information received from the Government and such knowledge, possession, or independent development can be shown;

(3) Was received by the receiving contractor from a party other than the owner of the restricted information, who has the authority to release the restricted information and did not require the receiving contractor to hold it in confidence;

(4) Is released to or becomes available to a third party on an unrestricted basis from the owner of the restricted information, someone acting under the owner's control, or with the prior written approval of the owner; or

(5) Is required to be released under a valid order of a court or Government agency, provided that the Contractor provides prior written notice to the owner of the restricted information of such obligation and the opportunity to oppose such disclosure.

(g) Contractor personnel requiring privileged access or limited privileged access to NASA information technology systems that contain restricted information and that are the primary responsibility of another contractor are subject to screening using the standard National Agency Check (NAC) forms appropriate to the level of risk for adverse impact to NASA missions. The Contracting Officer may allow the Contractor to conduct its own screening, provided the contractor employs substantially equivalent screening procedures.

(h) This clause does not affect NASA's responsibilities under the Freedom of Information Act.

3. Subcontracts. The Contractor shall insert, or require the insertion of subparagraphs 1 and 2 of this clause, including this paragraph (3), suitably modified to reflect the relationship of the parties, in all subcontracts (regardless of tier).

4. Evaluation of Proposals. Whenever the Contractor performs an evaluation of a proposal received from NASA incorporating restricted information, the Contractor agrees that JPL personnel involved in evaluating that proposal and having access to that restricted information shall abide by the obligations of this clause and the "Agreement and Conditions for Evaluation of Proposals" in Attachment G.

H-13 SUBCONTRACT NEW TECHNOLOGY AND PATENT FOLLOW-UP

(a) In accordance with procedures mutually agreed upon, the Contractor shall:

(1) General. Review the technical data submitted for all subcontracts, and the work delivered thereunder, which contain either the New Technology clause or other patent rights clause as

required by paragraph (h) of NFS 1852.227-70, New Technology (MAY 2002), or paragraph (k) of FAR 52.227-11, Patent Rights—Ownership by the Contractor (DEC 2007)(Alt IV)(JUN 1989). (Mod 6) Any "Reportable Items" of New Technology, or any "Subject Invention", as defined in paragraph (a) of NFS 1852.227-70 which are identified by the Contractor shall be noted and, if not reported by the subcontractor, the Contractor shall request the subcontractor to make the necessary reports.

(2) Subcontract Copies. Furnish to the Contracting Officer upon request a copy of a subcontract or subcontracts and a copy of all technical data submitted under such subcontract or subcontracts.

(3) Withholding of Payment. Where the "New Technology" clause is included in the subcontract, withhold final payment to the subcontractor pursuant to the withholding provisions of that clause until satisfied that the subcontractor has complied with the provisions of such clause, or, in the case of a disagreement as set forth in (b) below, the Contracting Officer has made a determination that the subcontractor has complied with the provisions of the New Technology clause and the Contractor has received authorization from the Contracting Officer for the release of such withheld funds.

(b) Subcontract Disagreements. In the event that there is a disagreement between the Contractor and a subcontractor as to whether any invention, discovery, improvement or innovation has been or should be reported, or whether such invention, discovery, improvement or innovation has been properly reported, the Contracting Officer upon notice shall thereupon assume responsibility for any further follow-up with the subcontractor as to such invention, discovery, improvement or innovation, and for determining compliance by the subcontractor with the New Technology or other patent rights clause.

H-14 PATENT AND NEW TECHNOLOGY SERVICES

The Contractor agrees:

(a) Patent Services. With respect to Patent Services:

(1) To utilize qualified patent personnel to prepare, at the request of the Contracting Officer, detailed technical descriptions in patent specification form on inventions made by the Contractor's employees and by subcontractors' employees in the performance of work under this Contract or subcontracts issued thereunder provided said subcontractors' employees' inventions have been reported to the Contracting Officer and said inventions were subject inventions at the time of request;

(2) To utilize qualified patent personnel to prepare, at the request of the Contracting Officer, responsive evaluations of Patent Office Examiners' actions taken on patent applications filed on inventions made by the Contractor's employees and by subcontractors' employees in the performance of work under this Contract provided such applications on said subcontractors' employees' inventions relate to inventions, title to which is vested in the Government;

(3) To assist NASA patent personnel in evaluation of Patent Office Examiners' actions taken on patent applications filed on inventions made by the Contractor's employees in the performance of work under this Contract;

(4) To assist in the evaluation of reportable items related to this Contract and subcontracts hereunder;

(5) To prepare invention award abstracts, at the request of the Contracting Officer, on those reportable items determined to be inventions and on which patent applications have been filed or prepared.

(b) New Technology Services. With respect to New Technology Services:

(1) To assist in the evaluation of reportable items relating to this Contract and subcontracts hereunder for possible publication in the NASA Tech Briefs magazine, *Spinoff* Magazine, and/or *Innovation* Magazine, publications and evaluation of potential uses for New Technology;

(2) To furnish available backup materials assembled in a Technical Support Package (TSP) on all reportable items which are made by Contractor or subcontractor employees as defined by NFS 1852.227-11 (MAY 2002) and FAR 52.227-11 (DEC 2007)(Alt IV)(JUN 1989) (Mod 6) in this Contract entitled "Patent Rights—Retention by the Contractor (Short Form)" and "Patent Rights—Ownership by the Contractor" respectively and which have been published as a Tech Brief;

(3) To furnish written replies to inquiries from NASA, other Government organizations, Government contractors and private individuals or industries, relating to reportable items incorporated in said Tech Briefs, Spinoff, and/or Innovation Magazine, utilizing only information in possession of the Contractor or made available to the Contractor by the Contracting Officer.

(4) Perform such other work and services as may be provided by a task order issued by the Contracting Officer.

H-15 NASA OFFICES

(a) The Contracting Officer may require the Contractor to assign adequate space and facilities for Government personnel resident at the JPL Oak Grove facility or a JPL-related facility (e.g., Goldstone Deep Space Communications Complex). The Contractor shall also provide office supplies and equipment, light, power, heat, communications, information technology support and such other support as may be required for the operation of such offices as directed by the Contracting Officer.

(b) In specific instances, the Contracting Officer may also require the Contractor to provide communication and information technology support for NASA personnel at remote sites in

the Southern California area other than the JPL Oak Grove facility and remote facilities related to JPL programs or operations.

H-16 PROPERTY RIGHTS IN RECORDS

(a) Government Records.

(1) Except as provided in (b) of this clause, all records acquired, generated or maintained by the Contractor in its performance of this Contract shall be the property of the Government and shall be delivered to the Government or otherwise disposed of by the Contractor either as the Contracting Officer or the NASA Records Officer may from time to time direct or, as the Contracting Officer shall direct upon completion or termination of the Contract. This sub-paragraph (a) shall not apply to documents owned by third parties that are in the possession of the Contractor (e.g., documents containing trade secrets of third parties).

(2) To the extent Government records are in the possession of the Contractor (e.g., Government-owned, Contractor-held), the Government shall have full and prompt access to the same. The Government's full and prompt access to data or records generated (or otherwise produced or prepared) at, by, or for JPL endure irrespective of form or medium of the data and apply to all such data or records without regard to the date or origination of such data or records, and without regard to ownership.

(3) Government records include, not only the deliverables specified by the Contract, including any Task Order (e.g., scientific and technical data, information, reports, or records), but all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by the Contractor in performance of this Contract. For purposes of this clause, Government records also includes any supporting or backup data used to create the deliverables, and related scientific, technical, health, safety, security, environmental, administrative, and management data or information.

(4) Government records include, but are not limited to, all environmental, occupational health, safety, and security records generated during the performance of Government funded activities at, by, or for JPL or for NASA related activities. Such records will be maintained at JPL and are the property of the Government.

(5) The Government shall have unlimited rights in information incidental to Contract administration including administrative and management information created under the Contract by the Contractor and specified for delivery to NASA in performance of the Contract, expressly excluding Confidential Contractor financial information. The Government shall also have the right to release such administrative and management information to any third party to satisfy the Government's requirements.

(b) Contractor Records. Not all records at JPL are Government records; NASA recognizes the right of the Contractor to retain ownership to certain records.

(1) Contractor-owned records include:

(i) Personal notes, logs, memoranda, or other similar documents created by an employee of the Contractor for the employee's own personal convenience and which are not intended for distribution through the normal course of the Contractor's business; and legal records, including legal opinions, litigation files, and documents covered by the attorney-client (i.e., facts confidentially communicated to an attorney from a client for the purpose of seeking legal assistance and opinions given by an attorney based on those facts) and documents covered by the attorney work product privileges;

(ii) Employment-related records containing personally identifying information concerning employees (e.g., personnel, payroll, and medical records maintained on individual employees of the Contractor);

(iii) Employment-related records not containing personally identifying information concerning employees;

(iv) Confidential Contractor financial information, and correspondence between the Contractor and other segments of the Contractor located away from the NASA facility (i.e., the Contractor's corporate headquarters); and

(v) Contractor Procurement-related records (confidential financial information and correspondence obtained by the Contractor for use in its subcontracts; source selection and other confidential, pre-decisional, or similar documents relating to the Contractor's deliberative process in selecting subcontractors).

(vi) Pre-decisional documents that are a direct part of the Contractor's deliberative process in that they make recommendations or express opinions on matters of policy directly affecting the Contractor's business operations.

(2) In accordance with the Privacy Act of 1974, 5 U.S.C. 552a (P.L. 93-579) and implementing NASA Regulations (14 CFR 1212, Privacy Act - NASA Regulations), the Contractor shall, upon written direction from the Contracting Officer, maintain one or more separate "Systems of Records" on individuals in order to accomplish the NASA functions and in that case FAR 52.224-1, Privacy Act Notification (APR 1984) and FAR 52.224-2, Privacy Act (APR 1984) shall become applicable.

(c) Rights in Data. Ownership of documents by either the Government or the Contractor shall not in any way affect the respective rights the parties may otherwise have to data contained on or in the documents under other provisions in the Contract.

(d) Contract Completion or Termination.

(1) In the event of completion or termination of this Contract, the Contractor agrees to leave Government-owned data at the JPL, and upon request of the Government, the Contractor agrees to deliver such Government-owned data to NASA or its designees, including successor contractors.

(2) In the event of completion or termination of this Contract, copies of any of the Contractor-owned records identified in paragraph (b)(1)(iii), and (v) of this clause, and with the consent of the employees, (b)(1)(i) and (ii), upon the request of the Government, shall be delivered to NASA or its designees, including successor Contractors. Upon delivery, title to such records shall vest in NASA or its designees, and such records shall be protected in accordance with applicable federal laws (including the Privacy Act), as appropriate.

(e) Inspection, Copying, and Audit of Records.

(1) All records acquired or generated by the Contractor under this Contract in the possession of the Contractor, except those described at paragraph (b)(1)(i), (ii) and (vi) of this clause, shall be subject to inspection, copying, and audit by the Government or its designees at all reasonable times, and the Contractor shall afford the Government or its designees reasonable facilities for such inspection, copying, and audit; provided, however, that upon request by the Contracting Officer, the Contractor shall deliver such records to a location specified by the Contracting Officer for inspection, copying, and audit.

(2) Contractor Records described in paragraph (b)(1)(ii) of this clause shall be subject to (e)(1) of this clause, but subject to the following conditions:

(i) With regard to personally identifying information that can be redacted from the record, the Contractor shall provide the Government access to the record as expeditiously as possible.

(ii) The Contractor acknowledges that the Government may, for purposes of health, medical, safety, security, or law enforcement, need access to records containing information identifiable to individual employees of the Contractor. With regard to these records, the Contractor shall provide the Government access to the record in accordance with applicable law, legal process, or subpoena. The Government shall use such records in accordance with applicable federal laws (including the Privacy Act), as appropriate.

(iii) The parties agree that it is in their mutual interest for the Contractor to conduct self-assessments that are kept confidential to the Contractor. The Contractor agrees that it will notify NMO of any self-assessments that are initiated and will promptly brief NMO on actions intended to be taken as a result of such self-assessments. Upon completion, the Contractor will report and certify which actions were taken. It is the intent of the Government and the Contractor, however, that any record documenting the self-assessment be strictly confidential and not be available to the Government or any third party without the express consent of the Contractor.

In those instances where a basis for asserting a joint defense privilege exist, the Contractor will provide attorney/client privileged or work product information to counsel for NASA pursuant to a joint defense agreement.

(3) Without limiting the generality of the foregoing, the Contractor may use, make, or retain copies of Government records to the extent necessary to perform work generally described in Section C of this Contract.

(f) Records Retention and Storage.

(1) Government Owned, Contractor-held records shall be maintained by the Contractor in accordance with NPD 1440.6H, NASA Records Management, dated March 24, 2008, and NPR 1441.1D, NASA Records Retention Schedules, dated February 24, 2003 with change 5, June 26, 2009.

(2) The Contractor shall ensure that Contractor-owned records can be segregated from Government-owned, Contractor-held records.

(3) The NASA Record Retention Schedules (i.e., NPR 1441.1D with change 5, June 26, 2009 are applicable for the classes of records described therein for Government records. The Contractor shall provide container lists for all storage boxes containing such records in accordance with at least the secondary identification codes (e.g., 1150) for files falling within the 1000 series and primary identification codes (e.g., 2100) for files falling within the 2000 through 9000 series as set forth in the NASA Record Retention Schedules when files are sent to Record Storage. The Contractor will implement NPR 1441.1D with change 5, June 26, 2009 for records disposition.

(4) Any such documents delivered to and stored by the Government may, during their period of storage, be made available to the Contractor for inspection, copying and use, upon its request. The Contractor shall submit requests for such documents stored by the Government through the Contracting Officer for processing.

(5) Contractor shall provide NASA personnel full access to the JPL Archives.

(6) Upon request, the Contractor shall submit to the Contracting Officer the latest inventory of the catalogued records in the JPL archives and to the NASA Records Officer statistics and reports concerning records under the Contractor's control as requested by the NASA Records Officer of all NASA Installation records managers.

H-17 SERVICE CONTRACTS

The Contractor agrees, except to the extent that such subcontracts are exempted by the regulations of the Secretary of Labor or FAR 52.244-6, Subcontracts for Commercial Items (DEC 2010), to insert the following clause with such changes as are necessary to appropriately identify the parties in all subcontracts as applicable: FAR 52.222-41 Service Contract Act of 1965 (NOV 2007).

H-18 LIMITATION OF LIABILITY

The provisions of FAR 52.246-24 (FEB 1997), Limitation of Liability—High Value Items, shall apply to all items delivered to the Government under this Contract, which have a unit cost

exceeding $100,000. The provisions of FAR 52.246-23 (FEB 1997) Limitation of Liability, shall apply to all other items delivered to the Government under this Contract.

H-19 SUPPORT FOR HISTORICALLY BLACK COLLEGES AND OTHER MINORITY UNIVERSITIES

As part of its program of supporting research, the Contractor shall develop relationships and involvement with Historically Black Colleges and Universities, and other Minority Universities.

H-20 CONSTRUCTION CLAUSES

The following clauses, suitably modified to identify the parties, shall be included by the Contractor in subcontracts for construction as prescribed in FAR Part 22 for work within the United States. The Contractor shall also require the insertion of said clauses in all lower tier subcontracts for construction that fall within the FAR Part 22 prescriptions. Such clauses are:

	FAR Reference No.	Title
(a)	52.222-6	Davis-Bacon Act (JUL 2005)
(b)	52.222-7	Withholding of Funds (FEB 1988)
(c)	52.222-8	Payrolls and Basic Records (JUN 2010)
(d)	52.222-9	Apprentices and Trainees (JUL 2005)
(e)	52.222-10	Compliance with Copeland Act Requirements (FEB 1988)
(f)	52.222-11	Subcontracts (Labor Standards) (JUL 2005)
(g)	52.222-12	Contract Termination--Debarment (FEB 1988)
(h)	52.222-13	Compliance with Davis-Bacon and Related Act Regulations (FEB 1988)
(i)	52.222-14	Disputes Concerning Labor Standards (FEB 1988)
(j)	52.222-15	Certification of Eligibility (FEB 1988)
(k)	52.222-16	Approval of Wage Rates (FEB 1988)
(l)	52.222-27	Affirmative Action Compliance Requirements for Construction (FEB 1999)

H-21 AUDIT NEGOTIATION—ACCESS TO COMPUTERS

In applying the provisions of FAR 52.215-2, Audit and Records—Negotiation (OCT 2010) (ALT I)(MAR 2009)(ALT II)(APR 1998) it is understood and agreed that this clause with regard to computer access, pertains primarily to access to information that is stored on computers used at JPL rather than access to the computers themselves. When the Contractor is required to provide information pursuant to the requirements of this clause which is on computers used by

JPL personnel it shall therefore be provided in any media or form normally used by the Contractor and which can be utilized by the auditors on their computers. At their option, Government auditors may be present when the Contractor extracts, compiles or otherwise processes information or test transactions on or from computers used by JPL personnel for the purpose of providing information to Government auditors. Government auditors will also be provided, at their option, access to physically inspect and inventory computer systems, equipment, and software used at JPL. This clause is applicable to all computers used at JPL, regardless of who owns the computers.

H-22 COMPETITION IN SUBCONTRACTING

In applying FAR 52.244-5, Competition in Subcontracting (DEC 1996), subcontracts are to be awarded on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the Contract. The Contractor shall send the Contracting Officer an informational copy of all noncompetitive source board waivers exceeding $5,000,000 promptly upon issuance. The Contracting Officer shall advise the Contractor of any waiver concerns within five working days unless extended. Upon noncompetitive source board evaluation and selection of a procurement that exceeds $10,000,000, the Contractor shall forward the selection memorandum to the Contracting Officer for concurrence.

H-23 APPLICATION OF CROSS-WAIVERS OF LIABILITY

In applying the NFS Clauses 1852.228-72 (SEP 1993), 1852.228-76 (DEC 1994), and 1852.228-78 (SEP 1993), the Contractor shall incorporate the appropriate clause into subcontracts, which are for $100,000 or more when the work to be performed is in support of “Protected Space Operations” as defined in paragraph (b)(5) of each clause.

H-24 ADVISORY AND ASSISTANCE SERVICES

(a) In accordance with the policies set forth in FAR Part 37.203, this Contract may be used to obtain advisory and assistance services, subject to the restrictions set forth in (b) below.

(b) As noted in FAR 37.203(c), advisory and assistance services shall not be:

(1) Used in performing work of a policy, decision-making, or managerial nature that is the direct responsibility of agency officials.

(2) Used to bypass or undermine personnel ceilings, pay limitations, or competitive employment procedures;

(3) Contracted for on a preferential basis to former Government employees;

(4) Used under any circumstances specifically to aid in influencing or enacting legislation; or

(5) Used to obtain professional or technical advice that is readily available within the agency or another Federal agency.

H-25 SUBCONTRACTOR PROGRESS PAYMENTS

In making progress payments to subcontractors and suppliers on fixed price subcontracts, the Contractor shall use the policies, standards, and procedures of Subpart 32.2 and 32.5 of the FAR and Subparts 1832.2 and 1832.5 of the NASA FAR Supplement (NFS) as guidelines.

H-26 ADDITIONAL NASA REQUIREMENTS

(a) The following government policies are incorporated herein. In performing work under this Contract, the Contractor shall comply with the requirements of these government policies, or parts thereof. Additions, modifications, or deletions of specific requirements shall be in accordance with Article G-13 (NASA Issuance System and Government Policies) of this Contract.

(1) NPD 8020.7G - Biological Contamination Control for Outbound and Inbound Planetary Spacecraft, dated February 19, 1999 revalidated November 25, 2008

(2) NPR 4310.1 - Identification and Disposition of NASA Artifacts, dated March 16, 1999 revalidated with change 2, January 31, 2006).

(3) NPD 2110.1F, Foreign Access to NASA Technology Transfer Materials, dated November 20, 2008

(4) NPD 2570.5E, NASA Electromagnetic Spectrum Management, dated July 11, 2011

(5) NPR 2570.1B, NASA Radio Frequency (RF) Spectrum Management Manual dated December 5, 2008

(6) NPD 8010.3B, Notification of Intent to Decommission or Terminate Operating Space Systems and Terminate Missions, dated June 14, 2004 revalidated April 30, 2009

(7) NPR 8020.12D, Planetary Protection Provisions for Robotic Extraterrestrial Missions, dated April 20, 2011 is incorporated into this Contract with the understanding that paragraph 5.3.1 is replaced with: “5.3.1 PP Category III and IV missions to Mars shall comply with all applicable requirements.”

(8) NPD 8900.4D, NASA Use of Global Positioning System Precise Positioning Service, dated April 27, 1999, revalidated June 15, 2009, is incorporated into this Contract with the understanding that it is applicable to efforts funded by NASA sponsors only. The Contractor will provide notification on GPS PPS receiver location and use to NASA’s Associate Administrator for Human Exploration Operations Mission Directorate (HEOMD) if requested per DoD-NASA interagency agreement.

(9) NPD 1000.5A, Policy for NASA Acquisition, dated January 15, 2009 revalidated March 17, 2010.

(10) NPD 1460.1, Agency Mail Management Program, dated October 8, 2010

(11) NPD 8610.7D, Launch Services Risk Mitigation Policy for NASA-Owned and/or NASA-Sponsored Payloads/Missions, dated January 31, 2008

(12) NPD 8610.12G, Space Operations Mission Directorate (SOMD) Space Transportation Services for NASA and NASA-Sponsored Payloads, dated February 23, 2005 revalidated April 13, 2010

(13) NPD 8610.23C, Launch Vehicle Technical Oversight Policy, dated August 18, 2006

(14) NPD 8610.24C, Launch Services Program Pre-Launch Readiness Reviews, dated May 12, 2005 revalidated May 12, 2010

(15) NPD 8074.1, Management and Utilization of NASA's Space Communication and Navigation Infrastructure, dated August 11, 2009

(16) The Contractor will implement NPD 8610.6G, Graphic Markings on Space Transportation Vehicles, U.S. Components of the International Space Station Component Systems, and Payloads, dated October 30, 2003 revalidated June 15, 2009 , when using graphic markings on any payload.

(17) NPR 2841.1, Identity, Credential and Access Management Services, dated January 6, 2011, is incorporated into this Contract with the understanding that it is applicable to situations where JPL uses NASA's IT systems/facilities.

H-27 CLAUSE FLOWDOWN REQUIREMENT

(a) Although the following contract clauses are not applicable to the Contractor, the Contractor shall incorporate these clauses, when appropriate and as suitably modified to identify the parties, into its subcontracts. This provision only applies to new subcontracts the Contractor enters into after the Contracting Officer's approval of standard subcontract terms and conditions in accordance with (c) below. Additionally, this provision will not apply to any subcontract when the solicitation for the subcontract was issued prior to the Contracting Officer's approval of the standard terms and conditions in accordance with subparagraphs (b) and (c). This paragraph (a) does not apply to subcontracts for commercial items as defined in FAR Section 2.101.

(1)	FAR 52.215-15	Pension Adjustments and Asset Reversions (OCT 2010)
(2)	FAR 52.215-17	Waiver of Facilities Capital Cost of Money (OCT 1997) (where a subcontract does not include Cost of Money as a proposed cost)
(3)	FAR 52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other than Pensions (JUL 2005)
(4)	FAR 52.227-21	Technical Data Declaration, Revision and Withholding of Payment—Major Systems (DEC 2007), in all subcontracts for a "major system" as that term is defined in 41 U.S.C.A. 403.

(5) FAR 52.229-8 Taxes—Foreign Cost-Reimbursement Contracts (MAR 1990)

(6) FAR 52.249-14 Excusable Delays (APR 1984)

(7) NFS 1852.227-85 Invention Reporting and Rights—Foreign (APR 1986)

(b) The flowdown requirements of FAR 52.244-6, Subcontracts for Commercial Items (DEC 2010) shall apply to commercial subcontracts. In addition, the Contractor shall insert the following clause in all subcontracts for commercial items which are funded under the American Recovery and Reinvestment Act (Recovery Act): FAR 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010)

(c) Additionally, Sections H and I of this Contract may contain other contract flowdown requirements that are not included in the Contractor's previously approved standard subcontract terms and conditions. In accordance with paragraph (d) below, the Contractor shall update its standard subcontract terms and conditions to reflect these changes. The Contractor shall continue to use its previously approved subcontract terms and conditions until the Contractor's new subcontract term and conditions containing the contract flowdown requirements are approved by the Contracting Officer. Additionally, the previously approved subcontract terms and conditions will apply to all solicitations for subcontracts issued prior to the Contracting Officer's approval of the new standard subcontract terms and conditions.

(d) The Contractor shall submit, within 90 days after the effective date of this Contract, or modifications thereto that change the subcontract flowdown requirements of this Contract, its revised standard terms and conditions incorporating the changes required by paragraphs (a), (b), and (c) above for Contracting Officer approval. Once approved by the Contracting Officer, the Contractor shall incorporate the above provisions in its subcontracts consistent with the approved standard terms and conditions.

H-28 PRINTING, DUPLICATING, AND COPYING

(a) The terms "documentation" referred to in paragraph (a), "printing" referred to in paragraph (b), and "production units" referred to in paragraph (c) of NFS 1852.208-81, Restrictions on Printing and Duplicating (NOV 2004) (Mod 6), pertain solely to "Government publications". "Government publications" is defined as (1) reports intended primarily for internal use by the Government and (2) reports or other materials of the type that the Government itself distributes to the public under an agency program. "Government publications" shall, unless subject to exemption under applicable regulations, be printed according to the requirements of 48 CFR Subpart 8.8 even though the distribution of these reports and materials may be effectuated by the Contractor for the Government.

(b) Examples of documents which are "Government publications" include, but are not limited to:

(1) publications released by the Contractor or a subcontractor to the public for the purpose of promoting NASA or a Government agency sponsor;

(2) deliverable final reports but not interim drafts of such reports;

(3) deliverable review board presentations and conclusions in which a majority of the review board membership consists of Government representatives.

(c) Examples of documents that are not "Government publications" include, but are not limited to:

(1) publications for internal JPL usage and communication such as the JPL Telephone Directory and the Universe newspaper;

(2) public information, education and public service documents, and award certificates printed for JPL rather than Government usage, including those which may contain an incidental reference to sponsorship by NASA or another Government agency;

(3) publications for which the printing costs are not paid for by the Government;

(4) non-deliverable reports provided to the Government for informational purposes which are suitable for publication in academic, technical or professional journals and similar publications; and

(5) review board presentations and conclusions in which a majority of the formal review board membership consists of Contractor or subcontractor representatives, where Government attendance is only incidental, and the contract does not expressly require Government approval of the proceedings.

(d) Requests for waivers to permit printing of "Government publications" other than via the process defined in 48 CFR Subpart 8.8 in cases of exigencies or other appropriate circumstances shall be submitted by the JPL Installation Printing Management Officer to the NASA Printing Management Officer through the Contracting Officer.

(e) The Contractor will implement NPD 1490.1H, NASA Printing, Duplicating, and Copying Management, dated September 17, 2010.

H-29 CLAUSES APPLICABLE ON A TASK ORDER BASIS

The parties agree that certain contract clauses do not apply to the entire contract and, instead, apply to the extent that they are required by sponsors on specified task orders. The following is an enumeration of these clauses and the guidelines for their applicability:

(a) FAR 52.247-68, Report of Shipment (RESHIP)(FEB 2006) shall be included in task orders which involve shipments of classified material; protected sensitive, and protected controlled material; explosives and poisons: class 1, division 1.1, 1.2 and 1.3; class 2, division 2.3 and class 6, division 6.1; or when a truckload/carload shipment of supplies weighing 20,000 pounds or more, or a shipment that occupies the full visible capacity of a railway car or motor vehicle are required for the task; or radioactive materials requiring the use of a III bar label;

(b) FAR 52.223-3, Hazardous Materials Identification and Material Safety Data, (JAN 1997) (ALT I)(JUL 1995) shall be included in task orders which include an identified list of hazardous materials for delivery.

(c) NFS 1852.234-2, Earned Value Management System (NOV 2006)(ALT I)(NOV 2006) shall be included in task orders deemed subject to NASA's Earned Value Management Requirements in existence at the time of execution of this Contract. Note: insert "Subcontractors subject to the requirement of this clause are identified in the task plan." to complete paragraphs (f)(1) and (f)(2).

(d) NPD 1080.1B, Policy for the Conduct of NASA Research and Technology (R&T), dated July 9, 2008, shall apply to all Task Orders for which NASA has delegated program-level functions to the Contractor.

(e) NPR 1080.1A, Requirements for the Conduct of NASA Research and Technology (R &T), dated May 30, 2008, shall apply to all Task Orders for which NASA has delegated program-level functions to the Contractor.

H-30 COST ACCOUNTING STANDARDS—JPL SUBCONTRACTORS

(a) Regarding applicable subcontracts entered into under this Contract, as defined in FAR 52.230-2, Cost Accounting Standards (OCT 2010), the following shall apply: First-tier subcontractors shall be required to submit their Disclosure Statements either to the Contractor or to the cognizant Government Contract Administration Officer. However, if a subcontractor has previously submitted its Disclosure Statement to another Government Administrative Contracting Officer the Subcontractor may satisfy that requirement by certifying to the Contractor the date of the Statement and the address of the Contracting Officer administering the contract.

(b) In any case where a subcontractor lower than the first-tier determines that the Disclosure Statement information is privileged and confidential and declines to provide it to a higher tier subcontractor, the first-tier subcontractor may authorize direct submission of that lower-tier subcontractor's Disclosure Statement to the same Government offices to which the first-tier subcontractor was required to make submission of its Disclosure Statement.

(c) If a subcontractor is a business unit which, pursuant to 48 CFR 9903.201-2(b)(OCT 2010), is entitled to elect modified contract coverage and to follow Cost Accounting Standard 9904.401 (Consistency in Estimating, Accumulating, and Reporting Costs) Cost Accounting Standard 9904.402 (Consistency in Allocating Costs Incurred for the Same Purpose), Cost Accounting Standard 9904.405 (Accounting for Unallowable Costs), and Cost Accounting Standard 9904.406 (Cost Accounting Period), all of which Standards are referenced in 48 CFR 9903.201-2(b)(OCT 2010), the clause at FAR 52.230-3, Disclosure and Consistency of Cost Accounting Practices (OCT 2008), shall be inserted in lieu of the clause prescribed in paragraph (d) of FAR 52.230-2, Cost Accounting Standards (OCT 2010), of this Contract.

H-31 PROTECTION OF SCIENTIFIC AND TECHNICAL INFORMATION OF NATIONAL INTEREST

NASA requires that its scientific and technical information (STI) that may impact the United States' national economic and/or national security interests and/or U.S. competitiveness be protected. Consistent with these concerns, the Contractor shall comply with the terms of this Contract and with United States laws and regulations in the dissemination of technical information.

(a) The Contractor shall manage the informational results of its research and development efforts by conducting an STI Program. STI is defined as the results (the analyses of data and facts and resulting conclusions) of basic and applied scientific, technical, and related engineering research and development;

(b) The Contractor shall collect, manage, disseminate, safeguard, and have archived its NASA STI for use by NASA and NASA contractors and grantees, and where appropriate, the public, to advance scientific and technical knowledge in support of NASA's goals in science, exploration, and aeronautics, strengthen the effectiveness and improve the productivity and cost effectiveness of the NASA research effort, reduce unnecessary duplication, and improve U.S. competitiveness in science and technology.

(c) Unless restricted by U.S. statute or regulation or the terms of this Contract, the Contractor shall provide for the "widest practicable and appropriate dissemination" of STI resulting from NASA's research effort, while complying with Article H-12, Handling, Protection and Release of Restricted Information, and in keeping with the National Aeronautics and Space Act of 1958, as amended;

(d) Unless restricted by U.S. statute or regulation or the terms of this Contract, the Contractor may initiate, prepare and distribute to persons in the scientific and technical communities unclassified-unlimited (as appropriate) scientific and technical reports, when, in its judgment, such distribution will effectuate the purposes of this Contract or is desirable in order to disseminate scientific and technical knowledge and information;

(e) The Contractor shall ensure documentation, approval and dissemination of NASA STI are responsive to the following requirements:

(1) For all final, formal published reports prepared for NASA funded or sponsored science, technology, research and development, and space flight projects, the Contractor shall submit to NASA:

(a) One electronic copy of the STI report;

(b) One electronic copy of JPL Form 1330, showing approval to disseminate and appropriate release requirements.

(2) The Contractor shall assume responsibility for reviewing, approving, and correctly marking all reports, including those for export controlled or limited or restricted STI, pursuant to existing U.S. statutes and regulations. No external distribution of such STI

may be made prior to such review and marking. Document markings shall be consistent and understandable between NASA and the Contractor, and the reports shall contain appropriate reference to NASA or the appropriate reimbursable sponsor;

(3) Requirements for STI reports disclosing inventions are addressed in NASA FAR Supplement (48 CFR Chapter 18) Clause 1852.227-70, referenced in Section H-13 of this contract;

(f) The Contractor shall ensure that the following requirements are met for NASA funded or sponsored work that is performed on subcontracts. The Contractor shall submit the subcontractor's final published report to the NASA Contracting Officer. The subcontractor's final published report shall:

(1) Indicate that the work is funded by NASA;

(2) Be correctly marked to ensure appropriate dissemination; and

(3) Be forwarded to the Contractor.

H-32 END OF CONTRACT OPTIONS

(a) Prior to the end of the Contract's term, the Government may elect to proceed with one or more of the following end of Contract options:

(1) An orderly phase-down and closure of the FFRDC,

(2) A transfer of sponsorship of the FFRDC to another sponsor;

(3) A transition of the FFRDC to another contractor, or

(4) A renewal of the Contract with the Contractor.

(b) This provision does not alter the Government's right to terminate the Contract pursuant to the termination provisions of the Contract, as the circumstances dictate.

(c) Phase-down.

(1) Notice. The Contracting Officer will provide the Contractor with notification of its election to phase-down the FFRDC prior to the expiration date of the Contract.

(2) Phase-down Period. The phase-down period will commence at the end of the Contract term. The phase-down shall not exceed two years unless the parties mutually agree to an extension. The Contract term set forth in Section F shall be extended to coincide with the phase-down period and any extensions thereof.

(3) Terms and Conditions. The terms and conditions in this Contract shall be applicable during any phase-down period except that the Scope of Work set forth in Section C will be revised to incorporate any phase-down plan that the parties agree to implement as set forth in subparagraph (c)(6) below.

(4) Phase-down Costs. NASA will reimburse the Contractor for phase-down costs that are related to the orderly shutdown of the FFRDC and close out of the Contract provided they are reasonable, allocable and allowable under cost principles identified in Clause B-5 (Allowable Costs) of the Contract. This may include costs related to the disposal of assets and reassignment, and assumption or settlement of accrued liabilities incurred by the Contractor during the course of performance. The Government recognizes that all such costs may not be identified prior to the expiration of the phase-down period. NASA will reimburse the Contactor for such costs that are identified after Contract expiration only to the extent they meet the applicable cost principles.

(5) Fee. A fee for work performed under phase-down activities will be negotiated by the parties prior to initiation of the activity.

(6) Proposed Schedule and Objectives for Phase-down.

(i) Within 120 days after the initial notification, NASA shall provide the Contractor with its proposed objectives for the phase-down process as well as a proposed schedule for phase-down. NASA will provide the Contractor with (1) a list of the task orders it intends to allow to continue during phase-down; (2) the proposed term of the phase-down; and (3) a proposed listing of the tasks that the Government expects to remain incomplete at the expiration of the phase-down period.

(ii) Within 120 days of receipt of NASA's proposal, the Contractor shall provide a proposal describing the activities required for phase-down and Contract close out and associated cost estimates. Additionally, the Contractor shall immediately use its best efforts to mitigate cost expenditures for all tasks the Government does not intend to complete during the phase-down, including the exercise of termination provisions in subcontracts or the use of expedited close out procedures when requested by NASA. Using NASA's objectives and the Contractor's proposal, the parties shall enter into good faith negotiations to mutually agree upon an implementation plan for phase-down.

(iii) If the parties are unable to reach agreement upon one or more material aspects of an implementation plan within a reasonable period of time, the Contractor may seek to resolve the issues though the disputes process by submitting a claim or claims to the Contracting Officer pursuant to the Contract Disputes Act.

(iv) In accordance with specific direction of the Contracting Officer, the Contractor shall begin preparing an inventory of all items that are not deliverable or will not be consumed during the phase-down period of performance. All Government property on the inventory shall be reported to the NASA Property Officer for disposition instructions as soon as such property is no longer required for the performance of the Contract. Additionally, the Contractor shall promptly provide NASA with recommended disposition of all lease and other use agreements after a careful review of said leases and agreements. When requested by NASA, the Contractor shall attempt to renegotiate such lease or use agreements on non-NASA facilities to fit within the phase-down period of performance if a cost

effective agreement can be reached. All Contractor property on NASA facilities shall be subject to Government inspection and accounted for and removed per NASA approved procedures.

(d) Transfer to another Sponsor.

(1) Notice. At any time during the term of the Contract, the Contracting Officer may notify the Contractor that NASA has elected to transfer the FFRDC to a new sponsor. Upon receipt of notification, the Contractor shall work with NASA and the successor sponsor to ensure an orderly transfer of the FFRDC. Any such transfer shall not be effective until the Government and the Contractor come to a bilateral agreement on the transfer.

(2) Transfer Period. The transfer period shall not exceed three months unless the parties mutually agree to an extension. If the transfer should coincide with the expiration of this Contract, the Contract term set forth in Section F shall be extended to coincide with the transfer period and any extensions thereof.

(3) Transfer Costs. It is expected that transfer of the FFRDC to a new sponsor during the term of the Contract should have no significant impact on the Contractor's substantive performance under each task order as they relate to the current Contract. Similarly, such a transfer is expected to have no significant impact on the day-to-day administration of the current Contract. Accordingly, the parties acknowledge that the transfer of the FFRDC to another sponsor should not result in any unique costs that must be specifically identified for reimbursement. However, in the event such a transfer takes place at the end of the Contract term, the parties acknowledge that the Contractor will be entitled to Contract close out costs in accordance with applicable cost principles set forth in Article B-5 (Allowable Costs) of the Contract. In addition, if such a transfer occurs in connection with the termination of the Contract by the Government, the parties acknowledge that other costs may be incurred that may be considered for reimbursement by NASA in accordance with the aforementioned cost principles and the termination provisions of this Contract.

(i) Terms and Conditions. The terms and conditions in this Contract shall be applicable during any transfer period.

(ii) Fee. A fee for work performed under Contract transfer activities will be negotiated by the parties prior to initiation of the activity.

(e) Transition to Another Contractor.

(1) Notice. Prior to the expiration date of the Contract, the Contracting Officer may notify the Contractor that it has elected to transition the FFRDC to a new contractor at the expiration of the Contract. Upon receipt of notification, the Contractor shall work with NASA and the successor contractor to ensure an orderly transition of the FFRDC.

(2) Transition Period. Unless the transition occurs in connection with the termination of the contact, the transition period will commence at the end of the Contract term. The transition period shall not exceed three months unless the parties mutually agree to an

extension. The Contract term set forth in Section F shall be extended to coincide with the transition period and any extensions thereof.

(3) Transition costs. The parties acknowledge that the transition of the FFRDC to a new contractor may result in additional costs related to transition activities, in addition to Contract close out costs. NASA will reimburse the Contractor for transition costs related to the orderly transition of the FFRDC to a successor contractor and Contract close out costs provided they are reasonable, allocable and allowable under the cost principles identified in Article B-5 (Allowable Costs) of this Contract. In the event such a transition takes place in connection with the termination of the Contract by the government, the parties acknowledge that other costs may be incurred that may be eligible for reimbursement by NASA in accordance with the cost principles set forth in Article B-5 (Allowable Costs) of the Contract.

(4) Terms and Conditions. The terms and conditions in this Contract shall be applicable during any transition period.

(5) Fee. A fee for work performed under Contract transition activities will be negotiated by the parties prior to initiation of the activity.

(6) Successor Contractor Rule. NASA will not reimburse the Contractor for lump sum severance payments made to its employees who are terminated by the Contractor and rehired by the successor contractor in the same or similar positions.

(f) Renewal of the Contract.

(1) Notice. Prior to the expiration date of the Contract the Contracting Officer may notify the Contractor of the Government's intent to pursue the possibility of renewing the Contract for an additional term. A ten-month notification period is contemplated but not mandatory. Within ten days of receipt of this notice, the Contractor will provide its response. If the Contractor agrees to pursue a renewal, the parties will engage in good faith negotiations to come to an agreement on the terms of renewal. If the Contractor declines the invitation, the Government will then exercise one or more of its options under subparagraphs (c), (d) or (e), above.

H-33 TRANSITION ACTIVITIES

(a) The Contractor recognizes that the work and services covered by this Contract are vital to the NASA mission and must be maintained without interruption, both at the commencement and the expiration of this Contract. It is therefore understood and further agreed in recognition:

(1) At the expiration of the Contract term or any earlier termination thereof, the Contractor shall cooperate with the successor organization and the Government by allowing its employees to interview for possible employment. If such employees accept employment with the successor organization, the Contractor shall release such employees at a time established by the successor organization or by the Government. The Contractor shall cooperate with the successor organization or the Government with regards to the

termination or transfer arrangements for such employees to assure maximum protection of employee service credits and fringe benefits.

(2) After selection by the Government of any successor Contractor, the Contractor and such successor Contractor shall jointly prepare detailed plans for transitioning operations. Such plans shall specify a training and orientation program for the successor Contractor to cover each phase of the scope of work covered by the Contract. A proposed date by which the successor Contractor will assume responsibility for such work shall be established. The Contractor shall retain full responsibility for such work until assumption thereof by the successor Contractor. Execution of the proposed plan or any part thereof shall be accomplished in accordance with the Contracting Officer's direction and approval.

(3) This clause shall apply to subcontracts as approved by the Contracting Officer.

(4) The Contractor shall be reimbursed for all reasonable phase-in and phase-out costs (i.e., costs incurred within the agreed period after *Contract* expiration that result from phase-in and phase-out operations).

(b) At the expiration of the Contract term or any earlier termination thereof, NASA will either substitute a successor contractor, which will assume the Contractor's performance obligations under the Monk Hill Treatment System Agreement, or itself assume the Contractor's performance obligations, thereby releasing the Contractor from any further performance obligations under the Monk Hill Treatment System Agreement. This clause shall apply to any other agreements the Contractor has entered into pursuant to Article H-8(b) to ensure the Contractor's performance obligations under these agreements are transitioned to the applicable successor Contractor or to the Government to the extent such Agreements so permit.

H-34 TRANSITION FROM CONTRACT NAS7-03001

(a) This Contract is a successor Contract intended to provide an orderly transition from Contract NAS7-03001 to this Contract. The transition provisions are set forth below.

(1) All task orders issued under Contract NAS7-03001 with statements of work where the technical performance has not been completed as of September 30, 2012, shall on and after October 1, 2012, be transferred to task orders issued under Contract NNN12AA01C on and after October 1, 2012. All available funds (with the exception of negative expenditures) which, as of September 30, 2012, remain allotted to such task orders and which are un-costed, as shown by the books and records of the Contractor's JPL operating division and verified by the Government, shall on and after September 30, 2012, be de-obligated from NAS7-03001and obligated to NNN12AA01C. All task orders issued under Contract NAS7-03001 with statements of work that have been completed shall remain under NAS7-03001.

(b) The Contractor agrees to take the following steps in performing the transition between Contract NAS7-03001 and Contract NNN12AA01C:

(1) Analyze NASA task orders to identify tasks where the period of performance has been completed.

(2) Associate all tasks where period of performance has been completed under Contract NAS7-03001 with LOC draws from Contract NAS7-03001 LOC.

(3) For task orders whose programmatic period of performance has not been completed:

(i) Review task orders and update only those task plans that it is mutually agreed do not reflect the current scope of work.

(ii) Consistent with the Contractor's standard accounting practices, accrue normal operating costs for work performed but not recorded through September 30, 2012 under Contract NAS7-03001.

(iii) The Contractor will reverse the standard fiscal year-end accruals for Travel and Inventory transactions transacted prior to September 30, 2012, against the Contract NAS7-03001 as recorded. The associated expenses for Inventory and Travel transactions will be recognized and recorded to NAS7-03001 as contractual operational costs as processed by the Contractor's financial systems.

(iv) Reverse the accrual against Contract NAS7-03001 in accordance with the Contractor's standard accounting process in coordination with the receipt and payment of individual vendor invoices and draw from Contract NAS7-03001 LOC on a first-in-first-out (FIFO) basis at the procurement instrument level from the Contract NAS7-03001 LOC until the FY12 accrual amount is equaled. Thereafter, draw all labor and material disbursements from a new LOC established by the Government for this Contract (the "Contract NNN12AA01C LOC").

(v) Charge actual labor and material transactions, plus allocated direct costs processed subsequent to September 30, 2012 to Contract NNN12AA01C.

(vi) Draw all disbursements (i.e., labor, material and allocated direct costs), not including accrual amount as reflected in (b) (3) (iv) above, subsequent to September 30, 2012 from the "Contract NNN12AA01C LOC". The Contractor will allocate the LOC cash requirements by task order for the months of October and November 2012, using the Contractor's recorded labor and allocated directed costs percentages until the NASA Form 533 submittal for October cost reporting is published, at which time the Contractor will follow the methodology referenced in B-6, Contractor Financing by Letter of Credit (b) (3).

(c) All allowable costs, liabilities, and commitments, including but not limited to those attributable to accrued vacation and unemployment compensation, which have been transitioned to, incurred, accrued or made by the Contractor under Contract NAS7-03001 as of September 30, 2012, but which have not by that date been shown as an expenditure on

the books and records of the JPL operating division, shall thereafter be deemed, for all purposes including but not limited to record retention purposes, to be allowable costs, liabilities or commitments incurred, accrued or made under Contract NNN12AA01C; and subsequent payments to the Contractor by the Government arising out of such costs, liabilities and commitments shall be deemed to have been made under Contract NNN12AA01C and shall not be included in the calculation or definition of final payment under Contract NAS7-03001 nor be subject to the "completion invoice" (or "completion voucher"), assignment, release, or other final payment-related requirements of Section I, Article 10, (Allowable Cost and Payment), of Contract NAS7-03001.

(d) All Government property which is in the possession of the Contractor as of September 30, 2012, for the performance of Contract NAS7-03001 shall remain in the possession of the Contractor for the performance of Contract NNN12AA01C, subject to subsequent use or disposition thereof in accordance with the applicable provisions of Contract NNN12AA01C.

H-35 STOP-WORK ORDER

The language in Clause F-3, FAR 52.242.15, Stop-Work Order (AUG 1989) (ALT I)(APR 1984) in paragraph (b) that refers to "any other terms of the contract" specifically includes task orders issued under this Contract.

H-36 SECURITY

(a) In establishing JPL procedures and practices in the areas of security, export control and the hiring, hosting or visits of foreign nationals, the Contractor shall comply with all applicable Federal laws and regulations including the NASA security policy and procedure issuances described below, and current issuances of the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, dated February 28, 2006. In any instance where the NISPOM and applicable NASA guidance requirements are in disagreement, and then only as it applies to classified national security information, NASA will resolve such disagreements with the Defense Security Service (DSS) and the Contracting Officer shall inform the Contractor of such resolution in writing. The Contractor shall comply with NASA's documented resolution.

(1) Federal Information Processing Standard (FIPS) 201-1, Personal Identification Verification (PIV) of Federal Employees and Contractors, dated March, 2006, with Change #1, dated June 23, 2006

(2) National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, dated February 28, 2006

(3) NPD 1600.2E, NASA Security Policy, dated April 28, 2004, revalidated April 1, 2009

i. Section 1 is incorporated with the following understandings:

a. All references to security in paragraphs (h) and (i) refer to physical security

b. Paragraph (l) is deleted in its entirety and replaced with:

(l) Developing, implementing, and maintaining an information database for physical access histories of non-Contractor personnel to include foreign national visitors, representatives, subcontractors, and students.

(4) NPD 1600.3, Policy on Prevention of and Response to Workplace Violence, dated September 4, 2007

(5) NPD 1660.1B, NASA Counterintelligence (CI) Policy, dated November 18, 2008

(6) FAR 52.204-9, Personal Identity Verification of Contractor Personnel (JAN 2011)

(7) RESERVED

(8) NPR 1600.2, NASA Classified National Security Information (CNSI), dated October 11, 2011

(9) JPL NPR 1600, Physical and Program Security, dated May 16, 2012

The NPR is incorporated into the Contract in Attachment H. The following conditions and understandings will apply as set forth below:

i. Chapter 1 is accepted with the following conditions:

a. Section 1.2.5 a.(1)(c.) is replaced by:

Ensure NASA/JPL/Caltech employees expeditiously report to CCPS any information concerning actual or suspected espionage. CCPS will expeditiously report any information with a reasonable basis concerning actual or suspected espionage to the servicing NASA CISA. Employees may report directly to NASA CISA.

ii. Chapter 2 is not applicable.

iii. Chapter 3 is accepted with the following conditions:

a. Sections 3.2.1b through 3.3.10 are deleted as not applicable

b. Section 3.8 is not applicable.

c. Section 3.11 is not applicable

d. Section 3.22.3 is deleted

e. 3.30.3 is clarified as follows: Any type of IT Security Incident that might have Agency security implications shall be reported to the NASA Security Operations Center (SOC), NASA Office of Inspector General (OIG), and

NASA Management Office (NMO) in a timely manner. IT Security Incidents will not be directly reported to AA, OPS.

f. 3.30.3 k. is replaced by: An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incident categories include unauthorized access, denial of service, malicious code, and inappropriate usage.

g. Chapter 3.33 is not applicable to the Contractor. In the event either party determines that there is a need for TSCM, NASA will provide such services.

iv. Chapter 4 is accepted with the following conditions:

a. Section 4.4 is not applicable.

v. Chapter 5 is accepted with the following conditions:

a. Section 5.2 is not applicable and Section 5.3 applies to the role of the NASA AA, OPS who is a civil servant.

b. 5.3.3a is accepted with the words “NASA NMO Chief” deleted.

c. 5.3.4.1 is accepted with the word “General” substituted for “Chief”.

(10) JPL NM 1600-96, Personnel Security, dated May 16, 2012

The document is incorporated into the Contract in Attachment I. The following understandings apply:

i. The Contractor will perform risk designations to include elements of physical access, logical/IT access, duration of access, and national security to determine the appropriate level of background investigation.

ii. Chapter 1 is accepted with the following conditions:

a. Section 1.3.3 – NMO or NASA Headquarters will perform actions involving civil servant employees.

b. Section 1.3.3 n is not applicable.

c. Section 1.3.4 a delete “Maintaining electronic files and”

d. Section 1.3.4 c. is not applicable.

e. Section 1.3.4 d. is not applicable.

f. Section 1.3.7 b. - Contractor HR will lead and coordinate with Acquisitions and OPS for the designation of risk for subcontractor employees and the timely on boarding of subcontractor employees.

iii. Chapter 3 is accepted with the following conditions:

a. Sections 3.4.1 and 3.4.4 are deleted as inapplicable

b. Section 3.4.6 (Additional Comment) is replaced by:

Additional Comment—Contractor employees will have a position description describing the nature of the work that will be performed. The position description will describe the nature of the duties and include a risk level and sensitivity determination to those duties of low, moderate or high or need for access to CNSI.

c. Section 3.11—PIV Smart Card Authorizer Role is performed solely by NMO Civil Servants.

d. Section 3.14.1—Adjudications are performed by NMO.

e. Section 3.14.3—NMO will perform all duties including issue decision letter. The Contractor's Center Chief of Security will be notified that an unfavorable determination has been issued.

f. Section 3.14.4—Reconsideration panel appointed by HQ OPS AA or designee. Panel members to include NMO representatives or other NASA Civil Servants.

g. Section 3.14.5—Panel decision elevated to HQ OPS AA or designee rather than Center Director.

(11) JPL NPR 1620.2, Facility Security Assessments, dated October 14, 2011, is incorporated into the Contract in Attachment J.

(12) JPL NPR 1620.3, Physical Security Requirements for NASA Facilities and Property, dated October 14, 2011, is incorporated into the Contract in Attachment K.

(13) JPL NPR 1660.1B,Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements, dated October 14, 2011, is incorporated into the Contract in Attachment L.

(14) JPL NM 1600-95, ID and Credential Management, dated May 16, 2012.

The document is incorporated into the Contract in Attachment M with the following understandings:

i. Chapter 2 is accepted with the following conditions:

a. Section 2.3.1—The Center PIV Issuing Facility Manager and Center Chief of Security at JPL are not federal civil servants.

b. Section 2.3.4—The PIV Sponsor role is not required to be a federal civil servant.

c. Section 2.3.6—The PIV Authorizer role is performed by NMO not Contractor Personnel Security staff (unless delegated by NMO).

d. Section 2.4—Contractor employees working in the Badging Office may have more than one role as long as it is not that of Authorizer.

ii. Chapter 4 is accepted with the following conditions:

a. Delete 4.11.1c. The Contractor does not perform fingerprint checks for Foreign National visitors that are visiting 29 days or less.

b. The Contractor shall comply with Section 4.3.3 effective October 1, 2012.

c. The word “for” in Section 4.10.2 shall be replaced with “or”.

d. Section 4.12.2 is replaced by: The Contractor will obtain NASA approval and ensure all required export control licensing will be in place for Foreign National access to “limited privileged” IT systems.

e. Section 4.12.5 is not applicable.

H-37 AGREEMENT ON COMPUTER SOFTWARE

(a) The parties agree that the Contractor shall own all copyrights in computer software, including derivative works, developed under this Contract. Therefore, the Contractor is granted permission to assert copyrights in computer software developed under this Contract, and this Clause H-37 serves as the prior written authorization as specified under FAR 52.227-14(c)(1) (DEC 2007) and NASA FAR Supplement 1852.227-14(3)(i).

For the purposes of this Contract, the term “computer software” is defined as in FAR 52.227-14(a)(DEC 2007). Notwithstanding said Contractor rights, including the right to license such copyrights, the Government shall retain the license set forth in FAR 52.227-14(c)(iii)(DEC 2007).

Additionally, for computer software developed under a Task Order under this Contract for NASA’s Earth Science Division within the Science Mission Directorate that is used for processing of scientific data from Earth-orbiting instruments to create data products that are hosted on an Earth Observing System–Distributed Active Archive Center for public distribution, Contractor shall provide an Algorithm Specification Document (ASD) or, at the option of the Contractor, the computer software source code associated with the computer software under a license for the limited purpose of validation of the data products generated by the computer software to any requesting entity. Any ASD provided under such a license

shall provide information to validate the data products generated by the computer software to the same extent that is provided by the computer software source code. The license will be made available at no cost for non-commercial purposes and the Contractor shall negotiate reasonable terms and conditions to provide the license for commercial purposes. The requirements described herein to issue licenses and distribute ASDs or computer software source code are subject to applicable laws, including, without limitation, export control laws and procedures. Should Contractor determine said applicable laws, or other reasons, restrict the dissemination of the ASDs or computer software source code to any requesting entity, Contractor shall inform NASA of such determination including the grounds upon which said determination was based.

(b) On the licensing or assignment by the Contractor of copyrights on computer software developed under this Contract, the parties agree to share equally in any royalties received from said licensing or assignment. Any payments to inventors and/or authors of software programs shall be calculated and paid prior to division of the remaining royalties between the parties. The Contractor shall provide the U.S. Government its 50 percent share of the gross royalties or monies received by the Contractor, after any payment to inventors and/or authors of computer software, from said licensing or assignment as an offset to allowable costs incurred under this Contract. These funds shall be provided and applied on a quarterly basis specifically as an offset to allowable costs incurred under this Contract in the performance of software technology development, and transfer and commercialization activities at JPL. In addition, the Contractor may elect to provide, in the same manner and for the same purpose, additional royalties or monies received by the Contractor from the licensing or assignment of copyrights on computer software, and other intellectual property developed under this Contract.

(c) The Contractor shall also provide a quarterly report to the Contracting Officer on the licensing of intellectual property rights on computer software developed under this Contract. For such computer software, this report shall include actual licensing and/or assignment of intellectual property rights; the receipt and distribution of gross royalties or monies received by the Contractor during the reporting period; and a listing of active licenses or assignments and the royalty amounts attributed to specific licenses or assignments during the reporting period and the year to date.

(d) In the licensing and distribution of computer software developed under the Contract, the Contractor agrees to comply with all applicable laws and regulations concerning the export of commodities and technical data.

H-38 AGREEMENT ON ESTABLISHMENT OF RIGHTS, TECHNOLOGY TRANSFER, AND DISTRIBUTION OF INCOME WITH RESPECT TO MASK WORKS

The parties have agreed to the following arrangement in the belief that certainty with respect to the grant of statutory rights in Mask Works will enhance the transfer to third parties of semiconductor chip product technology.

(a) Within six (6) months after written disclosure of a Mask Work has been made to Contractor personnel responsible for implementation of Article H-14 (Patent and New Technology

Services), the Contractor shall furnish the Contracting Officer a full and complete technical report thereon, together with notice of whether or not Contractor elects to apply for registration, or publication with appropriate notice, of any Mask Work to which Contractor elects to retain title. In such instances Contractor will file an application to register Mask Works in a timely manner, but no later than six months after said notification. In the event it fails to do so, the rights otherwise provided to Contractor herein shall revert to the Government, with the reservation of a royalty free, nonexclusive license to Contractor for research and educational purposes.

(b) In the event Contractor receives royalty or other monetary consideration from the grant of Mask Work rights to a third party, after deduction of 25 percent which includes distribution according to Contractor's established royalty sharing plan, costs associated with registration and licensing, and other administrative costs, the remaining 75 percent shall be shared equally with the Government.

(c) The Contractor shall report such shared income quarterly to the Government specifying the licensed mask works, the licenses, and the income attributed to specific licenses. In the licenses and distribution of Mask Works developed under the Contract, the Contractor shall include statements regarding any export restrictions that may apply, and shall comply with all applicable U. S. export laws and regulations.

(d) This clause constitutes the permission required to claim copyright under Article G-12 (References to FAR "Rights in Data" Clause).

H-39 GOVERNMENT-FURNISHED COMPUTER SOFTWARE AND RELATED TECHNICAL DATA

(a) *Definitions.* As used in this clause—

"Government-furnished computer software" or "GFCS" means computer software: (1) in the possession of, or directly acquired by, the Government whereby the Government has title or Government purpose license rights thereto; and (2) subsequently furnished to the Contractor for performance of a Government contract.

"Computer software," "data" and "technical data" have the meaning provided in the Federal Acquisition Regulations (FAR) Subpart 2.1—Definitions and the Rights in Data—General clause (FAR 52.227-14).

(b) The Government shall furnish to the Contractor the GFCS described in this contract or in writing by the Contracting Officer. The Government shall furnish related technical data needed for the intended use of the GFCS.

(c) *Use of GFCS and related technical data*. The Contractor shall use the GFCS and related technical data, and any modified or enhanced versions thereof, only for performing work under this contract unless otherwise provided for in this contract or approved by the Contracting Officer.

(1) The Contractor shall not, without the express written permission of the Contracting Officer, reproduce, distribute copies, perform publicly, display publicly, release, or disclose the GFCS or related technical data to any person except for the performance of work under this contract.

(2) The Contractor shall not modify or enhance the GFCS except as required pursuant to the performance of work under this contract. If the GFCS is modified or enhanced pursuant to this contract, the Contractor shall provide to the Government the complete source code, if any, of the modified or enhanced GFCS.

(3) Allocation of rights associated with any GFCS or related technical data modified or enhanced under this contract shall be defined by the FAR Rights in Data clause(s) included in this contract as modified by clause H-37.

(4) The Contractor may provide the GFCS, and any modified or enhanced versions thereof, to subcontractors as required for the performance of work under this contract. Before release of the GFCS, and any modified or enhanced versions thereof, to such subcontractors (at any tier), the Contractor shall insert, or require the insertion of, this clause, including this paragraph (c)(4), suitably modified to identify the parties as follows: references to the Government are not changed, and in all references to the Contractor the subcontractor is substituted for the Contractor so that the subcontractor has all rights and obligations of the Contractor in the clause.

(d) The Contracting Officer may by written notice, at any time—

(1) Increase or decrease the amount of GFCS under this contract;

(2) Substitute other GFCS for the GFCS previously furnished, to be furnished, or to be acquired by the Contractor for the Government under this contract;

(3) Withdraw authority to use the GFCS or related technical data; or

(4) Instruct the Contractor to return or dispose of the GFCS and related technical data.

(e) *Title to or license rights in GFCS*. The Government shall retain title to or license rights in all GFCS. Title to or license rights in GFCS shall not be affected by its incorporation into or attachment to any data not owned by or licensed to the Government.

(f) *Waiver of Claims and Indemnification*. The Contractor agrees to waive any and all claims against the Government and shall indemnify and hold harmless the Government, its agents, and employees from every claim or liability, including attorney's fees, court costs, and expenses, arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of the GFCS and related technical data by the Contractor or by any person to whom the Contractor has, without authorization, released or disclosed such GFCS or related technical data. The Government makes no warranty with respect to the serviceability and/or suitability of the GFCS for contract performance. Nothing in this subparagraph shall limit the Contractor's rights under this contract with regards to costs allowability under paragraph B-5, Allowable Cost and FAR

52.228-7, Insurance—Third Party Liability. In addition, equitable adjustments shall be made in accordance with the procedures of the Changes clause in the event of a delivery of Government furnished computer software to the Contractor in a condition not suitable for its intended use.

H-40 PAYMENT OF OVERTIME PREMIUMS

For purposes of administering FAR 52.222-2, Payment of Overtime Premiums (JUL 1990), prelaunch activities and mission performance or delivery related events of an urgent nature shall be deemed to be activities covered by FAR 52.222-2 paragraph (a)(3). In order to aid in contract administration, the Contractor shall provide the Contracting Officer with a quarterly report evidencing overtime hours performed. Upon receipt of a written request from the Contracting Officer, JPL shall provide any additional information in this regard within fifteen calendar days.

H-41 REQUIRED SOURCES OF SUPPLIES AND SERVICES

The Contractor shall acquire radioisotopes, liquid hydrogen, propellants, and mercury per NFS 1808.003-70, 71, 72, and 73.

H-42 USE OF FACILITIES PLAN

The Contractor shall prepare, maintain, and comply with a Use of Facilities Communications Plan. The terms of the Plan shall be subject to the approval of the Director of the NMO. The Plan shall set forth:

(1) Notification requirements applicable to use of Government-owned and Government-leased facilities provided under Article C-2 (Resources for Performance of the Contract) of this Contract for specified categories of activity associated with performance of this Contract and

(2) Approval requirements applicable to use of such facilities by third parties.

H-43 INFORMATION TECHNOLOGY

a. All of the Contractor's Information Systems are under the direct management and control of the Contractor and are reported to the OMB as external contractor system unless a determination is made that the system should be reported as an internal NASA system. The Contractor shall follow applicable Federal and NASA security and privacy policies and regulations as outlined clause I-7 "*Security Requirements for Unclassified Information Technology Resources, NFS 1852.204-76*".

b. In the planning and execution of its activities under this Contract, the Contractor shall perform in such a manner so as to support NASA in meeting the legal and policy mandates associated with managing the government's information technology (IT) infrastructure, systems, assets and information. To accomplish this, the Contractor will assist by providing technical, logistical, and other services as may be necessary to NASA. Further, the Contractor shall, in consultation with the NASA OCIO, establish and maintain procedures to

substantiate that JPL-related IT and information resources are acquired and managed in a manner that safeguards NASA's IT infrastructure, systems, assets and information.

c. The Contractor shall provide an IT environment at JPL that meets the following requirements:

(1) Select and implement appropriate security controls designed to protect the confidentiality, integrity, and availability of the system and its information for all JPL information systems or system-of-systems as outlined in clause I-7. Among other elements, include security controls that provide for (i) incident response training; (ii) incident response testing and exercise; (iii) incident handling; (iv) incident monitoring; (v) incident reporting; and (vii) assessment responsibilities (e.g., NASA or other government auditors; self-assessment; independent verification and validation assessors).

(2) The Contractor, when requested, shall support NASA in its reporting efforts about Agency IT and information activities to Agency Officials, Office of Management and Budget (OMB), Congress, the Government Accountability Office, NASA OIG, and other external oversight organizations.

(3) NASA shall have the use of all software assets at JPL to the extent allowed by the individual license agreement entered into by the Contractor under this contract that has been paid for by NASA.

(4) The Information Management staffs of the Contractor shall be available for participation in NASA-wide information management efforts on matters of NASA-wide policies. JPL shall support the NASA OCIO Enterprise Architect (EA) on agency wide reporting, data collection and align with agency enterprise architecture as it relates to JPL systems that interface or share data with NASA systems.

(5) The IT staffs of the Contractor shall be available for participation in NASA information technology prototype and pilot efforts. The contractor shall support the NASA OCIO IT Chief Technology Officer (CTO) working group efforts to plan and govern IT innovation and technology infusion efforts.

(6) At the request of NASA's OCIO, the Contractor shall support NASA in its analysis of or in its implementation of government-wide IT initiatives.

(7) Domains and Websites

a. Domains: In light of JPL's role as NASA's FFRDC, the Contracting Officer authorizes the contractor to utilize the JPL.NASA.GOV domain.

b. Websites: JPL websites hosted outside of the nasa.gov portal shall be developed, managed and maintained by the Contractor and follow the policies, procedures, and guidelines developed by the Contractor's Office of the Chief Information Officer and meet the requirements outlined in clause I-7. The Contractor shall

provide NASA verification and validation that their policies, procedures, and guidelines meet Federal laws and regulations applicable to the contractor.

(8) All electronic and information technology (EIT) products intended for use by the Government or public, and resulting from work performed under this Contract, regardless of whether or not the product(s) is specified as a deliverable of a task order, shall comply with the requirements of Section 508 of the Rehabilitation Act 29 U.S.C. 794(d), as described by the Architectural and Transportation Barriers Compliance Board ("Access Board") at 36 CFR Part 1194. "EIT" is defined by the Access Board at 36 CFR Part 1194.4. This requirement does not apply to electronic and information technology that is incidental to the contract or to web pages that are not located at .gov web address. The Contractor shall be responsive to the Government's requests to prepare plans for a report status on adherence to Section 508 requirements. The Contractor shall comply with Section 508 requirements unless an exception is documented in writing by the Contracting Officer. Exceptions to the law must be submitted to the Contracting Officer and the appropriate NASA OCIO official in writing and include the specific reason(s), consistent with the exceptions and undue burden considerations permitted under Section 508, why a specific product cannot be made accessible.

d. In order to ensure that information technology (IT) and information resources are acquired and managed in a manner that implements the Contractor's policies, procedures, and priorities, the Contractor shall perform the following activities:

(1) Mission Enablement: Ensure that IT enables the Contractor's missions, goals, and objectives; and promote the use of IT by the Contractor to improve the productivity, efficiency, and effectiveness of the Contractor's programs;

(2) IT Infrastructure Management: Manage the IT infrastructure as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration;

(3) IT Application Portfolio Management: Develop and maintain an application portfolio management process to drive application standardization and efficiency;

(4) Enterprise Architecture and IT Planning: Develop, maintain, and implement an Enterprise Architecture (EA), Information Resources Management (IRM) Strategic Plan, and other plans, standards, models, documents, and guidance that define the Contractor's IT environment;

(5) IT Governance: Develop and maintain an effective IT governance structure and Request Notification of Change processes to ensure that IT strategy, investment, implementation, and operations decisions are integrated with organizational planning, budget, financial management, human capital management, and programmatic decisions and processes;

(6) IT Investment Management: Ensure that Contractor IT investments are selected, controlled, and evaluated through effective IT governance, investment management, and program/project management processes;

(7) IT Security Management: Ensure the appropriate confidentiality, integrity and availability of information residing on, or processed by automated information systems through implementation and enforcement of risk-based policies, procedures, standards, guidelines, control techniques, and training mechanisms;

(8) IT Budgeting: Implement planning, programming, budgeting and execution, and program and project management processes to formulate, implement, and operate Contractor IT services and initiatives; and—

(9) IT Workforce Planning: Ensure appropriate competency of the Contractor's IT workforce through training, mentoring, and professional development. Ensure that required skills are identified, developed, recruited, retained, and available to support Contractor activities.

H-44 LITIGATION MANAGEMENT PLAN

(a) A litigation management plan is a statement describing in advance the Contractor's practices for managing legal costs for litigation matters for which it procures the services of retained counsel. The Contractor shall prepare a litigation management plan that assures that retained legal counsel provides efficient and effective conduct of JPL-related litigation at a reasonable cost.

(b) The Contractor shall submit its JPL litigation management plan to the Contracting Officer within 90 days after the effective date of this Contract. The Contractor shall annually review and update its litigation management plan and submit any changes to the Contracting Officer.

(c) The Contractor is responsible for accounting for costs incurred in connection with procuring the services of retained litigation counsel and for maintaining records adequate to demonstrate that costs claimed have been incurred, are allocable to the Contract, and comply with the applicable cost principles. The Contractor shall maintain such records for a period of three years after final payment and provide the Government access to such records for purposes of auditing expenditures. The Contractor is responsible for ensuring that the rates for professional fees of retained litigation counsel are reasonable for the services provided.

(d) The Contractor shall provide notice of JPL litigation to NASA pursuant to FAR 52.228-7(g)(1), Insurance – Liability to Third Persons (MAR 1996) and shall state whether the Contractor has reached a decision to engage outside counsel and the identity of such counsel. In addition, the notice shall state whether the litigation involves class actions or environmental torts or any other issue that the Contractor reasonable believes is of particular interest to NASA or the Government as a whole. Further, the notice shall state whether the Contractor reasonably anticipates asserting a claim or defense materially adverse to that of the Government.

(e) For those legal matters charged as a direct cost pursuant to B-5(b) rather than B-5(c)(2) of this Contract, the Contractor, if requested in writing by the Contracting Officer, shall prepare a case assessment as well as a staffing and resource plan for any matter for which

the Contractor has given notice to NASA pursuant to FAR 52.228-7(g)(1), Insurance—Liability to Third Persons (MAR 1996). The Contractor will ordinarily respond to a request for case assessment and/or staffing and resource plan within 30 days after responding to the complaint and will provide the following information:

(1) Case budget broken down by phases in the litigation including:

(i) Initial case development;

(ii) Pretrial pleadings and motions;

(iii) Discovery;

(iv) Trial preparation and trial; and

(v) Appeal.

(2) Case assessment including:

(i) Comprehensive analysis of the case;

(ii) Recommendations for resolution.

(3) The procedure for keeping the Contracting Officer informed about the matter as it proceeds through the adjudicator process and, if necessary, interacting with the Department of Justice.

(f) Nothing in this Article H-44 is intended to abridge or constitute a waiver of any attorney-client privilege or attorney work product privilege and it is understood that in complying with H-44, the Contractor shall maintain any such privileges.

H-45 INTEGRATION OF ENVIRONMENT, SAFETY, AND HEALTH INTO THE CONTRACTOR'S MANAGEMENT SYSTEM

(a) For the purposes of this Article,

(1) The environmental, safety, and health system (ESHS) encompasses safety and health of employees, protection of environment, and the protection of the facility (plant) and products from damage, and includes pollution prevention, waste minimization, efficient energy management practices; and

(b) In performing work under this Contract, the Contractor shall perform work safely, in a manner that ensures adequate protection of the public, employees, the facility (plant) and product from damage, and the environment, and shall be accountable for the safe performance of work. The Contractor shall integrate environmental, safety and health requirements into JPL program missions and Center operations. Environment, safety, and health programs shall be operated as an integral and visible part of how the organization conducts both its mission and facility operational business, including the management of

both routine and emergency operations. The Contractor shall exercise due care commensurate with the associated hazards of the work. The Contractor shall ensure that management of environment, safety and health functions and activities becomes an integral and visible part of the Contractor's work planning and execution processes. The Contractor shall, in the performance of work, ensure that:

(1) Line management is responsible for establishing, maintaining, and enforcing safe and healthful working conditions and procedures for all personnel. All personnel shall take every reasonable measure to ensure safe and healthful operations and conditions in accomplishing its work, including the protection of the public, the facility, the product, and the environment from injury, illness, or damage.

(2) Clear and unambiguous lines of authority and responsibility for ensuring appropriate environment, safety and health processes are established and maintained at all organizational levels.

(3) Employees possess the experience, knowledge, skills, and abilities that are necessary to discharge their responsibilities.

(4) Resources are effectively allocated to address environment, safety and health, programmatic, and operational considerations. Protecting the public and the employees from injury or illness, the facility (plant) and product from damage and the environment is a priority whenever activities are planned and performed.

(5) The ESHS implements the requirements of NPR 8553.1B, NASA Environmental Management System, dated September 22, 2009. The ESHS will be designed to integrate management of environmental practices, and ensure compliance with applicable laws, regulations, and policies. NPR 8553.1B is incorporated with the following understandings:

(i) All Center-led reviews referenced in the NPR are self-assessments.

(ii) Regarding paragraph 2.1.4(d), the Contractor's environmental policy shall not be made available to the public.

(iii) Regarding paragraphs 4.2.1(a) and 4.2.1(b), Contractor-wide training will be made available to Contractor employees who elect to take it; however, this will not be considered mandatory training. This does not exempt employees from taking mandatory training required under federal, state or local regulation.

(6) Before work is performed, the associated hazards are evaluated and environment, safety and health standards and requirements are established which, if properly implemented, should provide adequate assurance that employees, the public, and the environment are protected from adverse consequences.

(7) Administrative and engineering controls to prevent and mitigate hazards are tailored to the work being performed and associated hazards. Emphasis should be on designing

the work and/or controls to reduce or eliminate the hazards and to prevent accidents and unplanned releases and exposures.

(c) The Contractor shall manage and perform work in accordance with a documented site-wide integrated ESHS that fulfills all conditions in paragraph (b) of this clause at a minimum. Documentation of the ESHS shall describe how the Contractor will:

(1) Define the scope of work;

(2) Identify and analyze hazards associated with the work;

(3) Develop and implement hazard controls;

(4) Perform work within controls;

(5) Provide feedback on adequacy of controls and continue to improve safety management; and;

(6) Describe how the Contractor will measure system effectiveness.

(d) The Contractor shall submit to the Contracting Officer documentation of its ESHS for review and comment. The Contracting Officer will establish dates for submittal, review, and comment on the ESHS documentation. Guidance on the preparation, content, review, and approval of the ESHS will be provided by the Contracting Officer. The Contractor shall review and update its ESHS on an annual basis and submit documentation to the Contracting Officer for review.

(e) The Contractor shall maintain the integrity of its ESHS and ensure it is integrated with the Contractor's business processes for work planning, budgeting, authorization, execution, and change control.

(f) The Contractor shall comply with, and assist the Government in complying with, environment, safety and health requirements of all applicable laws and regulations, and applicable Government Policies. The Contractor shall cooperate with Federal and non-Federal agencies having jurisdiction over environment, safety and health matters under this Contract.

(g) The Contractor shall promptly evaluate and resolve any non-compliance with applicable environmental, safety, and health requirements of this Contract, and the ESHS. If the Contractor fails to provide resolution or if, at any time, the Contractor's action or inaction causes substantial harm or an imminent danger to the environment or health and safety of employees or the public, the Contracting Officer may issue an order stopping work in whole or in part. Any stop work order issued by a Contracting Officer under this clause (or issued by the Contractor to a subcontractor in accordance with paragraph (i) of this clause) shall be without prejudice to any other legal or contractual rights of the Government. In the event that the Contracting Officer issues a stop work order, an order authorizing the resumption of the work may be issued at the discretion of the Contracting Officer. The Contractor shall not be entitled to an extension of time or additional fee or damages by reason of, or in connec-

tion with, any work stoppage ordered in accordance with the warranted exercise of this paragraph of the Article.

(h) The Contractor is responsible for flowing down the environment, safety and health requirements applicable to this Contract to subcontracts at any tier to the extent necessary to ensure the Contractor's compliance with the requirements.

(i) The Contractor shall include an Article substantially the same as this Article in subcontracts involving hazardous work on site at a NASA-owned or-leased facility. Such subcontracts shall provide for the right to stop work under the conditions described in paragraph (g) of this Article. Depending on the complexity and hazards associated with the work, the Contractor may choose not to require the subcontractor to submit an ESHS for the Contractor's review and approval.

H-46 NASA AUTHORITY DURING EMERGENCIES

(a) The authority expressed by NASA in this Article does not in any way reduce or diminish the responsibility the Contractor otherwise has under the terms of this Contract with regard to emergency preparedness and for executing the Emergency Plan prepared pursuant to Article H-7(2) (Safety and Health) of this Contract.

(b) The Contractor recognizes that NASA may, in the event of an emergency (e.g., specific environmental, health, safety hazard, or security threat), direct the Contractor to take necessary action to shutdown JPL in a timely, but safe and protective manner. Such direction will be coordinated through the NMO Director or designee and the Contractor's action taken consistent with the Emergency Plan prepared pursuant to Article H-7(2) (Safety and Health) of this Contract.

(c) The Contractor further recognizes that NASA may, in the event of an emergency (e.g., specific environmental, health, safety hazard, or security threat), direct the Contractor to take necessary action to timely cooperate with local, State, or federal public safety or emergency response organizations. Such direction will be coordinated through the NMO Director or designee and the Contractor's action taken consistent with the Emergency Plan prepared pursuant to Article H-7(2) (Safety and Health) of this Contract.

H-47 NASA OFFICE OF THE INSPECTOR GENERAL PROGRAMS

(a) It is NASA policy that all NASA contractors cooperate fully with the NASA Office of Inspector General (NASA OIG) and its designees. Particularly in view of JPL's status as a FFRDC, the Contractor agrees to cooperate fully with the NASA OIG during the conduct of its programs, including audits, investigations, inspections, assessments, reviews, or other activities relating to JPL conducted pursuant to the authority conferred upon the NASA Inspector General by the Inspector General Act of 1978, as amended.

(b) In fulfilling its obligations under section (a) of this clause, the Contractor shall, in collaboration with the NASA OIG, establish and maintain procedures for cooperating with OIG audits, inspections and investigations and for supporting the OIG's investigations into unauthorized intrusions into NASA-owned or NASA-funded computer systems (including

networks) operated by JPL. These procedures shall ensure the NASA OIG is timely informed of allegations that provide a reasonable basis to suspect that a crime may have been committed. The Contractor shall submit these procedures to the OIG for review and comment within 30 days after the effective date of this Contract.

(c) Nothing in this Contract is intended to abridge or be in derogation of the Inspector General's authority under the Inspector General Act of 1978, as amended.

H-48 RESPONSE TO INFORMATION CORRECTION REQUESTS

As requested by the Government, the Contractor shall validate the accuracy of information that is the subject of a public request for correction pursuant to Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554), also known as the Data Quality Act. Pursuant to the requirements of the Act, the Contractor shall determine whether correction of the challenged information is warranted, and if so, the Contractor shall correct the information in accordance with existing statutes, regulations, and procedures. If the Contractor decides not to correct the information, the Contractor shall inform the Government of the reason for the decision. The Contractor shall be responsive to the Government's requests to prepare plans for and report status on adherence to Data Quality Act requirements.

H-49 COORDINATION WITH NASA ON NOTICES AND CORRECTIVE ACTIONS

(a) For purposes of this clause, the term "Notice" includes, but is not limited to Notice of Deficiency, Notice of Non-compliance, Notice of Violation, Notice of Alleged Violation, Notice of Regulatory Violation, Notice of General Violation, Notice of Serious Violation, or any other similar type communication from a federal, state, or local regulator that has jurisdiction over environmental, safety, and health matters relating to work performed under the Contract.

(b) Protection of workers, the public, and the environment are fundamental responsibilities of the Contractor. However, the Contractor recognizes JPL is a Government-owned facility and that NASA has certain responsibilities for the conduct of all programs funded through the Contract and for assuring that the Government funds are properly and effectively utilized. Therefore, the Contractor shall establish and maintain a procedure for keeping NASA informed of communications and interactions the Contractor might have with federal, state, or local regulators and for coordinating the Contractor's response with NASA prior to submitting its response to the regulators.

(c) Consistent with paragraph (b) of this Article, the Contractor shall verbally notify the Contracting Officer or designee within 48 hours of any Notice the Contractor may receive, as described in paragraph (a) of this Article. The Contractor shall notify the Contracting Officer or designee in writing, along with submitting a copy of the Notice, not more than five (5) days after receipt of the Notice.

(d) Consistent with (b) of this clause, the Contractor shall coordinate the Contractor's proposed response to the Notice with NASA prior to submitting its response to the regulators. Coordination with NASA should be initiated early enough to ensure any time line set forth in the Notice or established by the cognizant regulator is timely met. Continuing

coordination by the Contractor with NASA may, depending on the subject matter and circumstances surrounding the Notice, be necessary. If warranted, NASA may provide additional guidance to the Contractor to facilitate the coordination process, especially if a corrective action or other similar response plan must be submitted by the Contractor to the cognizant regulator.

(e) The Contractor, if requested to do so by the Contracting Officer, shall provide assistance to the Government concerning any matter arising under or relating a Notice as described in paragraph (a) of this Article.

(f) When NASA or another NASA contractor receives a Notice with respect to a facility described in Article C-2 (Resources for Performance of the Contract), NASA shall provide (or require its contractor to provide) the Contractor with a copy of the Notice.

H-50 AIRCRAFT OPERATIONS

(a) Routine flight operations at JPL are not authorized unless and until the JPL helipad is in full compliance with NASA and Federal airfield/heliport safety standards. Until such time, the area formerly used as the JPL helipad can only be utilized for emergency operations with approval from the Director of HQ Aircraft Management Division, on a case by case basis.

(b) When leasing, chartering, or renting aircraft or aircraft services to include Unmanned Aerial Systems (UAS) for research, passenger transportation, or technology demonstration the Contractor shall comply with the following:

(1) The Contractor will ensure that all aviation subcontracts are approved by the NASA Dryden Flight Research Center (DFRC) aircraft management office to ensure compliance with NASA aviation safety program and aircraft management policies. DFRC Chief of Flight Operations is responsible for ensuring all Contractor flight operations are conducted in accordance with the applicable policies and procedures contained NPR 7900.3C, NASA Aircraft Operations Management Manual, dated July 15, 2011.

(i) The Contractor will notify and receive approval from the NASA Dryden Flight Research Center for all aircraft airworthiness certification processes and flight readiness reviews for all Contractor aircraft projects. The Contractor must have Dryden Flight Research Center airworthiness and flight readiness approval prior to conducting any flights. Dryden Flight Research Center will handle all of the appropriate NASA HQ notifications in regards to Contractor aircraft usage regardless of when a NASA asset (aircraft) is utilized or when a Contractor contracted aircraft is utilized. Dryden Flight Research Center will handle all coordination with other centers as appropriate to obtain airworthiness certification and/or flight readiness reviews for the Contractor’s activities. DFRC will provide the safety data compliance requirements for aircraft services.

(ii) The Contractor will be responsible to ensure that a sufficiently detailed risk analysis of the research or technology demonstration is conducted and provided to Dryden Flight Research Center for review and approval in a timely manner (at

least 30 days in advance) to allow DFRC time to conduct airworthiness reviews and on-site evaluations.

(iii) The Contractor will provide support as appropriate and as requested to enable DFRC to conduct proper and complete flight airworthiness approvals and flight readiness reviews are conducted for all aircraft usage by the Contractor.

(2) Purchase of contract aircraft services shall require the approval of the Assistant Administrator for the Office of Strategic Infrastructure, in accordance with NPR 7900.3C. This approval shall be obtained through the NASA Management Office.

(3) Costs associated with the Dryden Flight Research Center support and oversight of Contractor aircraft operations will be the responsibility of the HQ NASA Programs that require aircraft services.

(4) NPR 7900.3C, NASA Aircraft Operations Management Manual, dated July 15, 2011, is applicable with the following exceptions:

(i) Section 1.1.6.1 is acceptable with the understanding that the NASA Management Office shall review and concur upon any Center contract or agreement that includes aviation operations.

(ii) Section 1.1.6.2 is not applicable.

(iii) Chapter 2 is not applicable.

(iv) Chapter 3 is not applicable.

(v) Chapter 4 is not applicable.

(vi) Section 6.3.1.9 is accepted with the understanding that all safety and emergency response at the Goldstone Deep Space Communications Complex airstrip are performed by NASA and U.S. Army, Ft Irwin.

(vii) Section 6.4.1.a.b.c is not applicable.

(viii)Section 7.2.4 is accepted with the understanding that medical screening may be conducted by a non-NASA MD for qualified non-crew members. The screening will be accomplished by a medical authority authorized to operate at the JPL Federal facility.

(xi) Chapter 8 is not applicable.

(x) Chapter 9 is not applicable.

(xi) Chapter 12 is not applicable.

(xii) Sections 13.3.1–13.3.1.3 are accepted with the understanding that all safety and emergency response at the Goldstone Deep Space Communications Complex airstrip are performed by NASA and the U.S. Army, Ft. Irwin.

The Contractor will be responsible to ensure that a sufficiently detailed risk analysis of the flight program/project is conducted and provided to *DFRC* for review and approval for flight airworthiness that meets the NASA operations safety standards.

H-51 TRANSPORTATION EFFICIENCY

(a) Transportation Efficiency. The Contractor shall comply with the Federal fleet and transportation efficiency goals and requirements as follows. The Contractor shall:

(1) Reduce the fleet's total consumption of petroleum products by two percent annually through the end of fiscal year 2015 using fiscal year 2005 as the baseline.

(2) Increase the total fuel consumption that is non-*petroleum-based* by ten percent annually.

(3) Use plug-in-hybrid (PIH) vehicles when PIH vehicles are commercially available at a cost reasonably comparable, on the basis of life-cycle cost, to non-PIH vehicles.

(4) Provide annual reports on acquisition and use of Government-owned vehicles using the Federal Automotive Statistical Tool (FAST) web-based reporting tool, not later than October 15th of each calendar year in accordance with NFS 1852.223-76, Federal Automotive Statistical Tool Reporting (July 2003).

H-52 RESERVED

H-53 LIMITATION OF FUTURE CONTRACTING

(a) The Government and the Contractor understand that JPL personnel will be allowed access to Government and supplier data, including sensitive and proprietary data, and to Government employees and facilities beyond that which is common to the normal contractual relationship. Because of this special relationship, activities under this Contract may result in organizational conflicts of interest. The Contractor agrees to take affirmative measures to mitigate and avoid such conflicts, and have full disclosure of its affairs to NASA. The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest.

(b) The nature of this conflict may include, but is not limited to:

(1) The Contractor provides advisory and assistance services in assisting NASA in the review, selection, award, and monitoring of Announcements of Opportunity, NASA Research Announcements, and other Broad Agency Announcements.

(2) The Contractor provides advisory and assistance services to NASA in program and project management roles (e.g., NASA program lead, NASA project lead), which

includes program and project planning that may result in subsequent competitive acquisition of supplies and services.

(3) The Contractor provides advisory and assistance services in assisting NASA in other decision-making roles (e.g., export control; energy management; education/outreach; and NASA's SBIR program)

(4) The Contractor manages the Research and Technology (RNA) program and the Caltech streamlined subcontracting process for the award of observation time on programs such as the Spitzer Space Telescope (SST). The Contractor may be tasked with similar roles for other programs in the future.

(5) The Contractor has access to technical and business information that should not be disclosed to outside interests.

(6) The Contractor has access to NASA internal technical and business information.

(7) The Contractor may hold financial interests in organizations that it conducts business with.

Due to the circumstances set forth above, the Contractor might be in a position to favor its own products or capabilities and/or may have an unfair competitive advantage.

(c) Based upon these roles performed by the Contractor, restrictions upon future contracting are set forth as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop complete specifications or statements of work that are to be incorporated into a Government solicitation for non-developmental items, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing NASA contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with other companies. Evaluation of proposal information will be governed by Article H-12, Handling, Protection and Release of Restricted Information, Paragraph 4.

(3) The Contractor is required to have written Conflict of Interest procedures subject to approval and periodic audit by the Government. The written procedures shall address policies to eliminate or mitigate potential conflicts as set forth in paragraph (b) above and any other potential conflicts that may be identified by the Contracting Officer during performance of the Contract.

(4) For tasks that may result in subsequent competitive acquisition of developmental items (e.g., flight hardware), a written conflict of interest avoidance plan will be developed as part of the task plan for the work effort and will be approved by NASA prior to

initiation of the task. Although NASA may identify potential conflicts to the Contractor prior to initiation of the task, it is incumbent upon the Contractor to review the work to be performed under the task to identify potential conflicts. Conflict of interest avoidance plans will contain the following elements:

(i) A description of the potential conflict of interest.

(ii) A written management plan (i.e., organizational conflict of interest avoidance and mitigation plan) to avoid or mitigate the conflict of interest, including the organizational controls that will be put in place to ensure effective separation of organizational units that may be involved in planning and determining requirements from those organizations that may be involved in proposing for such work efforts.

(iii) The requirement that personnel who will be involved in planning and determining requirements for tasks where a potential conflict of interest exists will be required to sign a non-disclosure agreement attesting that they will not be involved in working on a proposal in response to any solicitation resulting from the task, and that they will not talk or provide information about the task to anyone who has not signed the non-disclosure agreement. The written non-disclosure agreements will be kept on file by the program or project manager and will be available for NASA's inspection.

(iv) The requirement that the responsible official (e.g., program or project manager) will maintain a comprehensive list of all persons with access to information about the task and each person's organizational affiliation.

(v) The requirement that persons involved in planning and determining requirements for tasks will be required to answer questions and provide additional information related to a subsequent procurement actions only through the procedures set forth by the JPL contracting organization, allowing equal access to information by all potential offerors.

(vi) The names of persons in the organization, by specific job title, who will be responsible for ensuring that the conflict of interest avoidance plan is followed.

(vii) Signature of the plan by the responsible official.

(viii) Approval of the plan by the Contracting Officer prior to initiation of the task. For conflicts that are not identified until after initiation of the task, the potential conflict will be identified immediately to the Contracting Officer, who will determine the timeframe for approval of the plan and any restrictions for immediate implementation prior to the plans formal approval.

H-54 ADVANCE PAYMENTS

In applying I-11, Advance Payments (FAR 52.232-12)(MAY 2001) (Alternate II) (MAY 2001) (Alternate IV) (APR 1984),(Alternate V) (MAY 2001) as modified by NFS 1852.232-70 (MAR

2010) (Deviation), delivery of the Contractor's annual audited financial statements to the Contracting Officer shall be deemed to satisfy the requirements of paragraph (j)(1); and paragraphs (l) and (m) shall not be deemed to take effect (nor shall the specific amounts in paragraph (m) be determined) unless and until, with Contracting Officer approval, an advance payment is taken for estimated costs for future work to be performed under this Contract and such paragraphs shall remain in effect only until that advance payment has been fully utilized for contract performance or refunded.

Advance Payments to Subcontractors

(1) The Contractor shall not use funds provided by the LOC to make advance payments to its subcontractors, other than commercial advance payments in accordance with FAR 32.2 or those described in item (2) below, without the approval of the Contracting Officer.

(2) The Contractor may provide advance payments in the following instances, but only where such payments are common practice in the industry and are required by the vendor for all customers: subscriptions to periodicals; conference sponsorship/ registration fees; purchase of office equipment; rentals/leases of commercial equipment; and software maintenance agreements. Other than as described in the first sentence, commercial subcontractors shall not be paid advance payments greater than 15% of the subcontract price.

(3) When advance notice or written consent is required by the terms of Clause I-5, Subcontracts (FAR 52.244-2)(OCT 2010)(ALT I)(JUN 2007)(Deviation), the Contractor shall not use advance payments for non-commercial items until such advance notification has been provided and written subcontract consent has been received.

H-55 LIABILITY FOR SUBCONTRACTOR'S DEFECTIVE COST OR PRICING DATA

Clause 52.215-10, Price Reduction For Defective Cost or Pricing Data (AUG 2011) (Mod 6) is incorporated into the Contract with the understanding that while it may render the Contractor liable under the terms of the clause for the certifications of its subcontractors, the clause does not require, by its terms, that the Contractor submit a Certificate of Current Cost or Pricing Data under this Contract.

H-56 REQUIREMENT FOR INFORMATION TECHNOLOGY BUDGET PLAN

(a) On an annual basis, the Contractor shall prepare an Information Technology (IT) Budget Plan for presentation to the NASA Chief Information Officer (CIO). The Budget Plan shall describe all expenditures for operation of and modifications to the JPL IT infrastructure, as well as initiatives for research, applied research, or engineering of new IT solutions related to the JPL IT infrastructure, proposed for the fiscal year. IT infrastructure is defined here to be the data and telecommunications networks, telecommunications systems, servers, services, application software systems, commercial off-the-shelf software, personnel, and all other IT resources that are shared across multiple JPL task orders.

(b) Any content modifications to the IT Budget Plan must be submitted to the NASA CIO.

H-57 RESERVED.

H-58 MONTHLY PROPERTY FINANCIAL REPORTING

(a) The Contractor shall provide monthly property financial reports, electronically submitted, using the Contractor-Held-Asset Tracking System (CHATS) in the format described in the CHATS user's manual. Monthly property financial reports shall be submitted with item level supporting data. This data shall be submitted for all items with an acquisition cost of $100,000 or more, in the Contractor's and subcontractors' possession, in the following classifications: real property, equipment, special test equipment, special tooling, and agency peculiar property. Monthly reporting is not required for property in the above classifications with an acquisition cost under $100,000. Monthly data shall also be submitted for items of any acquisition cost in the classifications of materials, construction in progress (CIP), and contract work-in-process (CWIP). Itemized monthly data is required for materials and WIP line items of $100,000 and over. Summary monthly data is required for materials line items under $100,000. For CIP and CWIP the total cost regardless of values will be reported.

(b) Acquisition costs should be developed using actual costs to the greatest extent possible, especially costs directly related to fabrication such as labor and materials. Supporting documentation shall be maintained and available for all amounts reported, including any amounts developed using estimating techniques.

(c) Adjustments shall be thoroughly explained and directly related to a specific fiscal year. If the fiscal year cannot be determined the default shall be the previous fiscal year.

(d) Contractor acquired property (CAP), CWIP, and any new materials acquired will be reported to the Task Order defined WBS structure and not a separate WBS structure.

(e) The Monthly reports are due the 21st day of the month following the calendar month to be reported.

(f) The Monthly reports required by this clause are separate from and in addition to the annual NF1018 reports required under Article G-2 of this Contract.

H-59 AMERICAN RECOVERY AND REINVESTMENT ACT ("RECOVERY ACT")

(a) The following provisions are applicable only to any non-construction Task Order which specifically states that it is funded in whole or in part by the American Recovery and Reinvestment Act of 2009 (or Recovery Act), thereby invoking this Clause H-59:

(1) FAR 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010)

(2) FAR 52.204-11, American Recovery and Reinvestment Act—Reporting Requirements (JUL 2010)

(3) FAR 52.215-2, Audit and Records – Negotiation (Oct 2010)(ALT I) (MAR 2009) (ALT II)(APR 1998)

(b) Recovery Act funded Task Orders for Construction – Reserved.

H-60 SYSTEMS ENGINEERING

NPR 7123.1A, NASA Systems Engineering Processes and Requirements, dated March 26, 2007, with change 1, dated November 4, 2009, will be implemented predicated on the following conditions:

(a) NPR 7123.1A applies to Task Orders issued after March 9, 2012, for the delivery of new missions and projects. NPR 7123.1A also applies to ongoing Task Orders for the delivery of missions and projects provided the missions/projects were prior to Key Decision Point C on March 9, 2012.

(b) Section 3.1.2.4—The term "NASA workforce" is understood to mean "NASA or the Contractor's workforce".

(c) Chapter 4—This is accepted with the understanding that the responsibilities defined within apply to the positions of those Contractor employees performing the specified functions or subcontractors performing such functions.

(d) Sections 5.3.1.3, 5.3.1.5, 5.3.1.6, and 5.3.1.7 are acceptable subject to the text "in accordance with the review entry and success criteria defined in tables . . . of Appendix G" being understood to mean "as guided by the review entry and success criteria in tables . . .of Appendix G."

(e) Section 6.2.2 is accepted with the understanding that the content of Appendix D, Systems Engineering Management Plan, is for guidance purposes in developing a SEMP.

(f) Sections 6.2.2 and 6.2.4—The Contractor shall create the SEMP baseline as early in Phase B as reasonably feasible for two-step AO-driven projects and missions and as early in Phase A as is reasonably feasible for all other projects and missions.

H-61 SOFTWARE ENGINEERING REQUIREMENTS

NPR 7150.2A, NASA Software Engineering Requirements, dated November 19, 2009, is incorporated with the following understandings:

(a) NPR 7150.2A applies to software created or acquired as Class A, B, and C as defined in Appendix E, Software Classifications. These requirements also apply to Class D software to be used in space, or to support operations of space assets. NPR 7150.2A also applies to software created or acquired for use by other NASA Centers or other NASA organizations regardless of the software classification. NPR 7150.2A is not applicable to software not included in the description above.

(b) NPR 7150.2A applies to new Task Orders for the delivery of missions and projects, and to ongoing Task Orders for the delivery of missions and projects provided the missions/projects are prior to Key Decision Point C and/or Preliminary Design Review on October 1, 2010.

H-62 NON-APPLICABILITY OF LOWER-TIER DOCUMENTS

Documents referenced in or linked from incorporated NPRs, NPDs and all other documents within this Contract are not applicable as requirements for the Contractor unless they are expressly incorporated into the Contract.

H-63 RESPONSIBILITIES OF CONTRACTOR PERSONNEL

The responsibilities defined within NPRs, NPDs and NIDs incorporated into this Contract for the Center personnel, up to and including the Center Director, are understood to apply to the positions of those Contractor employees performing the specified functions.

H-64 FLIGHT PROJECTS PRODUCT DATA MANAGEMENT

The Contractor shall maintain institutional processes and systems for creating, maintaining and controlling data on flight projects. Each flight project shall develop a plan demonstrating how institutional processes and systems shall be implemented on the project. The plan shall be updated and delivered to the sponsoring NASA Program/Project Office at every Key Decision Point (KDP) as defined in NPR 7120.5E draft, dated January 31, 2012 and the plan shall be assessed at every Key Decision Point (KDP) as defined in NPR 7120.5E draft, dated January 31, 2012 and updated as required. Updates shall be delivered to the sponsoring NASA Program/ Project Office.

H-65 IMPLEMENTATION OF FAR 52.222-54, EMPLOYMENT ELIGIBILITY VERIFICATION (JAN 2009)

FAR 52.222-54, “Employment Eligibility Verification”, dated January 2009, is incorporated into this Contract with the following understanding: The Contractor’s completion of a background investigation and issuance of credentials pursuant to Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, of their employees at JPL is deemed to satisfy the requirements of this clause. This clause shall be inserted in all lower-tier subcontracts where the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal Information System.

H-66 POST-RETIREMENT BENEFITS LIABILITY RE-OPENER CLAUSE

Notwithstanding any other Contract provision herein, the Contract will be re-opened at the Government’s discretion for the sole purposes of negotiating and implementing a plan that reduces or liquidates existing unfunded liabilities for Post-Retirement Benefits (PRB) that may have accumulated in prior Contracts between the Parties relative to the operation of the Jet Propulsion Laboratory (JPL). The Parties agree to use best efforts to negotiate and implement a plan that reduces or liquidates existing unfunded liabilities for PRBs no later than September 30, 2012, or another date mutually agreed upon by the Parties.

Further, the Parties agree as follows:

a) By August 30, 2012, the Contractor shall provide to the Contracting Officer a written plan identifying the estimated accumulated PRB liability as of October 1, 2012, (the "Initial Base") with underlying actuarial assumptions, and a description of the methodology to fund the PRB liability and the process to implement it, including any required changes to the Contractor's accounting system or disclosure statement.

b) The Initial Base amount of the total accumulated unfunded PRB liability will be adjusted within two weeks of implementation of the plan and may only be revised based on changes in the yearly actuarial assumptions or market conditions. The Contractor shall submit, no sooner than March 1st but no later than May 1st of each calendar year, a written briefing to the Contracting Officer identifying the changes, if any, in the yearly actuarial assumptions or market conditions. NASA reserves the right to audit or review the actuarial assumptions or market conditions at any time.

c) Any terms, conditions, or clauses contained in the Contract that are impacted by the resulting agreement shall be modified accordingly.

d) All terms and conditions of the resulting agreement shall be clearly documented in writing and incorporated into the Contract.

H-67 RESERVED

H-68 CONTRACTOR'S USE OF GOVERNMENT PROPERTY

a) Pursuant to FAR 52.245-9, "Use and Charges" (APR 2012), paragraph (b)(3), for the duration of this Contract, the Contractor is granted authorized use without charge for such work, to use Government property, buildings, and facilities on a rent-free, non-interference basis for the Contractor's research, development, or educational programs and related administration. This authorization benefits NASA as a recipient of knowledge gained or transferred from research and collaboration, independent research and development, and exploration at JPL and all Contractor facilities. The contractor will not acquire property solely for the purposes discussed in this provision. The Contractor will not authorize profit-making subcontract organizations to use government property for commercial purposes.

b) This authorization permits Government property to be used at the Contractor's campus facilities and at other locations. Property will be loaned to these locations, on a non-interference, no charge loan basis, under written procedures, including property and reporting procedures that must be approved by the Contracting Officer. However, Government property that has no use under this Contract will not be retained solely for the Contractor's use, and will be dispositioned in accordance with the property terms of this Contract.

H-69 IMPLEMENTATION OF FAR 52.203-13, CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (APR 2010) (MOD 6)

The parties agree that FAR 52.203-13 pertains solely to this Contract and sole Sponsoring Agreement between the Contractor and the Government for the operation of the Jet Propulsion Laboratory.

H-70 IMPLEMENTATION OF NFS 1852.235-73, FINAL SCIENTIFIC AND TECHNICAL REPORTS (DEC 2006)

NFS 1852.235-73, Final Scientific and Technical Reports, dated December 2006, is incorporated into this Contract with the understanding that paragraphs (a)–(d) are satisfied by the Contractor's task order-level final reports submitted in accordance with Article G-5, Task Ordering Procedure.

[END OF SECTION]

PART II—CONTRACT CLAUSES

SECTION I—CONTRACT CLAUSES

I-1 LISTING OF CLAUSES

This Contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

I. FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1)

CLAUSE NUMBER	DATE	TITLE
52.202-1	JAN 2012	DEFINITIONS
52.203-3	APR 1984	GRATUITIES
52.203-5	APR 1984	COVENANT AGAINST CONTINGENT FEES
52.203-6	SEP 2006	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT
52.203-7	OCT 2010	ANTI-KICKBACK PROCEDURES
52.203-8	JAN 1997	CANCELLATION, RECISSION AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY
52.203-10	JAN 1997	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY
52.203-12	OCT 2010	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS
52.203-13	APR 2010	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (Mod 6)
52.204-2	AUG 1996	SECURITY REQUIREMENTS (ALT 1) (APR 1984)
52.204-4	MAY 2011	PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER
52.204-9	JAN 2011	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL
52.204-10	JUL 2010	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS
52.208-8	APR 2002	REQUIRED SOURCES FOR HELIUM AND HELIUM USAGE DATA
52.209-6	DEC 2010	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT

CLAUSE NUMBER	DATE	TITLE
52.209-9	FEB 2012	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS
52.211-15	APR 2008	DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS
52.215-2	OCT 2010	AUDITS AND RECORDS – NEGOTIATION (ALT I) (MAR 2009) (ALT II) (APR 1998)
52.215-8	OCT 1997	ORDER OF PRECEDENCE - UNIFORM CONTRACT FORMAT
52.215-9	OCT 1997	CHANGES OR ADDITIONS TO MAKE OR BUY PROGRAM
52.215-10	AUG 2011	PRICE REDUCTION FOR DEFECTIVE CERTIFIED COST OR PRICING DATA
52.215-12	OCT 2010	SUBCONTRACTOR CERTIFIED COST OR PRICING DATA
52.215-14	OCT 2010	INTEGRITY OF UNIT PRICES (ALTERNATIVE I) (OCT 1997)
52.215-19	OCT 1997	NOTIFICATION OF OWNERSHIP CHANGES
52.215-23	OCT 2009	LIMITATIONS ON PASS-THROUGH CHARGES (ALT I)(OCT 2009)
52.219-8	JAN 2011	UTILIZATION OF SMALL BUSINESS CONCERNS
52.219-9	JAN 2011	SMALL BUSINESS SUBCONTRACTING PLAN
52.219-16	JAN 1999	LIQUIDATED DAMAGES – SUBCONTRACTING PLAN
52.222-1	FEB 1997	NOTICE TO THE GOVERNMENT OF LABOR DISPUTES
52.222-2	JUL 1990	PAYMENT FOR OVERTIME PREMIUMS
52.222-3	JUN 2003	CONVICT LABOR
52.222-4	JUL 2005	CONTRACT WORK HOURS AND SAFETY STANDARDS ACT – OVERTIME COMPENSATION
52.222-20	OCT 2010	WALSH-HEALY PUBLIC CONTRACTS ACT
52.222-21	FEB 1999	PROHIBITION OF SEGREGATED FACILITIES
52.222-26	MAR 2007	EQUAL OPPORTUNITY
52.222-29	JUN 2003	NOTIFICATION OF VISA DENIAL
52.222-35	SEP 2010	EQUAL OPPORTUNITY FOR VETERANS (ALT I)(DEC 2001) (Mod 6)
52.222-36	OCT 2010	AFFIRMATIVE ACTION FOR WORKERS WITH DISABILITIES (ALT I)(JUN 1998)
52.222-37	SEP 2010	EMPLOYMENT REPORTS ON VETERANS (Mod 6)

CLAUSE NUMBER	DATE	TITLE
52.222-40	DEC 2010	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT
52.222-50	FEB 2009	COMBATING TRAFFICKING IN PERSONS (MOD 6)
52.222-54	JAN 2009	EMPLOYMENT ELIGIBILITY VERIFICATION
52.223-6	MAY 2001	DRUG-FREE WORKPLACE
52.223-7	JAN 1997	NOTICE OF RADIOACTIVE MATERIALS is added with the following information to fill in the blank for paragraph (a): “30 days”
52.223-9	MAY 2008	ESTIMATE OF PERCENTAGE OF RECOVERED MATERIAL CONTENT FOR EPA-DESIGNATED -ITEMS (Mod 6) is added with the following information to complete part (b)(2): (b) The Contractor, on completion of this Contract shall (1) estimate the percentage of the total recovered material used in contract performance, including, if applicable, the percentage of post-consumer material content and (2) submit this estimate to NMO Health, Safety and Environmental manager AND NASA Headquarters (ALT 1)(MAY 2008)
52.223-10	MAY 2011	WASTE REDUCTION PROGRAM
52.223-11	MAY 2001	OZONE-DEPLETING SUBSTANCES
52.223-12	MAY 1995	REFRIGERATION EQUIPMENT AND AIR CONDITIONERS
52.223-18	AUG 2011	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING (Mod 6)
52.224-1	APR 1984	PRIVACY ACT NOTIFICATION
52.224-2	APR 1984	PRIVACY ACT
52.225-1	FEB 2009	BUY AMERICAN ACT – SUPPLIES
52.225-8	OCT 2010	DUTY FREE ENTRY
52.225-11	MAR 2012	BUY AMERICAN ACT – CONSTRUCTION MATERIALS UNDER TRADE AGREEMENTS (Mod 6)
52.225-12	FEB 2009	NOTICE OF BUY AMERICAN ACT REQUIREMENTS – CONSTRUCTION MATERIALS UNDER TRADE AGREEMENTS
52.225-13	JUN 2008	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES
52.226-1	JUN 2000	UTILIZATION OF INDIAN ORGANIZATIONS AND INDIAN-OWNED ECONOMIC ENTERPRISES (Mod 6)
52.227-1	DEC 2007	AUTHORIZATION AND CONSENT (ALTERNATE I) (APR 1984)

CLAUSE NUMBER	DATE	TITLE
52.227-2	DEC 2007	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT
52.227-10	DEC 2007	FILING OF PATENT APPLICATIONS – CLASSIFIED SUBJECT MATTER
52.227-11	DEC 2007	PATENT RIGHTS – OWNERSHIP BY THE CONTRACTOR (ALT IV) (JUN 1989) (Mod 6)
52.227-14	DEC 2007	RIGHTS IN DATA – GENERAL (ALT II) (DEC 2007) (ALT III) (DEC 2007) FOR ALL TASK ORDERS FOR BASIC OR APPLIED RESEARCH (ALT V) (DEC 2007) AS MODIFIED BY NASA FAR SUPPLEMENT 1852.227-14 FOR ALL TASK ORDERS NOT FOR BASIC OR APPLIED RESEARCH
52.227-16	JUN 1987	ADDITIONAL DATA REQUIREMENTS
52.228-7	MAR 1996	INSURANCE--LIABILITY TO THIRD PERSONS
52.230-2	OCT 2010	COST ACCOUNTING STANDARDS
52.230-6	JUN 2010	ADMINISTRATION OF COST ACCOUNTING STANDARDS
52.232-9	APR 1984	LIMITATION ON WITHHOLDING OF PAYMENTS (Mod 6)
52.232-17	OCT 2010	INTEREST
52.232-23	JAN 1986	ASSIGNMENT OF CLAIMS
52.232-33	OCT 2003	PAYMENT BY ELECTRONIC FUNDS TRANSFER – CENTRAL CONTRACTOR REGISTRATION
52.233-1	JUL 2002	DISPUTES (ALT I) (DEC 1991)
52.233-3	AUG 1996	PROTEST AFTER AWARD (ALT I) (JUN 1985) (Mod 6)
52.233-4	OCT 2004	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM
52.242-1	APR 1984	NOTICE OF INTENT TO DISALLOW COSTS
52.242-13	JUL 1995	BANKRUPTCY
52.243-2	AUG 1987	CHANGES – COST REIMBURSEMENT (ALT V) (APR 1984)
52.244-5	DEC 1996	COMPETITION IN SUBCONTRACTING
52.244-6	DEC 2010	SUBCONTRACTS FOR COMMERCIAL ITEMS
52.245-1	APR 2012	GOVERNMENT PROPERTY
52.245-9	APR 2012	USE AND CHARGES (Mod 6)
52.246-23	FEB 1997	LIMITATION OF LIABILITY
52.246-24	FEB 1997	LIMITATION OF LIABILITY – HIGH VALUE ITEMS (APPLICABLE TO PROPERTY OTHER THAN REAL PROPERTY)
52.247-1	FEB 2006	COMMERCIAL BILL OF LADING NOTATIONS
52.247-63	JUN 2003	PREFERENCE FOR U.S.-FLAG AIR CARRIERS

CLAUSE NUMBER	DATE	TITLE
52.247-64	FEB 2006	PREFERENCE FOR PRIVATELY OWNED U.S.-FLAG COMMERCIAL VESSELS (ALT I) (APR 2003) (Mod 6)
52.247-67	FEB 2006	SUBMISSION OF TRANSPORTATION DOCUMENTS FOR AUDIT (FILL-IN: NMO PROPERTY MANAGER, NASA MANAGEMENT OFFICE, 4800 OAK GROVE DR., M/S 180-801, PASADENA, CA 91109)
52.250-1	APR 1984	INDEMNIFICATION UNDER PUBLIC LAW 85-804 (Mod 6)
52.251-2	JAN 1991	INTERAGENCY FLEET MANAGEMENT SYSTEM VEHICLES AND RELATED SERVICES
52.253-1	JAN 1991	COMPUTER GENERATED FORMS

II. NASA FAR SUPPLEMENT (48 CFR CHAPTER 18) CLAUSES

CLAUSE NUMBER	DATE	TITLE
1852.203-70	JUN 2001	DISPLAY OF INSPECTOR GENERAL HOTLINE POSTERS
1852.216-89	JUL 1997	ASSIGNMENT AND RELEASE FORMS
1852.219-74	SEP 1990	USE OF RURAL AREA SMALL BUSINESSES
1852.219-75	MAY 1999	SMALL BUSINESS SUBCONTRACTING REPORTING
1852.219-76	JUL 1997	NASA 8 PERCENT GOAL
1852.219-77	MAY 2009	NASA MENTOR PROTÉGÉ PROGRAM
1852.219-79	MAY 2009	MENTOR REQUIREMENTS AND EVALUATION
1852.223-74	MAR 1996	DRUG- AND ALCOHOL-FREE WORKFORCE (MOD 6)
1852.223-76	JULY 2003	FEDERAL AUTOMOTIVE STATISTICAL TOOL REPORTING
1852.228-75	OCT 1988	MINIMUM INSURANCE COVERAGE
1852.234-2	NOV 2006	EARNED VALUE MANAGEMENT SYSTEM (ALT I) (NOV 2006)
1852.235-70	DEC 2006	CENTER FOR AEROSPACE INFORMATION
1852.237-70	DEC 1988	EMERGENCY EVACUATION PROCEDURES
1852.242-78	APR 2001	EMERGENCY MEDICAL SERVICES AND EVACUATION
1852.243-71	MAR 1997	SHARED SAVINGS

I-2 INCORPORATION IN FULL TEXT

The following clauses are incorporated in full text because they require insertion of supplementary information or are deviations.

I-3 CLAUSES INCORPORATED BY REFERENCE (FAR 52.252-2) (FEB 1998)

This Contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

FAR: https://www.acquisition.gov/Far/

NASA FAR Supplement: http://www.hq.nasa.gov/office/procurement/regs/nfstoc.htm

(End of Clause)

I-4 OMBUDSMAN (NFS 1852.215-84) (NOV 2011) (ALTERNATE I) (JUN 2000)

(a) An ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and contractors during the preaward and postaward phases of this acquisition. When requested, the ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the ombudsman is not to diminish the authority of the contracting officer, the Source Evaluation Board, or the selection official. Further, the ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of formal contract disputes. Therefore, before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommenda-tions to the contracting officer for resolution.

(b) If resolution cannot be made by the contracting officer, interested parties may contact the installation ombudsman, whose name, address, telephone number, facsimile number, and e-mail address may be found at: http://prod.nais.nasa.gov/pub/pub_library/Omb.html. Concerns, issues, disagreements, and recommendations which cannot be resolved at the installation may be referred to the Agency ombudsman identified at the above URL. Please do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the Contracting Officer or as specified elsewhere in this document.

(c) If this is a task or delivery order contract, the ombudsman shall review complaints from contractors and ensure they are afforded a fair opportunity to be considered, consistent with the procedures of the contract.

(End of clause)

I-5 SUBCONTRACTS (FAR 52.244-2) (OCT 2010) (ALT I) (JUNE 2007) (DEVIATION)

(a) Definitions. As used in this clause

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (d) or (e) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that—

(1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or

(2) Is fixed-price and exceeds—

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For contracts awarded by a civilian agency other that the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts: Any subcontract or class of subcontracts identified by the Contracting Officer in writing as selected for special surveillance.

(e) (1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason certified cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) If the Contractor has an approved purchasing system and consent is not required under paragraph (c), (d), or (e) of this clause, the Contractor nevertheless shall notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract in excess of $1,000,000, or (ii) fixed-price subcontract that exceeds the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of this contract. The notification shall include the information required by paragraphs (e)(1)(i) through (e)(1)(iv) of this clause.

(3) In addition, the Contracting Officer may require special surveillance of any acquisition, class of acquisitions or lease forecast under this contract. This special surveillance may include advance written notification to the Contracting Officer (including any other government official so designated by the Contracting Officer) by the Contractor of key acquisition milestones, briefings to appropriate government personnel on salient features of the acquisition, and the requirement for Government consent on the resulting subcontract.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination—

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(j) Paragraphs (d) and (f) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

(k) Consistent with the requirements of this contract, the Contractor shall establish procurement policies and procedures and conform to good business practice for the guidance of its personnel concerned with the negotiation, administration and termination of subcontracts. Contractor's General Provisions, Additional General Provisions and Standard Alterations which are based on Prime Contract flowdown requirements shall be subject to the approval of the Contracting Officer prior to implementation. Copies of all General Provisions and Additional General Provisions which are not based on Prime Contract flowdown requirements, procurement related policies, and procedures shall be provided to the Contracting Officer at the time of final publication.

(l) The Contractor shall include language in subcontracts (including leases) that allows for the assignment, novation, or transfer of the subcontract to a successor in interest, a successor contractor, or the Government, in the event of (1) a phasedown of the FFRDC; (2) transfer

of the FFRDC to another sponsor; (3) a termination of the contract; or (4) transition of the contract.

(End of Clause)

I-6 SECURITY CLASSIFICATION REQUIREMENTS (NFS 1852.204-75) (SEP 1989)

Performance under this Contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of TOP SECRET. See Federal Acquisition Regulation clause 52.204-2, Security Requirements (AUG 1996) in this Contract and DD Form 254, Contract Security Classification Specification, Attachment F.

I-7 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES, NFS 1852.204-76 (JANUARY 2011) (DEVIATION)

(a) The Contractor shall protect the confidentiality, integrity, and availability of NASA Information and IT resources and protect NASA Information from unauthorized disclosure.

(b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include Controlled Unclassified Information (CUI), for NASA in support of NASA's missions, programs, projects and/or institutional requirements. Applicable requirements are stated in paragraph (e) below.

(c) Definitions.

(1) IT resources means any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

(2) NASA Electronic Information is any data (as defined in the Rights in Data clause of this Contract) or information (including information incidental to contract administration, such as financial, administrative, cost or pricing, or management information) that is processed, managed, accessed or stored on a NASA IT system(s) in the performance of this NASA contract.

(3) IT Security Management Plan—This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this Contract. Unlike the IT security plan, which addresses the IT system, the IT Security Management Plan addresses how the Contractor will manage personnel and processes associated with IT Security on the instant Contract.

(4) IT Security Plan—The IT Security Plan is specific to the IT System and not the contract. The Contractor shall develop IT System Security Plans per the requirements stated in paragraph (e) below. All Contractor personnel requiring physical or logical access to NASA or Contractor IT resources must complete the NASA annual IT Security Awareness training or a Contractor's annual IT Security Awareness training, which is based on the NASA Annual IT Security Awareness Training and industry

resources and is supplemented by JPL-specific needs. The Contractor shall provide a copy of its annual IT Security Training to the NASA OCIO.

(d) The Contractor shall afford Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information contained in databases in accordance with the guidelines regarding Government Records, as outlined in Clause H-16 entitled: "Property Rights in Records." and personnel used in performance of the Contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include results of vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA Electronic Information or to the function of IT systems operated on behalf of NASA, and to preserve evidence of computer crime.

(e) Requirements:

(1) The Contractor shall establish procedures, roles, and responsibilities to implement the specified areas of IT Security.

(2) The Contractor shall protect the confidentiality, integrity, and availability of Contractor information systems in a manner commensurate with their sensitivity, value, and criticality by:

(i) Developing an IT security management plan;

(ii) Authorizing operation and accepting risk through certification and accreditation activities;

(iii) Communicating security responsibilities documented in approved security plans and in rules of behavior;

(iv) Assessing and documenting risk through the identification of potential threats and vulnerabilities, while considering the sensitivity of the information being protected;

(v) Ensuring the security of information systems and services when they are developed, acquired, or when software is installed by users;

(vi) Ensuring users receive the training necessary to perform their functions in a secure manner;

(vii) Managing the security impact of changes to information system configurations;

(viii) Ensuring the availability of resources by limiting the impact of disruptive events through the development of contingency plans, role-specific training, periodic contingency plan testing and updates;

(xi) Minimizing the impact of security incidents through training, testing, timely detection, and mitigation;

(x) Reducing the security risks associated with maintenance activities by managing and documenting when, how, and by whom information systems are maintained;

(xi) Ensuring that information system media are protected against unauthorized access when transported or stored, and by sanitizing media before being discarded or released for reuse;

(xii) Ensuring that only authorized personnel are granted access to facilities housing information systems and their distribution and transmission lines; and mitigating the risk of environmental hazards through emergency systems and the use of alternate work locations;

(xiii) Ensuring that personnel who require access to Contractor information systems have been screened consistent with the risk designation of their position;

(xiv) Protecting the integrity of software and data by detecting and correcting security flaws;

(xv) Preventing unauthorized use of Contractor information systems by providing managed and secure access;

(xvi) Ensuring that sufficient information is captured to reconstruct security-related events through creation, review, and retention of audit and accountability records;

(xvii) Ensuring that access to non-public Contractor information systems will be provided only to verified users and devices; and –

(xviii) Protecting stored, processed, or transmitted information by implementing secure communications, and separation of system services.

(f) The Contractor shall provide via mutually agreed-upon formats, all information required to assist NASA in their FISMA responsibilities.

(g) The Contractor shall report IT security incidents to NASA Security Operations Center (SOC) and collaborate with NASA SOC in investigation and resolution of IT security incidents.

(h) The Contractor shall insert this clause, including this paragraph in all subcontracts that process, manage, access or store NASA Electronic Information in support of the mission of the Agency.

(End of clause)

I-8 RESTRICTION ON FUNDING ACTIVITY WITH CHINA (1852.225-71) (FEB 2012)

(a) Definition - "China" or "Chinese-owned company" means the People's Republic of China, any company owned by the People's Republic of China or any company incorporated under the laws of the People's Republic of China.

(b) Public Laws 112-10, Section 1340(a) and 112-55, Section 539, restrict NASA from contracting to participate, collaborate, coordinate bilaterally in any way with China or a Chinese-owned company using funds appropriated on or after April 25, 2011. Contracts for commercial and non-developmental items are exempted from the prohibition because they constitute purchase of goods or services that would not involve participation, collaboration, or coordination between the parties.

(c) This Contract may use restricted funding that was appropriated on or after April 25, 2011. The Contractor shall not contract with China or Chinese-owned companies for any effort related to this Contract except for acquisition of commercial and non-developmental items. If the Contractor anticipates making an award to China or Chinese-owned companies, the Contractor must contact the Contracting Officer to determine if funding on this Contract can be used for that purpose.

(d) Subcontracts - The Contractor shall include the substance of this clause in all subcontracts made hereunder.

(End of clause) (Mod 6 – [[this Clause is]] effective 60 days from execution of this modification)

I-9 ALLOWABLE COST AND PAYMENT (FAR 52.216-7) (JUN 2011) (DEVIATION)

(a) Contractor Payments. The Government shall make payments to the Contractor as work progresses, by means of withdrawals by the Contractor from a Letter of Credit, as described in Clause B-6 of the Contract, (Contractor financing by Letter of Credit). Such payments shall be in amounts determined to be allowable by the Contracting Officer in accordance with this clause, with Clause B-5 of this contract and with other terms and conditions of this contract. Within fifteen (15) working days after the close of the Contractor's fiscal month the Contractor will submit to the Contracting Officer, a public voucher (i.e., no pay voucher) supported by a statement (using the same major categories of cost reported on in the NF533 reports) of the costs/expenditures made by the Contractor in the performance of this contract during the prior fiscal month and claimed to constitute allowable costs.

(b) Reimbursing costs.

(1) For the purpose of reimbursing allowable costs (except as provided in subparagraph (b)(2) of this clause, with respect to pension, deferred profit sharing, and employee stock ownership plan contributions), the term "costs" includes only—

(i) Those recorded costs that, at the time of the request for reimbursement, the Contractor has paid by cash, check, or other form of actual payment for items or services purchased directly for the contract;

(ii) When the Contractor is not delinquent in paying costs of contract performance in the ordinary course of business, costs incurred, but not necessarily paid, for—

(A) Supplies and services purchased directly for the contract and associated financing payments to subcontractors, provided payments determined due will be made—

(1) In accordance with the terms and conditions of a subcontract or invoice; and

(2) Ordinarily within 30 days of the submission of the Contractor's payment request to the Government;

(B) Materials issued from the Contractor's inventory and placed in the production process for use on the contract;

(C) Direct labor;

(D) Direct travel;

(E) Other direct in-house costs; and

(F) Properly allocable and allowable institutional indirect costs, as shown in the records maintained by the Contractor for purposes of obtaining reimbursement under Government contracts; and

(iii) The amount of financing payments that have been paid by cash, check or other form of payment to subcontractors.

(2) Accrued costs of Contractor contributions under employee pension plans shall be excluded until actually paid unless—

(i) The Contractor's practice is to make contributions to the retirement fund quarterly or more frequently; and

(ii) The contribution does not remain unpaid 30 days after the end of the applicable quarter or shorter payment period (any contribution remaining unpaid shall be excluded from the Contractor's indirect costs for payment purposes).

(3) Any statements in specifications or other documents incorporated in this contract by reference designating performance of services or furnishing of materials at the Contractor's expense or at no cost to the Government shall be disregarded for purposes of cost-reimbursement under this clause.

(c) Small business concerns. A small business concern may receive more frequent payments than every 2 weeks.

(d) Allocated direct costs.

(1) Allowability of the allocated direct costs will be determined in accordance with B-5 of this contract. The Contractor shall promptly respond to any questions concerning allowability and the method(s) used in the collection, control, distribution and accounting of allocated direct costs to the cost objectives of the period, and work with the Contracting Officer to resolve any outstanding issues.

(2) The Contractor and the Contracting Officer shall execute a written understanding setting forth any required changes in the Contractor's methods for the collection, control, distribution and accounting of allocated direct costs. Adjustments to the final allocated direct costs or its distribution to the cost objective of the period in question shall be accomplished if those amounts would have had a material effect upon the costs of the period. Any adjustments shall be accomplished by the Contractor in the current period, consistent with NASA's accounting requirements.

(3) Questions concerning the allowability of any final allocated direct costs which cannot be resolved by the Contracting Officer and the Contractor shall be deemed to be a dispute within the meaning of the Disputes clause.

(e) Quick-closeout procedures. Quick-closeout procedures are applicable when the conditions in FAR 42.708(a) (June 30, 2011) are satisfied.

(f) Audit. At any time or times before final payment, the Contracting Officer may have the Contractor's invoices or vouchers and statements of cost audited. Any payment may be—

(1) Reduced by amounts found by the Contracting Officer not to constitute allowable costs; or

(2) Adjusted for prior overpayments or underpayments.

(g) Final payment.

(1) The Contractor shall submit a completion invoice or voucher designated as such and a final SF1034 to close the Letter of Credit, promptly upon closeout of all task orders under this contract. Upon approval of a completion invoice or voucher submitted by the Contractor in accordance with this clause, and upon the Contractor's compliance with all terms of this contract, the Government shall promptly pay any balance of allowable costs and that part of the fee (if any) not previously paid.

(2) The Contractor shall pay to the Government any refunds, rebates, credits, or other amounts (including interest, if any) accruing to or received by the Contractor or any assignee under this contract, to the extent that those amounts are properly allocable to costs for which the Contractor has been reimbursed by the Government. Reasonable expenses incurred by the Contractor for securing refunds, rebates, credits, or other

amounts shall be allowable costs if approved by the Contracting Officer. Before final payment under this contract, the Contractor and each assignee whose assignment is in effect at the time of final payment shall execute and deliver—

(i) An assignment to the Government, in form and substance satisfactory to the Contracting Officer, of refunds, rebates, credits, or other amounts (including interest, if any) properly allocable to costs for which the Contractor has been reimbursed by the Government under this contract; and

(ii) A release discharging the Government, its officers, agents, and employees from all liabilities, obligations, and claims arising out of or under this contract, except—

(A) Specified claims stated in exact amounts, or in estimated amounts when the exact amounts are not known;

(B) Claims (including reasonable incidental expenses) based upon liabilities of the Contractor to third parties arising out of the performance of this contract; provided, that the claims are not known to the Contractor on the date of the execution of the release, and that the Contractor gives notice of the claims in writing to the Contracting Officer within 6 years following the release date or notice of final payment date, whichever is earlier; and

(C) Claims for reimbursement of costs, including reasonable incidental expenses, incurred by the Contractor under the patent clauses of this contract, excluding, however, any expenses arising from the Contractor's indemnification of the Government against patent liability.

(End of Clause)

I-10 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (EDUCATIONAL AND OTHER NONPROFIT INSTITUTIONS)(FAR 52.249-5) (SEP 1996) (DEVIATION)

(a) The Government may terminate performance of work under this contract in whole or, from time to time, in part if the Contracting Officer determines that a termination is in the Government's interest. The Contracting Officer shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date.

(b) After receipt of a Notice of Termination and except as directed by the Contracting Officer, the Contractor shall immediately proceed with the following obligations:

(1) Stop work as specified in the notice.

(2) Place no further subcontracts or orders (referred to as subcontracts in this clause), except as necessary to complete the continued portion of the contract.

(3) Terminate all applicable subcontracts and cancel or divert applicable commitments covering personal services that extend beyond the effective date of termination.

(4) Assign to the Government, as directed by the Contracting Officer, all right, title, and interest of the Contractor under the subcontracts terminated, in which case the Government shall have the right to settle or pay any termination settlement proposal arising out of those terminations.

(5) With approval or ratification to the extent required by the Contracting Officer, settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts, the cost of which would be reimbursable in whole or in part, under this contract, approval or ratification will be final for purposes of this clause.

(6) Transfer title (if not already transferred) and, as directed by the Contracting Officer, deliver to the Government any information and items that, if the contract had been completed, would have been required to be furnished, including—

(i) Materials or equipment produced, in process, or acquired for the work terminated; and

(ii) Completed or partially completed plans, drawings, and information, and

(7) Complete performance of the work not terminated.

(8) Take any action that may be necessary, or that the Contracting Officer may direct, for the protection and preservation of the property related to this contract that is in the possession of the Contractor and in which the Government has or may acquire an interest.

(9) Use its best efforts to sell, as directed or authorized by the Contracting Officer, termination inventory other than that retained by the Government under subparagraph (b)(6) of this clause; *provided, however*, that the Contractor

(i) is not required to extend credit to any purchaser and

(ii) may acquire the property under the conditions prescribed by, and at prices approved by, the Contracting Officer.

The proceeds of any transfer or disposition will be applied to reduce any payments to be made by the Government under this contract, credited to the price or cost of the work, or paid in any other manner directed by the Contracting Officer.

(c) The Contractor shall submit complete termination inventory schedules no later than 120 days from the effective date of termination, unless extended in writing by the Contracting Officer upon written request of the Contractor within this 120-day period.

(d) After termination, the Contractor shall submit a final termination settlement proposal to the Contracting Officer in the form and with the certification prescribed by the Contracting

Officer. The Contractor shall submit the proposal promptly but no later than 1 year from the effective date of termination unless extended in writing by the Contracting Officer upon written request of the Contractor within this 1-year period. If the Contractor fails to submit the termination settlement proposal within the time allowed, the Contracting Officer may determine, on the basis of information available, the amount, if any, due the Contractor because of the termination and shall pay the amount determined.

(e) Subject to paragraph (d) of this clause, the Contractor and the Contracting Officer may agree upon the whole or any part of the amount to be paid because of the termination. This amount may include reasonable cancellation charges incurred by the Contractor and any reasonable loss on outstanding commitments for personal services that the Contractor is unable to cancel; *provided* that the Contractor exercised reasonable diligence in diverting such commitments to other operations. The contract shall be amended and the Contractor paid the agreed amount.

(f) If the Contractor and the Contracting Officer fail to agree in whole or in part on the amount of costs and/or fee to be paid because of the termination of work, the Contracting Officer shall determine, on the basis of information available, the amount, if any, due the Contractor, and shall pay that amount, which shall include the following:

(1) All costs reimbursable under this contract, not previously paid, for the performance of this contract before the effective date of the termination, and those costs that may continue for a reasonable time with the approval of or as directed by the Contracting Officer; however, the Contractor shall discontinue those costs as rapidly as practicable.

(2) The cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the contract if not included in subparagraph (f)(1) of this clause.

(3) The reasonable costs of settlement of the work terminated, including—

(i) Accounting, legal, clerical, and other expenses reasonably necessary for the preparation of termination settlement proposals and supporting data;

(ii) The termination and settlement of subcontracts (excluding the amounts of such settlements); and

(iii) Storage, transportation, and other costs incurred, reasonably necessary for the preservation, protection, or disposition of the termination inventory.

(4) A portion of the fee payable under the contract, determined as follows:

(i) If the contract is terminated for the convenience of the Government, the settlement shall include a percentage of the fee equal to the percentage of completion of work contemplated under the contract, but excluding subcontract effort included in subcontractors' termination proposals, less previous payments for fee.

(5) If the settlement includes only fee, it will be determined under subparagraph (f)(4) of this clause.

(g) The cost principles and procedures in Article B-5 of this contract and Subpart 31.2 of the Federal Acquisition Regulation (FAR), in effect on the date of the Contract, shall govern all costs claimed, agreed to, or determined under this clause.

(h) The Contractor has the right of appeal as provided under the Disputes clause, except that if the Contractor failed to submit the termination settlement proposal within the time provided in paragraph (d) of this clause and failed to request a time extension, there is no right of appeal.

(i) The Contractor and Contracting Officer must agree to any equitable adjustment in fee for the continued portion of the contract when there is a partial termination. The Contracting Officer shall amend the contract to reflect the agreement.

(j) (1) The Government may, under the terms and conditions it prescribes, make partial payments against costs incurred by the Contractor for the terminated portion of this contract, if the Contracting Officer believes the total of these payments will not exceed the amount to which the Contractor will be entitled.

(2) If the total payments exceed the amount finally determined to be due, the Contractor shall repay the excess to the Government upon demand, together with interest computed at the rate established by the Secretary of the Treasury under 50 U.S.C. APP. 1215(b)(2). Interest shall be computed for the period from the date the excess payment is received by the Contractor to the date the excess is repaid. Interest shall not be charged on any excess payment due to a reduction in the Contractor's termination settlement proposal because of retention or other disposition of termination inventory until 10 days after the date of the retention or disposition, or a later date determined by the Contracting Officer because of the circumstances.

I-11 ADVANCE PAYMENTS (FAR 52.232-12) (MAY 2001) (ALT II) (MAY 2001) (ALT IV) (APR 1984) (ALT V) (MAY 2001) AS MODIFIED BY NFS 1852.232-70 (MAR 2010) (DEVIATION)

(a) Requirements for payment. Advance payments will be made under this contract under a letter of credit. The Contractor shall withdraw cash only when needed for disbursements acceptable under this contract and report cash disbursements and balances as required by the administering office. The Contractor shall apply terms similar to this clause to any advance payments to subcontractors.

(b) Use of funds. The Contractor may use advance payment funds only to pay for properly allocable, allowable, and reasonable costs for direct materials, direct labor, indirect costs, or such other costs approved in writing by the administering contracting office. Payments are subject to any restrictions in other clauses of this contract. Determinations of whether costs are properly allocable, allowable, and reasonable shall be in accordance with generally accepted accounting principles, subject to any applicable Subparts of Part 31 of the Federal Acquisition Regulation.

(c) Repayment to the Government. At any time, the Contractor may repay all or any part of the funds advanced by the Government. Whenever requested in writing to do so by the administering office, the Contractor shall repay to the Government any part of unliquidated advance payments considered by the administering office to exceed the Contractor's current requirements.

(d) Maximum payment. Unliquidated advance payments, unpaid interest charges, and other payments shall not exceed $100,000,000 (not including fixed-fee, if any) at any time outstanding for the work under this Contract, or the Government may withhold further payments to the Contractor. Upon completion or termination of the Contract, the Government shall deduct from the amount due to the Contractor all unliquidated advance payments and interest charges payable. The Contractor shall pay any deficiency to the Government upon demand.

(e) Interest. No interest shall be charged to the prime Contractor for advance payments, except during a period of withholding of advance payment as described in (h) below. The terms of this paragraph concerning interest charges for advance payments shall not apply to the prime Contractor.

(1) The Contractor shall pay interest to the Government on the daily unliquidated advance payments at the daily rate specified in paragraph (e)(3) of this clause. Interest shall be computed at the end of each calendar month for the actual number of days involved. For the purpose of computing the interest charge, the following shall be observed:

(i) Advance payments shall be considered as increasing the unliquidated balance as of the date of the advance payment check.

(ii) Repayments by Contractor check shall be considered as decreasing the unliquidated balance as of the date on which the check is received by the Government authority designated by the Contracting Officer.

(iii) Liquidations by deductions from payments to the Contractor shall be considered as decreasing the unliquidated balance as of the dates on which the Contractor presents to the Contracting Officer full and accurate data for the preparation of each Letter of Credit draw. Credits resulting from these deductions shall be made upon the processing of the Letter of Credit draw through the Department of Health and Human Services—Payment Management System (DHHS/PMS) based upon the Contracting Officer's certification of the applicable dates.

(2) Interest charges resulting from the monthly computation shall be deducted from any payments on account of the fixed-fee due to the Contractor. If the accrued interest exceeds the payment due, any excess interest shall be carried forward and deducted from subsequent payments of the contract price or fixed-fee. Interest carried forward shall not be compounded. Interest on advance payments shall cease to accrue upon (i) satisfactory completion or (ii) termination of the Contract for the convenience of the Government. The Contractor shall charge interest on advance payments to subcontractors in the manner described above and credit the interest to the Government.

Interest need not be charged on advance payments to nonprofit educational or research subcontractors for experimental, developmental, or research work.

(3) If interest is required under this Contract, the Contracting Officer shall determine a daily interest rate based on the rate established by the Secretary of the Treasury under Pub. L. 92-41 (50 U.S.C. App., 1215(b)(2)). The Contracting Officer shall revise the daily interest rate during the contract period in keeping with any changes in the cited interest rate.

(f) Lien on property under contract.

(1) All advance payments under this Contract, together with interest charges, shall be secured, when made, by a lien in favor of the Government, paramount to all other liens, on the supplies or other things covered by this Contract and on all material and other property acquired for or allocated to the performance of this Contract, except to the extent that the Government by virtue of any other terms of this Contract, or otherwise, shall have valid title to the supplies, materials, or other property as against other creditors of the Contractor.

(2) The Contractor shall identify, by marking or segregation, all property that is subject to a lien in favor of the Government by virtue of any terms of this Contract in such a way as to indicate that it is subject to a lien and that it has been acquired for or allocated to performing this contract. If, for any reason, the supplies, materials, or other property are not identified by marking or segregation, the Government shall be considered to have a lien to the extent of the Government's interest under this Contract on any mass of property with which the supplies, materials, or other property are commingled. The Contractor shall maintain adequate accounting control over the property on its books and records.

(3) If, at any time during the progress of the work on the contract, it becomes necessary to deliver to a third person any items or materials on which the Government has a lien, the Contractor shall notify the third person of the lien and shall obtain from the third person a receipt in duplicate acknowledging the existence of the lien. The Contractor shall provide a copy of each receipt to the Contracting Officer.

(4) If, under the termination clause, the Contracting Officer authorizes the contractor to sell or retain termination inventory, the approval shall constitute a release of the Government's lien to the extent that-

(i) The termination inventory is sold or retained; and

(ii) The sale proceeds or retention credits are applied to reduce any outstanding advance payments.

(g) Insurance.

(1) The Contractor shall maintain with responsible insurance carriers-

(i) Insurance on plant and equipment against fire and other hazards, to the extent that similar properties are usually insured by others operating plants and properties of similar character in the same general locality;

(ii) Adequate insurance against liability on account of damage to persons or property; and

(iii) Adequate insurance under all applicable workers' compensation laws.

(2) Until work under this Contract has been completed and all advance payments made under the Contract have been liquidated, the Contractor shall-

(i) Maintain this insurance;

(ii) Maintain adequate insurance on any materials, parts, assemblies, subassemblies, supplies, equipment, and other property acquired for or allocable to this Contract and subject to the Government lien under paragraph (f) of this clause; and

(iii) Furnish any evidence with respect to its insurance that the administering office may require.

(h) Withholding of advance payments.

(1) If any of the following events occur, the Government may, by written notice to the Contractor, withhold further payments on this Contract:

(i) A finding by the administering office that the Contractor has failed to—

(A) Observe any of the conditions of the advance payment terms;

(B) Comply with any material term of this Contract;

(C) Make progress or maintain a financial condition adequate for performance of this Contract;

(D) Limit inventory allocated to this Contract to reasonable requirements; or

(E) Avoid delinquency in payment of taxes or of the costs of performing this Contract in the ordinary course of business.

(F) Timely comply with the financial reporting requirements in clause B-6(e), will result in an automatic withholding until the late SF-425 is submitted to DHHS/PMS.

(ii) The appointment of a trustee, receiver, or liquidator for all or a substantial part of the Contractor's property, or the institution of proceedings by or against the Contractor for bankruptcy, reorganization, arrangement, or liquidation.

(iii) The commission of an act of bankruptcy.

(2) If any of the events described in paragraph (h)(1) of this clause continue for 30 days after the written notice to the Contractor, the Government may take any of the following additional actions:

(i) Charge interest, in the manner prescribed in paragraph (e) of this clause, on outstanding advance payments during the period of any event described in paragraph (h)(1) of this clause.

(ii) Demand immediate repayment by the Contractor of the unliquidated balance of advance payments.

(iii) Take possession of and, with or without advertisement, sell at public or private sale all or any part of the property on which the Government has a lien under this Contract and, after deducting any expenses incident to the sale, apply the net proceeds of the sale to reduce the unliquidated balance of advance payments or other Government claims against the Contractor.

(3) The Government may take any of the actions described in paragraphs (h)(1) and (h)(2) of this clause it considers appropriate at its discretion and without limiting any other rights of the Government.

(i) Prohibition against assignment. Notwithstanding any other terms of this Contract, the Contractor shall not assign this Contract, any interest therein, or any claim under the Contract to any party.

(j) Information and access to records. The Contractor shall furnish to the administering office (1) monthly or at other intervals as required, signed or certified balance sheets and profit and loss statements, together with Standard Form 425, Federal Financial Report and, (2) if requested, other information concerning the operation of the contractor’s business. The Contractor shall provide the authorized Government representatives proper facilities for inspection of the Contractor’s books, records, and accounts.

(k) Other security. The terms of this contract are considered to provide adequate security to the Government for advance payments; however, if the administering office considers the security inadequate, the Contractor shall furnish additional security satisfactory to the administering office, to the extent that the security is available.

(l) Representations. The Contractor represents the following:

(1) The balance sheet, the profit and loss statement, and any other supporting financial statements furnished to the administering office fairly reflect the financial condition of the Contractor at the date shown or the period covered, and there has been no subsequent materially adverse change in the financial condition of the Contractor.

(2) No litigation or proceedings are presently pending or threatened against the Contractor, except as shown in the financial statements.

(3) The Contractor has disclosed all contingent liabilities, except for liability resulting from the renegotiation of defense production contracts, in the financial statements furnished to the administering office.

(4) None of the terms in this clause conflict with the authority under which the Contractor is doing business or with the provision of any existing indenture or agreement of the Contractor.

(5) The Contractor has the power to enter into this contract and accept advance payments, and has taken all necessary action to authorize the acceptance under the terms of this contract.

(6) The assets of the Contractor are not subject to any lien or encumbrance of any character except for current taxes not delinquent, and except as shown in the financial statements furnished by the Contractor. There is no current assignment of claims under any contract affected by these advance payment provisions.

(7) All information furnished by the Contractor to the administering office in connection with each request for advance payments is true and correct.

(8) These representations shall be continuing and shall be considered to have been repeated by the submission of each Letter of Credit draw for advance payments.

(m) Covenants. To the extent the Government considers it necessary while any advance payments made under this contract remain outstanding, the Contractor, without the prior written consent of the administering office, shall not—

(1) Mortgage, pledge, or otherwise encumber or allow to be encumbered, any of the assets of the Contractor now owned or subsequently acquired, or permit any preexisting mortgages, liens, or other encumbrances to remain on or attach to any assets of the Contractor which are allocated to performing this contract and with respect to which the Government has a lien under this contract;

(2) Sell, assign, transfer, or otherwise dispose of accounts receivable, notes, or claims for money due or to become due;

(3) Declare or pay any dividends, except dividends payable in stock of the corporation, or make any other distribution on account of any shares of its capital stock, or purchase, redeem, or otherwise acquire for value any of its stock, except as required by sinking fund or redemption arrangements reported to the administering office incident to the establishment of these advance payment provisions;

(4) Sell, convey, or lease all or a substantial part of its assets;

(5) Acquire for value the stock or other securities of any corporation, municipality, or Governmental authority, except direct obligations of the United States;

(6) Make any advance or loan or incur any liability as guarantor, surety, or accommodation endorser for any party;

(7) Permit a writ of attachment or any similar process to be issued against its property without getting a release or bonding the property within 30 days after the entry of the writ of attachment or other process;

(8) Pay any remuneration in any form to its directors, officers, or key employees higher than rates provided in existing agreements of which notice has been given to the administering office, accrue excess remuneration without first obtaining an agreement subordinating it to all claims of the Government, or employ any person at a rate of compensation over $(See H-54) a year;

(9) Change substantially the management, ownership, or control of the corporation;

(10) Merge or consolidate with any other firm or corporation, change the type of business, or engage in any transaction outside the ordinary course of the Contractor's business as presently conducted;

(11) Deposit any of its funds except in a bank or trust company insured by the Federal Deposit Insurance Corporation or a credit union insured by the National Credit Union Administration;

(12) Create or incur indebtedness for advances, other than advances to be made under the terms of this contract, or for borrowings;

(13) Make or covenant for capital expenditures exceeding $(See H-54) in total;

(14) Permit its net current assets, computed in accordance with generally accepted accounting principles, to become less than $(See H-54); or

(15) Make any payments on account of the obligations listed below, except in the manner and to the extent provided in this Contract: (See H-54)

(End of Clause)

I-12 LIMITATION OF COSTS (FAR 52.232-20) (APR 1984); LIMITATION OF FUNDS (FAR 52.232-22) (APR 1984) (DEVIATION)

(a) The parties estimate that performance of this contract will not cost the Government more than (1) the estimated cost specified in the Schedule (See B-2) or, (2) if this is a cost-sharing contract, the Government's share of the estimated cost specified in the Schedule. The Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within the estimated cost, which, if this is a cost-sharing contract, includes both the Government's and the Contractor's share of the cost.

(b) Each task order specifies the amount presently available for payment by the Government and allotted to such task order, the items covered, the Government's share of the cost if this is a cost-sharing contract, and the period of performance it is estimated the allotted amount will cover. The parties contemplate that the Government will allot additional funds incrementally to task orders up to the full estimated cost to the Government specified in each task order, exclusive of any fee. The Contractor agrees to perform, or have performed, work on each task order up to the point at which, in the exercise of reasonable judgment by the Contractor, costs incurred by the Contractor in performing work in-house, plus obligations incurred by the Contractor in subcontracting, approximate the amount of funds then allotted, by the Government as specified in each task order.

It is recognized that the point to which the Contractor is required to continue performance does not include an allowance for termination costs which will be incurred in the event the task order is terminated. It is the intention of the Government to allot the additional funds necessary to provide for termination costs to such terminated task order subject to the limitations set forth in paragraph (k) herein and using procedures set forth in Article G-7, (Funds Procedures for Termination of Task Orders).

(c) The Contractor shall notify the Contracting Officer in writing at least fifteen (15) days prior to the date on which, in the reasonable judgment of the Contractor, costs incurred by the Contractor in performing work in-house, plus obligations incurred by the Contractor in subcontracting, will approximate the amount of funds then allotted, by the Government as specified in each task order. The notice shall state the estimated amount of additional funds required to continue performance under the task order to completion or for 3 months whichever is less.

(d) If, after notification, additional funds are not allotted by the end of the period specified in the notification or another agreed-upon date, upon the Contractor's written request the Contracting Officer will terminate the task order on that date in accordance with the provisions of the Termination clause of this contract. If the Contractor estimates that the funds available will allow it to continue to discharge its obligations beyond that date, it may specify a later date in its request, and the Contracting Officer may terminate this contract on that later date.

(e) Except as required by other provisions of this contract, specifically citing and stated to be an exception to this clause-

(1) The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount allotted by the Government to the task order; and

(2) The Contractor is not obligated to continue performance of a task order or otherwise incur costs in excess of—

(i) The amount then allotted to each task order by the Government or;

(ii) If this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, until the Contracting Officer notifies the Contractor in writing that the amount allotted by the

Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to the task order.

(f) The estimated cost shall be increased to the extent that (1) the amount allotted by the Government or, (2) if this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, exceeds the estimated cost specified in the task order. If this is a cost-sharing contract, the increase shall be allocated in accordance with the formula specified in the Schedule.

(g) No notice, communication, or representation in any form other than that specified in paragraph (e)(2) of this clause, or from any person other than the Contracting Officer, shall affect the amount allotted by the Government to a task order. In the absence of the specified notice, the Government is not obligated to reimburse the Contractor for any costs in excess of the total amount allotted by the Government to a task order, whether incurred during the course of the contract or as a result of termination.

(h) When and to the extent that the amount allotted by the Government to the contract is increased, any costs the Contractor incurs before the increase that are in excess of—

(1) The amount previously allotted by the Government or;

(2) If this is a cost-sharing contract, the amount previously allotted by the Government to the Contract plus the Contractor's corresponding share, shall be allowable to the same extent as if incurred afterward, unless the Contracting Officer issues a termination or other notice and directs that that portion of the increase not required for outstanding obligations be used to cover termination or other specified expenses.

(i) Change orders shall not be considered an authorization to exceed the amount allotted by the Government specified in a task order, unless they contain a statement increasing the amount allotted.

(j) Nothing in this clause shall affect the right of the Government to terminate this Contract.

(k) Notwithstanding any other provision in this contract, in the event this contract is terminated in whole or in part pursuant to the Termination clause of this Contract, and the amounts necessary to settle the termination of any one or more task orders will cause the costs incurred under such task order or orders to exceed the amount allotted thereto then, and in that event, the limit of the Government's obligation to reimburse the Contractor for such costs shall be the amount allotted thereto and such other available unobligated funds, as determined by NASA, which may be lawfully used for the payment of such costs. The determination by NASA as to the availability of unobligated funds shall not be subject to appeal by the Contractor under the Dispute clause of this Contract.

(End of clause)

I-13 NOTIFICATION PRIOR TO ACQUIRING INFORMATION TECHNOLOGY SYSTEMS FROM ENTITIES OWNED, DIRECTED OR SUBSIDIZED BY THE PEOPLE'S REPUBLIC OF CHINA, NFS 1852.225-74 (JUNE 2013) (DEVIATION) (from PIC 13-04) (Mod 7)

(a) Definitions –

"Acquire" means procure with appropriated funds by and for the use of NASA through purchase or lease.

"Entity owned, directed or subsidized by the People's Republic of China" means any organization incorporated under the laws of the People's Republic of China.

"Information Technology (IT) System" means the combination of hardware components, software, and other equipment to make a system whose core purpose is to accomplish a data processing need such as the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data. IT systems include ground systems in support of flight hardware. IT systems do not include—

(i) Systems acquired by a contractor incidental to a contract;

(ii) Imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology systems;

(iii) Services in support of IT systems, such as help desk services; or

(iv) Flight hardware, which includes aircraft, spacecraft, artificial satellites, launch vehicles, balloon systems, sounding rockets, on-board instrument and technology demonstration systems, and equipment operated on the International Space Station; as well as prototypes, and engineering or brass boards created and used to test, troubleshoot, and refine air- and spacecraft hardware, software and procedures.

(b) Section 516 of the Consolidated and Further Continuing Appropriation Act, 2013 (Pub. L.113-6), requires NASA's Office of the Chief Information Officer (OCIO) to assess the risk of cyber-espionage or sabotage of an information technology (IT) system that is produced, manufactured, or assembled by an entity owned, directed or subsidized by the People's Republic of China (PRC). The Government retains the right to reject any IT system tendered for acceptance under this Contract, without any further recourse by, or explanation to, the Contractor, if the Government determines the IT system, in whole or in part, presents an unacceptable risk to national security.

(c) The Contractor shall obtain the approval of the Contracting Officer before acquiring any IT system(s) from entities owned, directed or subsidized by the People's Republic of China under this contract. Any Contractor request to use such items shall include adequate information for Government evaluation of the request, including—

(1) A brief description of the item(s); and

(2) Vendor/manufacturer's company name and address;

(d) The Contracting Officer will provide the information referenced in paragraph (c) to the NASA Office of the Chief Information Officer (OCIO) which will assess the risk of cyber-espionage or sabotage and make a determination if the acquisition of such system is in the national interest. Only items so approved shall be provided under the contract.

(End of clause)

NOTE: The above clause is effective 20 days after the bilateral execution [last date signed] of the Modification incorporating it, and is applicable only to subject new IT Systems purchased by the Contractor after that date which use FY 2013 Government funds.

(Mod 7 – Signed on November 12, 2013.)

[END OF SECTION]

PART III—LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J—LIST OF ATTACHMENTS

J-1 LIST OF DOCUMENTS, EXHIBITS, AND ATTACHMENTS

(a) The following documents, exhibits, and attachments are included in the solicitation and resulting Contract. Representations and certifications completed by the Contractor in response to this solicitation are incorporated by reference in the resulting Contract at time of award.

Title	Date	No. of Pages
Attachment A—Foreign Travel		1
Attachment B—NASA-JPL Policies and Procedures Regarding Public Information Programs and New Issuances		3
Attachment C—Bibliography of NASA Directives Contractually Implemented		17
Attachment D—Small Business Subcontracting Plan		16
Attachment E—Contract Data Requirements List (Mod 6)	June 4, 2013	11
Attachment F—DD Form 254		3
Attachment G—Agreement and Conditions for Evaluation of Proposals		1
Attachment H—JPL NPR 1600, NASA Physical and Program Security	May 16, 2012	72
Attachment I—JPL NM 1600-96, Personnel Security	May 16, 2012	17
Attachment J—JPL NPR 1620.2, Facility Security Assessments	October 14, 2011	16
Attachment K—JPL NPR 1620.3, Physical Security Requirements for NASA Facilities and Property	October 14, 2011	106
Attachment L—JPL NPR 1660.1B,Counterintelligence (CI)/ Counterterrorism (CT) Procedural Requirements	October 14, 2011	1
Attachment M—JPL NM 1600-95, ID and Credential Management	May 16, 2012	63
Appendix 1—NASA and Caltech Understanding Concerning the Jet Propulsion Laboratory		4

(End of Clause)

[END OF SECTION]

ATTACHMENT A

FOREIGN TRAVEL

Attachment A covers the coordination, review, and approval of foreign travel by Contractor employees and others (other than employees of subcontractors) on official business where the cost is paid by others or is chargeable to the Contract.

FOREIGN TRAVEL APPROVAL REQUIREMENTS

1. All foreign travel must be reviewed and approved in advance by the Contractor's Director, Deputy Director, Associate Director, or Director for the applicable Contractor Directorate.

2. The Contractor shall:

    a. Submit Country Clearance requests to the appropriate United States Embassy(ies) in advance of all foreign travel.

    b. Provide advance e-mail notice of all Contractor foreign travel to the Office of International and Interagency Relations (OIIR) and to HQ Mission Directorates, as appropriate. Copies of any formal papers or abstracts to be presented shall be included for NASA review and concurrence.

    c. Provide advance e-mail notice to the NMO Contracting Officer of any non-NASA sponsored foreign travel.

    d. Provide a weekly report of all approved foreign travel to OIIR.

    e. Provide trip reports to OIIR, if requested.

3. Contractor travelers are required to receive and acknowledge receipt of a foreign travel awareness information document from JPL Security prior to foreign travel.

4. Contractor travelers are responsible for obtaining appropriate medical clearance, if required, for all foreign travel.

ATTACHMENT B

NASA–JPL POLICIES AND PROCEDURES REGARDING PUBLIC INFORMATION PROGRAMS AND NEWS ISSUANCES

(a) Introduction. Consistent with Section 203 (a) (3) of the Space Act and the Freedom of Information Act (5 USC 552) it is NASA Policy to carry out a public affairs program designed to make available factual and timely information concerning its activities, its programs, and their results. In carrying out its statutory responsibilities NASA encourages its contractors not only to respond to queries from media, but to carry out a positive program of dissemination of factual and timely information relating to work being done for NASA. In doing so, contractors are expected to coordinate their activities with NASA Public Affairs officials. Review and approval of any material submitted to NASA does not constitute approval to expend funds; expenditures for information dissemination and advertising remain subject to applicable cost principles under the Contract.

(b) Applicability. The policies and procedures set forth herein apply to all public affairs activities and news issuances made by JPL or by JPL employees, bearing on work being performed by JPL for the civil aeronautics and space program of the United States. News issuances include information (textual and/or audiovisual) intended for or distributed to the general public (including via the Internet); i.e., to other than the technical and scientific communities. Information disseminated exclusively for internal JPL use is not considered a news issuance. Examples of news issuances include news releases, fact sheets, press kits, transcripts, speech reprints, notes to editors, feature articles, biographics, etc. News issuances do not include educational products and general information disseminated to the public as a part of routine JPL outreach activities. However, such products and information must be consistent with more news-oriented products coordinated through the clearance process for news issuances. House organs published with funds provided under this Contract are considered news issuances only when they are used to disseminate information to external audiences. Guidelines for news issuances by subcontractors of JPL, including lower tier subcontractors, shall be in accordance with guidelines established by the NASA Headquarters Office of Communications.

(c) Clearance Requirements for News Issuances.

(1) Except as otherwise provided in this Contract, information may be released to the public by JPL without prior NASA clearance, subject to the provisions of subparagraph (2) below.

(2) Prior NASA clearance is required for all public releases by JPL involving:

(i) discussion of launch vehicle selections or launch schedules.

(ii) planning, scheduling, and managing major development programs or space flight missions.

(iii) proposed budgets and financial plans.

(iv) proposed organization of effort for the execution of NASA programs, including management of projects and plans for use of NASA prime contractors or subcontractors.

(v) information on projects for which a NASA Center or an outside agency has the primary responsibility, except that this shall not be construed as a limitation on speeches or oral statements made by a Director for a Directorate or higher official of the JPL.

(vi) releases having an estimated total cost, including in-house effort, in excess of $10,000; for example, exhibits, films and pamphlets.

(vii) preferred or proprietary arrangements with any particular segment of the information media, publishing or entertainment industries, or any individual elements thereof; provided, however, this requirement in no way limits the Contractor's rights under FAR 52.227-14, Rights in Data—General (ALT II, III, V).

(viii) information on international matters or for release outside the United States.

(ix) information intended for national release, or any information which, because of the nature of the subject matter or timing involved, will, in the opinion of the Director of JPL, be likely to attract more than routine local or regional public interest.

(3) Where prior NASA clearance is required, requests will be directed to the NASA Assistant Administrator for Public Affairs or his designee. Requests will be made in writing, provided, however, that if time is critical, telephone requests may be made.

(4) The Director of JPL will establish guidelines and procedures covering public release of information at JPL. These guidelines and procedures will be consistent with the Space Act and the Freedom of Information Act and will follow the spirit and intent of 14 CFR Part 1213 Subpart 1.

(d) The Public Engagement Plan.

(1) General. Public affairs support of a significant program milestone or event such as a rollout, first flight, launch, space rendezvous/encounter, fly-by, high public-interest mission, etc., generally requires preparation and implementation of a Public Engagement Plan. The Public Engagement Plan sets forth the public affairs support activities, procedures, responsibilities; and the contractor-vs.-government furnished personnel, supplies, equipment, services and funding. Support activities and requirements usually include a combination of, or all of the following; on-site newsroom operation; guest invitations and operations; press conferences; news kits and news releases; still photo, motion picture and video releases; unique equipment and

special supplies; supplemental personnel and transportation; NASA feed to television networks, etc.

(2) Preparation of the Public Engagement Plan. Public Engagement Plans will be prepared by the NASA Office of Public Affairs, with input and assistance from JPL. JPL will respond to requests for assistance in the development of the Public Engagement Plan and assume its operational role and responsibilities upon implementation of the Plan.

(e) Identification of Releases.

(1) All written releases pertaining to NASA programs will identify NASA in a larger format than the JPL and/or the California Institute of Technology.

(2) All substantive releases which pertain to work being sponsored by NASA will clearly reflect this sponsorship and the NASA/Caltech contractual relationship.

ATTACHMENT C

BIBLIOGRAPHY OF NASA DIRECTIVES CONTRACTUALLY IMPLEMENTED

Document	Title and Date of Document	Contract Location
CODE OF FEDERAL REGULATIONS (CFR) (Other than FAR and NFS)		
10 CFR 433*	Federal Energy Efficiency Standards for design and construction	H-9(a)(11)
14 CFR 1212*	Privacy Act—NASA Regulations	H-16(b)(2)
14 CFR Part 1213, Subpart 1*		Attachment B—paragraph (4)(4)
15 CFR Parts 730–799	Export Administration Regulations (EAR)	G-14(b)(1), G-14(c), G-14(h) (Mod 6)
22 CFR Parts 120–130 (including 22 CFR 120.10, 22 CFR 125.4 (b)(3), and 22 CFR 126.4)	International Traffic in Arms Regulations (ITAR)	F-2, F-4(b)(1), F-4(b)(2), F-4(b)(2)(viii), G-14(a), G-14(b)(1), G-14(c), G-14(d), G-14(e), G-14(h) (Mod 6)
36 CFR Part 1194*	Electronic and Information Technology Accessibility Standards	H-43(b)(8)
36 CFR Part 1194.4*	Definitions	H-43(b)(8)
41 CFR 60-2, Subpart B, 41 CFR 60-2.11(b)		G-25(7)
	Federal Travel Regulation (FTR)*	G-23(b)
	Joint Travel Regulation*	G-23(b)
	OSHA Record Keeping Regulations*	H-10(d)(3)
	HIPAA Regulations*	H-10(d)(4)
(Mod 6)		
FAR/NASA FAR SUPPLEMENT—NFS (48 CFR)—Non-Clauses Only		
FAR		
FAR, Generally*		I-5(k)
2.1*, 2.101*	Definitions	H-27(a), I-5(a)

Document	Title and Date of Document	Contract Location
7.5*	Inherently Governmental Functions, Subsection 7.503(c)	C-7
Subpart 8.8	Acquisition of Printing and Related Supplies	H-28(a), H-28(d)
9.503*	Waiver	H-53(c)
9.505-1*	Providing systems engineering and technical direction	H-53(c)
9.505-2*	Preparing specifications or work statements	H-53(c)
9.505-3*	Providing evaluation services	H-53(c)
15.404-4(c)(4)(i)*	Statutory fee limitations	I-5(g)
Part 31, applicable Subparts*		I-11(b)
31.109(c)*	Advance Agreements	B-5(e)(12), B-5(e)(13)(i)
Subpart 31.2*	Contracts with Commercial Organizations	B-5(a), B-5(a)(1), B-5(e)(13)(i), G-23(b), I-10(g)
31.205-18*	Independent research and development and bid and proposal costs	B-5(d)(2)(ii)
31.205-20*	Interest and other financial costs	B-5(e)(12)
Subpart 32.2*	Commercial Item Purchase Financing	H-25, H-54(1)
Subpart 32.5*	Progress Payments Based on Costs	H-25
35.017*	Federally Funded Research and Development Centers	B-1(b)
35.017-1(c)(4)*		G-5(b)(2)(ii)
37.203*	Policy	H-24(a)
37.203(c)*		H-24(b)
42.708(a)*		I-9(e)
Part 44*	Subcontracting Policies and Procedures	I-5(a)
Subpart 44.3*	Contractors' Purchasing System Reviews	I-5(i)
NFS		
NFS, generally*		I-5(k)
1808.003-70, -71, -72, and -73	Required sources of radioisotopes, liquid hydrogen, propellants and mercury	H-41
		(Mod 6)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
1827.305-370*	NASA patent rights and new technology follow-up procedures	G-16(b)
1832.2*	Commercial Item Purchase Financing	H-25
1832.5*	Progress Payments Based on Costs	H-25
1845.7101-1 (NFS)*	Property classification	G-3
CAS		
9903.201-2(b)*		H-30(c)
9904.401*	Consistency in Estimating, Accumulating and Reporting Costs	H-30(c)
9904.402*	Consistency in Allocating Costs Incurred for the Same Purpose	H-30(c)
9904.405*	Accounting for Unallowable Costs	H-30(c)
9904.406*	Cost Accounting Period	H-30(c)
FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)		
FIPS 201-1*	Personal Identification Verification (PIV) of Federal Employees and Contractors dated March, 2006, with change notice 1, dated June 23, 2006	H-36(a)(1)
INDUSTRY STANDARDS AND CODES (Miscellaneous)		
ANSI*	Requirements	H-10(c)
ANSI/AIAA S-080-1998*	Space Systems—Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, dated September 13, 1999	H-7(2).(C)(ix)(g)b., H-7(2).(C)(ix)(h)
ANSI/AIAA S-081-2000*	Space Systems—Composite Overwrapped Pressure Vessels (COPVs), dated January 01, 2001	H-7(2).(C)(ix)(g)b.
ANSI/ESD S20.20-2007*	American National Standard (and Electrostatic Discharge Association)—Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices), dated March 1, 2007	H-7(1).(B)(xii)(e)

Document	Title and Date of Document	Contract Location
ANSI/ISEA Z358.1-2009	American National Standard for Emergency Eyewash and Shower Equipment, dated September 14, 2009	H-7(2).(C)(viii)
ANSI/NCSL Z-540.3-2006*	Requirements for the Calibration of Measuring and Test Equipment, dated August 3, 2006	H-7(1).(E)(x), H-7(1).(E)(x)(a), H-7(1).(E)(x)(b), H-7(1).(E)(x)(c)
ISO 9001*	Quality Management Systems—Requirements (2008)	H-7(K), E-1: FAR 52.246-11(a)
AS 9100C*	Quality Management Systems—Requirements for Aviation, Space and Defense Organizations (2009)	H-7(K), E-1: FAR 52.246-11(b), E-1: FAR 52.246-11(c)
MUTCD*	Manual on Uniform Traffic Control Devices for Streets and Highways, 2009 Edition, including Revisions 1 and 2, dated May 2012	H-7(2).(C)(iii)
Joint Industry Standard (J-STD)-001-ES*	Space Application Electronic Hardware Addendum to J-STD-001E Requirements for Soldered Electrical and Electronic Assemblies, dated December 2010	H-7(1).(B)(xii)(b)
NFPA 70*	National Electric Code, dated 2011, Including Amendment 1 and Errata (2011)	H-7(2).(C)(xi)
JPL DOCUMENTS AND FORMS		
	Capital Asset Report (CAR)	G-2(a)(7)(i), G-2(a)(8)P.2., G-2(a)(8)1.3.6.1, G-2(a)(8)1.3.6.2, G-2(a)(8)1.4.2.1, G-2(a)(8)1.4.2.2.1, G-2(a)(8)1.6.1.c, G-2(a)(8)1.6.3.e, G-2(a)(8)1.6.4.b.(2), G-2(a)(8)2.2.5.3.b, G-2(a)(8)4.4.3, G-2(a)(9)(ii)
	Occupational Health Services Policies & Procedures Manual*	H-10(e)(1)
	JPL Medical Surveillance Manual*	H-10(e)(2)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
	JPL Bloodborne Pathogens Manual*	H-10(e)(3)
	JPL AED Policy Manual*	H-10(e)(4)
	JPL Employee Assistance Program Guidelines and Procedures*	H-10(e)(5)
Form 7121*	Alternative Future Use Questionnaire	G-2(a)(8)(i), G-2(a)(8)(ii), G-2(a)(9)(i)
LAWS (Miscellaneous)		
5 U.S.C. §552*	Freedom of Information Act	Attachment B—paragraph (a), Attachment B—paragraph (c)(4)
5 U.S.C. §552a / PL 93-579*	Privacy Act of 1974	H-10(d)(1), H-16(b)(2), H-16(d)(2), H-16(e)(2)(ii)
15 U.S.C. §3710*	Stevenson-Wydler Technology Innovation Act of 1980, as amended	G-25(9)(ii)(A)
29 U.S.C. §794d*	Section 508 of the Rehabilitation Act	H-43(b)(7)
	Occupational Safety and Health Act of 1970*	H-7(2)(C)(i)
42 U.S.C. §9601*	Comprehensive Environmental Response, Compensation and Liability Act (CERCLA), as amended by 42 U.S.C. §9601 (et seq.)	B-5(e)(7), H-8(b)(3)
44 U.S.C. §3541, et seq.*	Federal Information Security Management Act of 2002 (FISMA)	I-7(f)
	American Recovery and Reinvestment Act (ARRA) of 2009*	B-6(b)(1)(i), H-27(b), H-59(a), H-59(b)
	CFO Act*	G-2(a)(2)
	Economy Act*	C-1(b)(4)
	National Aeronautics and Space Administration Act of 1958, as amended (the “Space Act”)*	B-5(e)(2), C-1(b)(4), C-4(b)(8)(b), Attachment B—paragraph (a), Attachment B—paragraph (c)(4)
104 Stat. 1485, P.L. 101-510, Nov. 5, 1990*	National Defense Authorization Act for Fiscal Year 1991*	G-2(a)(3)

Document	Title and Date of Document	Contract Location
	Occupational Safety and Health Act (OSHA) of 1970*	H-7(2).(C)(i), H-10(c)
	National Energy Conservation Policy Act of 1987 (NECPA)*	H-9(a)(3)(i), H-9(a)(12)
	Energy Independence Security Act of 2007 (EISA)*	H-9(a)(3)(i), H-9(a)(12)
	Energy Policy Act 2005*	H-9(a)(12)
	California Confidentiality of Medical Information Act	H-10(d)(2)
	Contract Disputes Act*	H-32(c)(6)(iii)
	Inspector General Act, as Amended*	H-47(a), H-47(c)
	Data Quality Act—Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law 106-554)*	H-48
Pub. L. 92-41 (50 U.S.C. App., 1215(b)(2))*		I-11(e)(3)
Public Law 95-507*		Attachment D, Section I.
MIL-STD AND OTHER DoD DOCUMENTS		
	DCAA Manual*	B-5(e)(7)
DD Form 254	Contract Security Classification Specification	I-6, J-1(a), Attachment F
DoD 5220.22-M*	National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006	H-36(a), H-36(a)(2)
NASA FORMS (NF)		
533		B-6(b)(3), G-2(a)(6)(iii), G-2(a)(6)(iv), G-2(a)(6)(v), G-2(a)(6)(v), G-2(a)(6)(vi), G-2(a)(6)(viii), G-2(a)(7)(ii), G-2(a)(8)(ii), I-9(a)

Document	Title and Date of Document	Contract Location
533M	Monthly NF 533 Reports	G-2(a)(6)(i), G-2(a)(6)(iv), G-2(a)(6)(viii), G-22(b), H-34(b)(3)(iv)
533Q	Quarterly NF533 Reports	G-2(a)(6)(ii)
799 EUL*		C-4(c)
799 PD*		C-4(c)
1018		G-2(a)(8)(ii), G-24(c), H-58(f)
1509	Facility Project Brief Project Document	C-4(a)(1), C-1(a)(3)(iv), C-1(a)(4)(i), C-1(a)(4)(ii), C-4(c), G-15(a)(3)
1579	Flash Bid Report	C-4(a)(6)
1739*	Alternative Future Use Questionnaire	G-2(a)(8)(i), G-2(a)(9)(i)
NASA MISCELLANEOUS		
	NASA NSPIRES agreement*	H-12(a)
NASA STANDARDS		
NASA Safety Standard (NSS) 1740.14*	Guidelines and Assessment Procedures for Limiting Orbital Debris, dated August, 1995	H-7(1).(B)(i)(c), H-7(1).(B)(i)(f), H-7(1).(B)(i)(g), H-7(1).(B)(i)(h), H-7(1).(B)(i)(i), H-7(1).(B)(i)(j), H-7(1).(B)(i)(k), H-7(1).(B)(i)(l), H-7(1).(B)(i)(m), H-7(1).(B)(i)(n)
NASA-STD-6008*	NASA Fastener Procurement, Receiving, Inspection, and Storage Practices for Spaceflight Hardware, dated July 11, 2008	H-7(1).(B)(x)(j)
NASA-STD-8709.20* (Mod 6)	Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements, dated August 6, 2010	H-7(F)
NASA-STD-8719.9*	Standard for Lifting Devices and Equipment, with Change 1, dated October 1, 2007 (Mod 6)	H-7(2).(C)(x) (Mod 6)

Document	Title and Date of Document	Contract Location
NASA-STD-8719.11A*	Safety Standard for Fire Protection, dated November 19, 2008	H-7(2).(C)(vi)
NASA-STD-8719.12*	Safety Standard for Explosives, Propellants, and Pyrotechnics, dated January 29, 2010	H-7(2).(C)(vii)
NASA-STD-8719.13B*	Software Safety Standard (with Change 1), dated July 8, 2004	H-7(1).(E)(i)
NASA-STD-8719.14*	Process for Limiting Orbital Debris, dated August 28, 2007, with Change 4, dated September 14, 2009	H-7(1).(B)(i)(c), H-7(1).(B)(i)(f), H-7(1).(B)(i)(g), H-7(1).(B)(i)(h), H-7(1).(B)(i)(i), H-7(1).(B)(i)(j), H-7(1).(B)(i)(k), H-7(1).(B)(i)(l), H-7(1).(B)(i)(m), H-7(1).(B)(i)(n), H-7(1).(B)(ii)
NASA-STD-8719.17A*	NASA Requirements for Ground-Based Pressure Vessels and Pressurized Systems (PVS)(Revision A), dated November 6, 2009	H-7(2).(C)(ix)(f)
NASA-STD-8739.1A*	Workmanship Standard for Polymeric Application on Electronic Assemblies, dated March 4, 2008, with Change 2 dated March 29, 2011	H-7(1).(B)(xii)(a)
NASA-STD-8739.4	NASA-STD-8739.4, Crimping, Interconnecting Cables, Harnesses, and Wiring, dated February 9, 1998, with Change 6, dated March 29, 2011	H-7(1).(B)(xii)(c)
NASA-STD-8739.8*	Software Assurance Standard, with Change 1, dated July 28, 2004	H-7(1).(B)(vii)
NID/NPD/NPR/NHBK/NASA HYBRID DOCUMENTS (e.g., JPL-NMs)		
	NASA Occupational Health Program Policy*	H-10(b)
NPD 1000.5A	Policy for NASA Acquisition, dated January 15, 2009, revalidated March 17, 2010	H-26(a)(9)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
NPR 1080.1A*	Requirements for the Conduct of NASA Research and Technology (R&T), dated May 30, 2008	H-29(a)
NPD 1080.1B*	Policy for the Conduct of NASA Research and Technology (R&T), dated July 9, 2008	H-29(d)
NPD 1440.6 H*	NASA Records Management, dated March 24, 2008	H-16(f)(1)
NPR 1441.1D*	NASA Records Retention Schedules, dated February 24, 2003, with Change 5, June 26, 2009	H-16(f)(1), H-16(f)(3)
NPD 1460.1	Agency Mail Management Program, dated October 8, 2010	H-26(a)(10)
NPD 1490.1H	NASA Printing, Duplicating, and Copying Management, dated September 17, 2010	H-28(e)
JPL NPR 1600*	NASA Physical and Program Security, dated May 16, 2012	H-36(a)(9), J-1(a), Attachment H (Full Text)
NPR 1600.2*	NASA Classified National Security Information (CNSI), dated October 11, 2011	H-36(a)(8) (a)(7) is “Reserved” in 5/30/12 version
NPD 1600.2E*	NASA Security Policy, dated April 28, 2004, revalidated April 1, 2009	H-36(a)(3)
NPD 1600.3*	Policy on Prevention of and Response to Workplace Violence, dated September 4, 2007	H-36(a)(4)
JPL NM 1600-95*	NASA Identity and Credential Management, dated May 16, 2012	H-36(a)(13), J-1(a), Attachment M (Full Text)
JPL NM 1600-96*	Personnel Security, dated May 16, 2012	H-36(a)(10), J-1(a), Attachment I (Full Text)
JPL NPR 1620.2*	Facility Security Assessments, dated October 14, 2011	H-36(a)(10) [2nd consecutive (a)(10)], J-1(a), Attachment J (Full Text)
JPL NPR 1620.3*	Physical Security Requirements for NASA Facilities and Property, dated October 14, 2011	H-36(a)(11), J-1(a), Attachment K (Full Text)
JPL NPR 1660.1B*	Counterintelligence (CI)/ Counterterrorism (CT) Procedural Requirements, dated October 14, 2011	H-36(a)(12), J-1(a), Attachment L (Full Text)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
NPD 1660.1B*	NASA Counterintelligence (CI) Policy, dated November 18, 2008	H-36(a)(5), Attachment L
NPR 1800.1C*	NASA Occupational Health Program Procedures, dated October 6, 2009 with change 1, dated December 31, 2009	H-10(e)
NPD 1800.2 C*	NASA Occupational Health Program, dated January 16, 2001, revalidated July 26, 2010	H-10(e)
NPD 2110.1F	Foreign Access to NASA Technology Transfer Materials, dated November 20, 2008	H-26(a)(3)
NPD 2190.1A*	NASA Export Control Program, dated May 24, 2001, revalidated May 5, 2006	G-14(a)
NPR 2190.1B*	NASA Export Control Program, dated December 27, 2011	C-1(a)(12), G-14(h)
NPR 2570.1B	NASA Radio Frequency (RF) Spectrum Management Manual, dated December 5, 2008	H-26(a)(5)
NPD 2570.5E	NASA Electromagnetic (EM) Spectrum Management, dated July 11, 2011	H-26(a)(4)
NPR 4310.1	Identification and Disposition of NASA Artifacts, dated March 16, 1999, revalidated with change 2, January 31, 2006	H-26(a)(2)
NPD 7120.4D*	NASA Engineering and Program/Project Management Policy, dated March 16, 2010	G-10(a)(1)
NPR 7120.5E*	NASA Space Flight Program and Project Management Requirements, draft dated January 31, 2012	G-10(b)(1)(i), G-10(b)(1)(ii), G-10(b)(1)(iii), H-7(1).(A), H-7(1).(B)(xiii), H-64
NPR 7120.6*	Lessons Learned Process, dated March 22, 2005 (revalidated with Change 1, dated January 22, 2010)	G-10(a)(2)

Document	Title and Date of Document	Contract Location
NPR 7120.7*	NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements, dated November 3, 2008	G-10(d)(1)
NPR 7120.8*	NASA Research and Technology Program and Project Management Requirements, dated February 5, 2008 (with Change 1, dated November 24, 2010)	G-10(c)(1)
NPR 7120.10*	Technical Standards Products for NASA Programs and Projects, dated April 22, 2011	G-10(a)(3)
NPR 7123.1A*	NASA Systems Engineering Processes and Requirements, dated March 26, 2007, with change 1, dated November 4, 2009	H-60, H-60(a)
NPR 7150.2A*	NASA Software Engineering Requirements, dated November 19, 2009	H-7(1).(E)(i)(a), H-61, H-61(a), H-61(b)
NPR 7900.3C*	Aircraft Operations Management Manual, dated July 15, 2011	H-50(b)(1), H-50(b)(2), H-50(b)(4)
NPR 8000.4A*	Agency Risk Management Procedural Requirements, dated December 16, 2008	H-7(1).(E)(ii), H-7(1).(E)(ii)(a)
NPD 8010.3B	Notification of Intent to Decommission or Terminate Operating Space Systems and Terminate Missions, dated June 14, 2004, revalidated April 30, 2009	H-26(a)(6)
NPD 8020.7G	Biological Contamination Control for Outbound and Inbound Planetary Spacecraft, dated February 19, 1999, revalidated November 25, 2008	H-26(a)(1)
NPD 8020.12D*	Planetary Protection Provisions for Robotic Extraterrestrial Missions, dated April 20, 2011	H-26(a)(7)
NPD 8074.1	Management and Utilization of NASA's Space Communication and Navigation Infrastructure, dated August 11, 2009	H-26(a)(15)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
NPD 8500.1B*	NASA Environmental Management, dated December 20, 2007	H-8(c)(1)
NPR 8530.1A*	Affirmative Procurement Program and Plan for Environmentally Preferable Products, dated June 6, 2004, revalidated with change 3, April 3, 2009	H-8(c)(2)
NPR 8553.1B*	NASA Environmental Management System, dated September 22, 2009	H-45(b)(5)
NPR 8580.1*	Implementing the National Environmental Policy Act (NEPA) and Executive Order 12114, dated November 26, 2001	H-8(c)(3)
NPR 8590.1*	NASA Environmental Compliance and Restoration (ECR) Program, dated June 14, 2007, with change 1 dated June 2, 2010	H-8(b)(2)
NPD 8610.6G*	Graphic Markings on Space Transportation Vehicles, U.S. Components of the International Space Station Component Systems, and Payloads, dated October 30, 2003, revalidated June 15, 2009	H-26(a)(16)
NPD 8610.7D	Launch Services Risk Mitigation Policy for NASA-Owned and/or NASA-Sponsored Payloads/ Missions, dated January 31, 2008	H-26(a)(11)
NPD 8610.12G	Space Operations Mission Directorate (SOMD) Space Transportation Services for NASA and NASA-Sponsored Payloads, dated February 23, 2005, revalidated April 13, 2010	H-26(a)(12)
NPD 8610.23C	Launch Vehicle Technical Oversight Policy, dated August 18, 2006	H-26(a)(13)
NPD 8610.24C	Launch Services Program Pre-Launch Readiness Reviews, dated May 12, 2005, revalidated May 12, 2010	H-26(a)(14)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
NPR 8621.1B*	NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping, dated May 23, 2006, with change 5, dated March 15, 2010, and in the change table, dated March 11, 2010 (Mod 6)	H-7(2).(D)(iii)(a), H-7(2).(D)(iii)(c)
NPR 8705.4*	Risk Classification for NASA Payloads, dated June 14, 2004, revalidated July 9, 2008	H-7(1)(D)(i)
NPR 8705.5A*	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, dated June 7, 2010	H-7(1).(B)(viii)
NPR 8705.6B*	Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments, dated May 24, 2011	H-7(1).(B)(ix)
NPD 8710.5D*	Policy for Pressure Vessels and Pressurized Systems, dated March 12, 2008	H-7(2).(C)(ix)(a)(6), H-7(2).(C)(ix)(b)(1)
NPR 8715.3C*	NASA General Safety Program Requirements, dated March 12, 2008, with change 7, dated February 25, 2011	H-7(1).(B)(iv)
NPR 8715.5A*	Range Flight Safety Program, dated September 17, 2010	H-7(1).(B)(v)
NPR 8715.6A*	NASA Procedural Requirements for Limiting Orbital Debris, dated May 14, 2009, with Change 1 dated May 14, 2009	H-7(1).(B)(i), H-7(1).(B)(i)(l), H-7(1).(B)(i)(n), H-7(1).(B)(v)(u)
NPR 8715.7*	Expendable Launch Vehicle Payload Safety Program, dated May 30, 2008	H-7(1).(B)(iii)
NHBK 8719.14*	NASA Handbook for Limiting Orbital Debris, dated July 30, 2008	H-7(1).(B)(i)(n)
NPD 8720.1C*	NASA Reliability and Maintainability (R&M) Program Policy, dated April 18, 2008	H-7(1).(B)(vi)
NPD 8730.1C*	Metrology and Calibration, dated June 27, 2011	H-7(1).(E)(ix), H-7(1).(E)(x)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
NPD 8730.2C*	NASA Parts Policy, dated November 3, 2008	H-7(1).(B)(x)
NPD 8730.5B*	NASA Quality Assurance Program Policy, dated October 27, 2005, revalidated June 29, 2011	H-7(1).(B)(xi)
NPD 8800.14D*	Policy for Real Estate Management, dated July 15, 2004, revalidated October 14, 2009	C-4(b)(1)
NPR 8800.15B*	Real Estate Management Program, dated June 21, 2010	C-4(b)(2)
NPR 8810.1*	Master Planning Procedural Requirements, dated April 28, 2005	C-4(b)(4)
NPD 8810.2A*	Master Planning for Real Property, dated December 9, 2009	C-4(b)(3)
NPD 8820.2C*	Design and Construction of Facilities, dated June 13, 2006	C-4(b)(5)
NPR 8820.2F*	Facility Project Requirements, dated January 28, 2008	C-4(a)(5), C-4(a)(6), C-4(a)(7), C-4(b)(6), G-15(a)(3)
NPD 8831.1E*	Maintenance and Operations of Institutional and Program Facilities and Related Equipment, dated June 19, 2003, revalidated June 16, 2008	C-4(b)(7)
NPR 8831.2E*	Facilities Maintenance and Operations Management, dated November 18, 2008	C-4(b)(8)
NPD 8900.4D*	NASA Use of Global Positioning System Precise Positioning Service, dated April 27, 1999, revalidated June 15, 2009	H-26(a)(8)
NPD 9250.1A*	Capital Asset Identification and Treatment, dated October 8, 2010	G-2(a)(9)
NPR 9250.1B*	Property, Plant, and Equipment and Operating Materials and Supplies dated January 6, 2011	G-2(a)(2), G-2(a)(7)(i), G-2(a)(8), G-2(a)(8)(ii)
NPR 9501.2E*	NASA Contractor Financial Management Reporting, dated May 27, 2011	G-2(a)(1), G-2(a)(7)
NPR 9680.1A*	NASA's Management of Grants and Cooperative Agreements, dated November 10, 2011	B-6(a), B-6(b)(6)

*Denotes conditional acceptance.
Please see the Contract source for applicable conditions.

Document	Title and Date of Document	Contract Location
OFPP POLICY LETTERS		
11-01*	Performance of Inherently Governmental and Critical Functions, dated October 12, 2011	C-7
OMB CIRCULARS		
A-11*	Preparation, Submission and Execution of the Budget	H-9(a)(10)
A-21*	Cost Principles for Educational Institutions	B-5(a)
OTHER MISCELLANEOUS POLICIES AND DOCUMENTS		
	California Electric Code (CEC)	H-7(2).(C)(xi)
	U.S. National Space Policy of 2006, Section 11*	H-7(1).(B)(i)(m)
	Monk Hill Treatment System Agreement*	H-33(b)
OTHER (Prior) CALTECH PRIME CONTRACTS WITH NASA		
NAS7-03001*		B-5(d)(1), B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi), B-6(b)(1)i, B-6(b)(3), B-6(b)(9), B-6(b)(10), H-34(a), H-34(a)(1), H-34(b), H-34(b)(2), H-34(b)(3)(ii), H-34(b)(3)(iii), H-34(b)(3)(iv), H-34(c), H-34(d)
NAS7-1407*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi), B-6(b)(9), B-6(b)(10)
NAS7-1260*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi), B-6(b)(10)

Document	Title and Date of Document	Contract Location
NAS7-918*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi)
NAS7-920F*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi)
NAS7-100*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi)
NAS7-270F*		B-5(e)(3), B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi)
NASW-6*		B-5(e)(6)(ii), B-5(e)(6)(iii), B-5(e)(6)(v), B-5(e)(6)(vi)
OTHER REGULATIONS (not in CFR)		
	Standardized Regulations (SR)	G-23(b)
OTHER REQUIREMENTS		
Nuclear Regulatory Commission*	Requirements	H-7(2).(C)(v), H-10(c)
National Institute for Occupational Safety & Health (NIOSH)*	Criteria Documents	H-10(c)
OTHER STANDARDS (besides NASA Standards)		
	State of California Title 24 Building Energy Efficiency Standards	H-9(a)(11)
	Occupational Safety and Health Administration (OSHA) Standards	H-10(a)(2)
PRESIDENTIAL DIRECTIVES		
Presidential Directive 25	National Security Council/ Presidential Directive 25, updated through May 8, 1996	H-7(2).(C)(v)

Document	Title and Date of Document	Contract Location
HSPD-12*	Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004	H-65
STANDARD FORMS (SF)		
425*	Federal Financial Report	B-6(b)(10), I-11(h)(1)(i)(F), I-11(j)
1034*	Public Voucher for Purposes and Services Other Than Personal	B-6(b)(10), I-9(g)(1)
1035*	Public Voucher for Services Other Than Personal (Continuation Sheet)	B-6(b)(10)

ATTACHMENT D

JET PROPULSION LABORATORY

(JPL)

SMALL BUSINESS SUBCONTRACTING PLAN

Table of Contents

I. **Introduction and Small Business Program Overview**

II. **Goals Based on Subcontracting & Contract Value (Both Percentages and Dollars)**

III. **Principal Products and Services to be Subcontracted**

IV. **Methods Used to Develop JPL Goals**

V. **Methods Used to Identify Potential Sources for Solicitation Purposes**

VI. **Indirect Cost and Estimate of Project Versus Non-Project Percentages**

VII. **Responsibility for Administration of the Subcontracting Plan**

VIII. **Efforts to Assure Small Businesses Have Maximum Practicable Equitable Opportunities to Compete for Subcontracts**

IX. **Subcontract Flowdown Requirement—FAR 52.219-9**

X. **Assurances**

XI. **Description of Records Kept**

XII. **Reporting**

XIII. **Management Commitment**

XIV. **Institutional Outreach**

XV. **Industry Outreach Participation**

XVI. **JPL Small Business Award**

I. Introduction and Small Business Program Overview

JPL is committed to maximum utilization of Small Businesses (SB); Small Disadvantaged Businesses (SDB); Women-Owned Small Businesses (WO); HUBZone (HUB) Businesses; Veteran-Owned Small Businesses (VO); Service-Disabled Veteran-Owned Small Businesses (SDVO); and Historically Black Colleges and Universities and Minority Institutions (HBCU/MI) in the subcontracting of services and supplies in accordance with Public Law 95-507 and FAR Clause 52.219-9.

The Business Opportunities Office is a section of JPL's Acquisition Division. The Office manages JPL's Small Business and Supplier Diversity Program. The office serves as the conduit between JPL and all contractors and suppliers seeking procurement opportunities. The mission of the Business Opportunities Office is to help small businesses think big. We are passionate about developing successful partnerships between JPL and suppliers by, a) Matching businesses to procurement opportunities, b) Advocating for under-utilized businesses and promoting supplier diversity and c) Providing outreach services that encourage growth and development.

The Office, to the maximum practicable extent, will ensure that small businesses (SDB, WO, HUB, VO, SDVO, and HBCU/MI) have an equitable opportunity to compete for JPL subcontracts. The Office's responsibility and commitment to small businesses is to increase competitive opportunities and act as a "go-between" for JPL end-users and potential suppliers by assisting small businesses with marketing opportunities, introductory meetings and product demonstrations for JPL's acquisition and technical staff.

II. Goals Based on Subcontracting & Contract Value (Both Percentages and Dollars)

A. JPL Goals Shown as a Percentage of 5-Year Projected Subcontracting Amount:

Fiscal Year	+Projected Subcontract-ing Amount	Small Business		Small Disadvantaged		Women-Owned		HUBZone		Veteran-Owned		Service-Disabled Veteran-Owned		HBCU/MI	
	$M	$M	%	$M	%	$M	%	$M	%	$M	%	$M	%	$M	%
2013	**441.26**	83.54	18.93	15	3.4	7.5	1.70	1.5	0.34	3.7	0.84	0.150	0.034	3.7	0.84
2014	**461.31**	115.38	25.01	16	3.47	8	1.73	1.8	0.39	4	0.87	0.175	0.04	4	0.87
2015	**379.43**	97.33	25.65	16.5	4.35	8.1	2.13	2	0.53	4.1	1.08	0.2	0.053	4.1	1.08
2016	**396.40**	104.22	26.29	17.5	4.41	8.8	2.22	2.4	0.61	4.4	1.11	0.25	0.063	4.4	1.11
2017	**436.40**	117.53	26.93	19.592	4.49	9.896	2.27	2.874	0.66	4.948	1.13	0.282	0.065	4.948	1.13
	***2,114.8**	518.0	24.49	84.592	4	42.296	2	10.574	0.5	21.148	1	1.057	0.05	21.148	1

+ Consistent with FAR 52.219-9 paragraph (l), only subcontracts involving performance in the United States or its outlying areas are included.

* Projected Total 5-Year Subcontracting Amount FY13 through FY17.

B. JPL Goals Shown as a Percentage of 5-Year Projected Contract Value:

Fiscal Year	+Projected Contract Value Amount	Small Business		Small Disadvantaged		Women-Owned		HUBZone		Veteran-Owned		Service-Disabled Veteran-Owned		HBCU/MI	
	$M	$M	%	$M	%	$M	%	$M	%	$M	%	$M	%	$M	%
2013	**1,391.12**	83.54	6.01	15	1.08	7.5	0.54	1.5	0.11	3.7	0.27	0.150	0.011	3.7	0.27
2014	**1,425.98**	115.38	8.09	16	1.12	8	0.56	1.8	0.13	4	0.28	0.175	0.012	4	0.28
2015	**1,295.51**	97.33	7.51	16.5	1.27	8.1	0.63	2	0.15	4.1	0.32	0.2	0.015	4.1	0.32
2016	**1,316.60**	104.22	7.92	17.5	1.33	8.8	0.67	2.4	0.18	4.4	0.33	0.25	0.019	4.4	0.33
2017	**1,356.60**	117.53	8.66	19.592	1.44	9.896	0.73	2.874	0.21	4.948	0.36	0.282	0.021	4.948	0.36
	***6,785.8**	518.0	7.63	84.592	1.25	42.296	0.62	10.574	0.16	21.148	0.31	1.057	0.02	21.148	0.31

+ Consistent with FAR 52.219-9 paragraph (l), only subcontracts involving performance in the United States or its outlying areas are included.

* Projected Total 5-Year Contract Value Amount FY13 through FY17.

C. Conditions Necessary to Achieve the Goals in Sections A. and B.

The goals in sections A. and B. are considered to be “stretch goals” and can likely be achieved only if these conditions occur:

1. Awards can be made under various large institutional subcontracts to responsible small businesses, technically capable of proposing to and providing the needs of JPL at reasonable prices that would be competitive with open-competition pricing; and—

2. Certain large institutional subcontracts can be re-competed or appropriately unbundled in a way which would not compromise technical and schedule requirements, nor create performance and/or other risk, hardship, legal liability or expense.

III. Principal Products and Services to be Subcontracted

The JPL Acquisition Division provides acquisition support for the Laboratory’s missions involving solar system exploration, earth sciences and applications, communications, and information systems. In addition to NASA funded activities, the Acquisition Division supports programs on a reimbursable basis for other government departments and agencies. The Acquisition Division also supports the Laboratory’s support services requirements, construction of facilities, and all institutional supplies and services. All categories of small businesses have an opportunity to compete for JPL subcontracts. Since JPL’s Prime Contract is Task Order based it is difficult to identify and plan subcontracting opportunities in advance, especially over the 5-year period of the Contract. However, the following represents the principal products and services where subcontracting opportunities exist for small businesses over the life of the Prime Contract. These products and services are currently ongoing small business subcontracts or will be evaluated to determine the potential applicability for small business set-asides and unbundling.

Description of Products/Services FY13–FY17	
IT Infrastructure Support	Hazardous Waste Cleanup
Temporary Technical Support	Environmental Engineering and Compliance
Logistic Services And Warehousing	Optical Design and Analysis
Student Program Support	Temporary Nurse Support
A/E T&M Services (Various)	Records Storage & Retrieval Services
T&M Construction (Various)	Web Application Support
Employee Assistance Program Augmentation	Table Mt Trash
ISO Registration	Duplication and Reproduction Services
Website Maintenance & Redesign	Reliability Support
Flight Cameras	Ground Support Equipment
Avionics Boards	Computer Equipment
Microwave Components	Office Supplies
Mechanical Fabrication	Electronic Enclosures

The above table does not include long-term award term subcontracts whose award term provisions preclude potential unbundling or termination during the term of this Plan. JPL will brief the NASA Management Office during the acquisition planning process for any future award term subcontracts that are not small business set-asides. In addition, JPL commits to exploring appropriate unbundling for the following subcontracts for when the existing subcontracts end:

Potential Small Business Opportunities Late in this Prime Contract or under a Potential Future Prime Contract:

Description of Products/Services	Current Subcontractor and Subcontract Number	Maximum Award-Term End Date
Plant protection (Security and Fire)	G4S Government Solutions—1401898	April, 2020
Modular Furniture	Corovan Moving & Storage Inc.—1371833	April, 2017
Data Systems Implementation and Operation	Raytheon—1338352	September, 2018
Desktop Computing	Lockheed Martin Integrated Systems Inc.—1312203	December, 2017
Facilities Maintenance and Operations	Emcor Government Service Inc.—1344396	September, 2018

IV. Methods Used to Develop JPL Goals

NASA submits a budget to Congress for approval on a yearly basis. The amount of funding authorized and flowed down to both NASA and JPL are directly related to approval of the submitted NASA budget. Therefore, the amount of funding JPL obtains annually is directly associated to the level of funding obtained by NASA from Congress.

JPL strongly supports NASA's Small Business Program and is aggressive in assisting the agency with meeting its goals. JPL's goal setting process is new for this new Prime Contract.

The method used:

- Is based on JPL's Institutional Business Forecast (IBF), an internal JPL process used to evaluate and project the business base of the Laboratory. The IBF, conducted semi-annually, generally in February and July of each fiscal year, is a six-year (current fiscal year in progress and five future years) forecast of cost and workforce data. The July IBF forecast is used by Financial Planning to develop cost estimation rates and factors for the next five years. The Executive Council uses the information generated by the IBF to support strategic planning and overall management of JPL.

  Program/project managers and project resource analysts work together under the auspices of the directorate business office to develop the forecast by analyzing approved budgets for existing work and considering planned and proposed future work. The Program directorates review and validate the IBF written forecast assumptions, cost and workforce data for achievability.

- The IBF includes a total Procurement estimate and a Total Cost estimate. It is a cost estimate, while our goals are tracked based on obligations. So our goals are a combination of costs and obligation numbers. The IBF is the only JPL forecasting tool available for a five year future period of time. The latest IBF, as discussed above, does not include Fiscal Year 2017, the last year of the Prime Contract. Therefore, the numbers projected for FY17 are the same as FY16.

- In the small business goal setting process, past business and small business trends were considered. JPL's desire for a steady growth of our small business program was factored in. In addition, JPL evaluated all of its large institutional term contracts to determine which ones, if any, could potentially be set-aside for small businesses during the term of this Prime Contract. However, because many of these subcontracts were set up as award-term and due to legal and cost (termination) liabilities, they could not be considered eligible for set-aside purposes during the period of this Prime. When the analysis was completed, it resulted in a final 24.49% adjusted small business subcontracting value stretch goal and a 7.63% adjusted small business contract value stretch goal over the total 5-year period.

- Goals for all other socioeconomic categories are also based on JPL's historical figures and future business trends.

V. Methods Used to Identify Potential Sources for Solicitation Purposes

It is the policy of the JPL Business Opportunities Office to the maximum practicable extent ensure that small businesses (SDB, WO, HUB, VO, SDVO, and HBCU/MI) shall have an equitable opportunity to compete for JPL subcontracts. The Office's responsibility and commitment to small businesses is to increase competitive opportunities and act as a "go-between" for JPL end-users and potential suppliers by assisting small businesses with marketing opportunities, organizing introductory meetings and product demonstrations for JPL's acquisition and technical staff. The following are continuing efforts that contribute towards achieving our objective:

A. Identifying categories of qualified small business suppliers by reviewing all categories of small business listings and directories prepared by government agencies, prime contractors, private sector companies, and all categories of small business organizations.

   For example, the Business Opportunities Office uses the Central Contractor Registration (CCR); an internet-based database of information on more than 590,000 active registrants (both large and small businesses). JPL Acquisition Division and end-user personnel are instructed to use CCR for source development. The Business Opportunities Office also utilizes the U.S. Small Business Administration's Dynamic Small Business Search (DSMS) to assist in small business source list development. Both sites have search capabilities for small business classifications; a means to identify veteran-owned small businesses, as well as all other small business classifications. Other databases utilized by the Business Opportunities Office include; internal small business database maintained by each Small Business Administrator in the Business Opportunities Office and 2) Department of Defense Western Regional Council Small Business Directory. Furthermore, constant communication between Small Business Liaison Officers at NASA Centers and the Business Opportunities Office also provides a platform of information for source development. JPL will use the NASA vendor database if NASA provides JPL with access.

B. Providing practical assistance to all categories of the small business community to better prepare them to respond to JPL solicitations, particularly in arranging for direct interface with cognizant buying and end-user personnel.

C. Building and maintaining awareness of the Small Business Program by briefing cognizant technical and acquisition personnel and complying with Public Law 95-507 as it pertains to small business plans.

D. Assuring all categories of small businesses are provided the opportunity to participate in all solicitations for products and/or services which they are capable of providing. This includes Alaska Native Corporations (ANC), Tribal-Owned businesses, Historically Black Colleges and Universities and Minority Institutions (HBCU/MI).

E. Establishing and maintaining records of solicitations, source list and subcontract award activity.

F. Preparing and submitting periodic subcontract reports to JPL Management, NASA, and the U.S. Small Business Administration (SBA).

G. Providing Acquisition and Technical personnel with tailored lists of small businesses who specialize in goods/services of interest to JPL.

VI. Indirect Cost and Estimate of Project Versus Non-project Percentages

Under the terms of the Prime Contract with NASA, JPL has no indirect costs. All costs are considered to be direct. Nonetheless, the rough estimate of program/project-related subcontract % in the subcontracting base goals is 77% versus non-program/project-related subcontract % (e.g., institutional, non-project facilities, etc.) of 23%.

VII. Responsibility for Administration of the Subcontracting Program

The Manager of the Business Opportunities Office, 4800 Oak Grove Dr., Pasadena, Calif. 91109, is responsible for administration of the Subcontracting Program, with oversight by the Acquisition Division Manager. Duties of the Manager of the Business Opportunities include:

A. Attend national small business conferences/trade fairs as a JPL representative;

B. Reporting—Includes all quarterly and annual reports related to the JPL socioeconomic program as submitted to JPL, CMS and NASA;

C. Training—Includes small business utilization training facilitated by the Business Opportunities Office for JPL personnel, small business training received at NASA Centers and government agencies, and training provided by Business Opportunities Office at small business outreach events;

D. Small Business Counseling—The Business Opportunities Office serves as a liaison between all interested suppliers and JPL end-users;

E. Award Nominations—Includes review of potential award nominee qualifications in relation to award evaluation criteria, selection of nominees, and preparation of award write-ups and submissions for agency-level awards;

F. Source Development—Small business source list development for subcontract managers and source list review and approval;

G. Review and verify small business size standards;

H. Review Announcement of Opportunity Proposals—provide Small Business template and collaborate with technical customers;

I. Review Requests for Proposals—work with JPL Contract Technical Managers and Subcontract Managers to develop socioeconomic goals strategy;

J. Provide small business advice to the Performance Evaluation Review Boards (PERBs);

K. Serve on Acquisition Strategy Review Board/Non-Comp Board reviews;

L. Joint-Counseling—facilitate procurement discussions between JPL prime subcontractors and potential lower-tier small business suppliers;

M. Complete self-assessments of all activities of the JPL Small Business Program for submission to the NMO.

N. Submit semi-annual reports detailing all small business utilization metrics, outreach events, programmatic initiatives, and small business counseling and support in the JPL Supplier Diversity Program;

O. Report JPL socioeconomic business awards to NASA/NMO;

P. Review Subcontract Plans and provide approval (or rejection) memos to Subcontract Managers; and—

Q. Host Outreach Events—Host three annual events which include the High-Tech Small Business Conference; the Small Business Round Table; and the Small Business Science Forum & Supplier Fair. In order to address small business topics as they relate to partnering with prime contractors, the Business Opportunities Office hosts the JPL Industry Council, a meeting where prime contractors are invited to discuss small business utilization.

R. Examine goals on an annual basis and from time to time make recommendations to NASA if goals need to be updated.

VIII. Efforts to Assure Small Businesses Have Maximum Practicable Equitable Opportunities to Compete for Subcontracts

A. Source Identification

The success of the JPL Small Business Program is dependent upon interaction with the small business community and with business development organizations and associations.

Open communication between JPL and all the NASA Centers regarding current and upcoming opportunities contributes to a strong networking partnership. It is mainly through this interaction, exchange of information and extensive market research that JPL can identify and develop the widest and most effective procurement base within all categories of the small business community.

JPL has developed several different areas of contact for the purpose of identifying all categories of small business capabilities and exchanging views on how to promote small business programs. We maintain close coordination with, and often take a participatory role in the following government and private sector organizations:

- NASA Small Business Specialists Council: Quarterly meetings to discuss small business issues that affect the agency and NASA Centers

- Department of Defense (DoD) Western Regional Council for Small Business (formerly named: Southern California Small Business Utilization Council)
- National Association of Small Disadvantaged Businesses
- U.S. Small Business Administration, Los Angeles District Office
- California Space Authority
- Disabled Veterans Business: The California Alliance
- National Association of Women Business Owners
- HUBZone Contractors National Council

Another prime source of identification of potential small business suppliers has been through maintaining close and continuous contact with small business development organizations and associations. JPL also actively participates in a number of Small Business conferences and outreach efforts. Outreach events attended annually include the:

- Navy Gold Coast Conference
- Federal Offices of Small Disadvantaged Business Utilization Procurement (OSDBU) Conference
- National Veteran Small Business Conference & Expo
- National MED Week Conference
- HUBZone Council Conference

JPL also participates in matchmaking, networking and recognition events sponsored by congressional representatives, government agencies, prime contractors, Chambers of Commerce and minority associations. JPL, whenever possible, attends specific conferences requested by NASA.

Furthermore, JPL evaluates and reports progress against the established goals by use of a weekly e-mail status on the Small Business Program which is sent to the JPL Deputy Director, Chief Financial Officer, Acquisition Managers, Acquisition Supervisors, and Subcontract Managers. The JPL-NMO and the NASA Office of Small Business Programs are sent semi-annual reports.

As a matter of policy and practice, JPL reviews solicitations to remove statements, clauses, etc., which may unduly restrict or prohibit small business participation.

Small Business set-asides will be pursued in instances where adequate competition at fair market prices are identified.

B. Mentor-Protégé Program

JPL will establish a new Mentor-Protégé Program to expand the diversity of the Laboratory's supplier base and to maintain JPL's commitment to enhance and increase small business utilization. The program will be designed to provide participants with access to tools, resources, and training in business development, infrastructure, technical expertise, and procurement performance.

The program will seek to achieve the following:

- Expand the diversity of the JPL supplier base;
- Enhance the technical capability of small businesses to successfully bid and manage subcontracts with the Laboratory and compete in the federal and prime contractor sectors;
- Increase dollars awarded to small business through establishing Mentor -Protégé subcontracts on a non-competitive basis; and -
- Increase dollars awarded to small businesses and meet and exceed socioeconomic goals through the successful training of potential suppliers and through awarding subcontracts to small businesses.

Currently, the Business Opportunities Office is actively pursuing opportunities and strategies to include additional companies in the Mentor-Protégé Program through the following:

- Marketing the program to the Engineering and Science Directorate (3X) and other science and technical directorates as a means of gaining funding or sponsorship of a subcontract for the Technical Development requirements of the Mentor-Protégé Program. The Office will utilize the previous Mentor-Protégé as a model to highlight the effectiveness of the Mentor-Protégé Program for establishing partnerships with future suppliers; providing exposure to technological innovations of small businesses, and demonstrating their overall impact on JPL programs and missions.
- Partnering with the JPL SBIR Office to include Phase II companies in the program. Participation of Phase II companies will assist JPL's quest to enhance research and development while mentoring new or emerging small businesses.
- Working with the JPL Minority Education Office to include Historically Black Colleges and Universities and Minority Institutions (HBCU/MI) in the program. The office will be working with the JPL Education Office to strategize methods to fund an HBCU/MI Mentor-Protégé agreement.

The Business Opportunities Office administers the California Institute of Technology, Jet Propulsion Laboratory's Mentor-Protégé Program in accordance with the spirit of the NASA's Mentor-Protégé Program while recognizing that Caltech/JPL is an independent contractor.

IX. Subcontract Flowdown Requirement—FAR 52.219-9

A flowdown clause entitled "Utilization of Small Business Concerns" is included in all subcontracts which offer further subcontracting opportunities. In addition, JPL requires that all subcontractors (except small business concerns) which receive subcontracts in excess of $650,000 ($1,500,000 for construction), submit a Small Business Subcontracting Plan, similar to this plan, which is submitted to JPL for approval prior to award of subcontract unless a subcontracting plan is not required. Written determination that there are no subcontracting opportunities shall be prepared by the Acquisition Division.

X. Assurances

The Contractor hereby provides its assurance that it will:

A. Cooperate in specific studies or surveys whenever feasible;

B. Submit periodic reports so that the Government can determine the extent of compliance by the Contractor with the Subcontracting Plan.

C. Submit the Individual Subcontract Report (ISR) and/or the Summary Subcontract Report (SSR), using the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov. The reports shall provide information on subcontract awards to small business concerns, veteran-owned small business concerns, service-disabled veteran-owned small business concerns, HUBZone small business concerns, small disadvantaged business concerns, women-owned small business concerns, and Historically Black Colleges and Universities and Minority Institutions.

D. Ensure subcontractors with subcontracting plans agree to submit the Individual Subcontract Report (ISR) and/or the Summary Subcontract Report (SSR). ISR and the SSR are submitted on a semi-annual basis. Each subcontractor, with a subcontract award in excess of $650,000 ($1,500,000 for construction), is required to report all subcontracting activities.

E. Provide its prime contract number, its DUNS number, and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports to all first-tier subcontractors with subcontracting plans so they can enter this information into the eSRS when submitting their reports.

F. Require that each subcontractor with a subcontracting plan provide the Prime Contract number, its own DUNS number, and the e-mail address of the Government or Contractor official responsible for acknowledging or rejecting the reports, to its subcontractors with subcontracting plans.

XI. Description of Records Kept

The Business Opportunities Office will maintain the following records:

A. Subcontract Plans and approval memos;

B. Source lists that identify both large and small business and Source list approvals;

C. Telephone, e-mail, and in-person liaison and counseling support;

D. Individual Subcontract Report (ISR) and the Summary Subcontract Report (SSR);

E. Request for Proposals listed on FedBizOpps;

F. Outreach events supported in order to identify small business sources;

G. NASA 45-Day Reports on all JPL outreach events;

H. Records to support award data submitted by the Contractor to the Government, including name, address and business size of each subcontractor; and—

I. Records of internal guidance and encouragement provided to the Contractor's buyers ("Acquisition Managers"), including:

   i. Workshops, seminars and training; and—

   ii. Weekly Socioeconomic Reports provided to Acquisition Division management and buying personnel as well as the Deputy Director and CFO/Director for Business Operations.

J. The individual procurement files shall maintain records in accordance with FAR 52.219-9(d)(11)(ii) and (iii) (JAN 2011).

XII. Reporting

JPL submits various periodic reports to the NMO and the NASA Office of Small Business Programs in support of the agency's policies. Reports submitted are as follows:

A. Individual Subcontract Report (ISR) and the Summary Subcontract Report (SSR) are submitted on a semiannual basis. Each subcontractor, with a subcontract award in excess of $650,000 ($1,500,000 for construction), is required to report all subcontracting activities. The reports provide an account of dollars subcontracted to small businesses;

B. NASA Small Business Program Report is submitted on a semi-annual basis. The purpose of the Small Business Program Report is to facilitate management of the Lab's Small Business Program. The report highlights prime statistics, small business improvement plans, acquisition planning & contract management, outreach, training, special assignments and awards;

C. 45-Day Reports are submitted within 45 days of the culmination of institutional outreach event. The purpose and/or goal of the report is to highlight the key elements of the event, guest speakers, number of attendees, provide the description of workshops and activities, and to reflect upon lessons learned; and—

D. The NASA Small Business Program initiatives for the Small Business Improvement Plan (SBIP) strategy meeting are submitted on an annual basis. The purpose of the SBIP is to establish three (3) agency-wide initiatives along with objectives for each initiative to improve the agency's small business program.

XIII. Management Commitment

Senior Management strongly supports JPL's Small Business Program. The Business Opportunities Office Manager has the ability to communicate directly with the Deputy Director, Chief Financial Officer, Chief Information Officer, Engineering and Science Directorate and other members of Senior Management to discuss key issues as the need arises. The Business Opportunities Office regularly coordinates with, and keeps JPL Management informed on the status of the Small Business Program.

The Project Acquisition Managers (PAM) assists the Business Opportunities Office with outreach, procurement forecast, and internal training to technical personnel. The Business Opportunities Office has oversight of, and updates Senior Management on the following programmatic activities:

A. Establishment of goals and meaningful program objectives to ensure that proper emphasis and support is provided by all elements of the Laboratory on a continuing basis;

B. Review, modify as necessary, and approve Small Business Plans submitted by Subcontractors;

C. Evaluate and report progress against the established goals by use of a weekly e-mail status on the Small Business Program which is sent to the Deputy Director, Chief Financial Officer, Acquisition Managers, Acquisition Supervisors, and Subcontract Managers. The JPL-NMO and the NASA Office of Small Business Programs are sent semi-annual reports; and—

D. Implement and provide status on continuing NASA Initiatives such as the Mentor-Protégé Program, the annual High-Tech Small Business Conference, the Small Business Round Table and the annual Small Business Science Forum and Supplier Fair.

In addition to these meetings, frequent interface takes place on any small business issues that require immediate attention. JPL management is supportive of the Small Business Program and assists fully in the implementation and institutionalization of new small business initiatives. JPL Senior Management participates in many small business outreach efforts.

XIV. Institutional Outreach

The Laboratory's outreach activities typically include the coordination of three national conferences known as 1) the annual High-Tech Small Business Conference, 2) the annual Small Business Round Table and 3) the annual Small Business Science Forum and Supplier Fair. These events are designed to educate small businesses on competing for contracts in the Federal and prime contractor sector.

JPL has coordinated the annual High-Tech Small Business Conference with NASA and the U.S. Small Business Administration (SBA) for more than 20 years. This conference has been very successful in providing an opportunity for all categories of small businesses to meet representatives from the federal government and prime contractor corporations to discuss potential contracting opportunities within their agencies. Workshops are presented on a variety of current interests.

The Small Business Round Table (formerly named Prime Contractor Small Business Round Table/SDB Forum), began in 1999 and is held annually at JPL. The Small Business Round Table's purpose is to enable JPL's prime contractors to interact with all categories of small businesses and pursue subcontracting opportunities; specifically on JPL contracts. A number of subcontractors, including small businesses, are asked to participate on a panel and are given specific topics to research. The Round Table's interactive format is an excellent way to address current issues, as it allows small businesses to interact with subcontractors on topics of mutual interest.

The Small Business Science Forum & Supplier Fair (formerly named "Semi-Annual Science Forum for Small Business"), began in 1997 and is hosted at JPL. The main objective of the forum is to enable additional teaming and partnering possibilities between other procuring organizations and all categories of small businesses. Between 25 to 30 subcontractors and small businesses are selected by the Business Opportunities Office, based on the subcontractor's level of business with JPL and the small businesses' potential for matching the subcontractor's high-tech interests.

Veteran-Owned and Service-Disabled Veteran-Owned Outreach, etc.

The Business Opportunities Office will initiate plans for a Veteran-Owned and Service-Disabled Veteran-Owned Business Outreach Campaign. The campaign will consist of an educational tour and information dissemination to local and statewide Veteran-Owned business support organizations, like the California Disabled Veteran Business Alliance and The Elite SDVOB Network. The tour will establish better communications with the Veteran-Owned business community and help JPL gain a better understanding of the type of industries represented by Veteran-Owned firms (R&D, IT, commodities, construction, etc.), the types of products and services that would be a best fit for JPL, and to gain a better understanding of the challenges veteran's face in doing business with JPL. The tour and information gained from the campaign would be a precursor to a possible JPL veteran outreach event. VO and SDVO concerns will be included on source lists when such concerns are identified as offering the commodity or service being procured.

XV. Industry Outreach Participation

- GovLink Conference
- Inland Empire MBE Center
- California Disabled Veterans Business: Keeping the Promise & Regional Matchmaking Conference
- National Veteran Small Business Conference /Expo

- GSA: Opening Doors Conference
- Navy Gold Coast Conference
- Federal Offices of Small Disadvantaged Business Utilization Procurement (OSDBU) Conference
- National MED Week Conference
- HUBZone Council Conference

**The Business Opportunities Office will strive to participate in Industry outreach events as the Acquisition Division's travel budget allows.*

XVI. JPL Small Business Award

JPL nominates a small business for the annual "NASA Small Business Subcontractor of the Year" and the Thomas H. May Legacy of Excellence Award. The Thomas H. May Legacy of Excellence Award is presented annually by JPL to a small business for excellence in subcontract performance. This award is presented to honorees during the annual JPL High-Tech Conference for Small Business.

ATTACHMENT E
June 4, 2013
CONTRACT DATA REQUIREMENTS LIST (CDRL) (Mod 6)

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
1	CM-001	Analysis of Draft NPR 7120.5E	Once	Complete by April 30, 2012	G-10, Program/Project Management (b)(1)(ii)	Contractor Format	NMO
2	CM-002	Anticipatory Costs	As Required	As Required	B-05, Allowable Costs, (e)(1), Anticipatory Costs	Contractor Format	NMO
3	CM-003	Overrun Reports	As Required	As Required	F-05, General Reports and Plans, (6), Overrun Reports	Contractor Format	NMO
4	CM-004	Provide Analysis of Final NPR 7120.5E	Once	Within 60 days of NASA's written notice to JPL of the final NPR 7120.5E release is in NODIS	G-10, Program/Project Management (b)(1)(iii)	Contractor Format	NMO
5	CM-005	Intergovernmental Personnel Act (IPA) Costs Report	Upon Request	Upon Request	B-05, Allowable Costs, (e)(11), Other Advance Understandings - Intergovernmental Personnel Act (IPA)	Contractor Format	NMO
6	CM-006	Excess Funds on Inactive Task Orders	Quarterly	Due 30 days after the close of the quarter	G-02, Cost Segregation and Reporting, (a)(5), Identification of Excess Funds on Inactive Task Orders	Contractor Format	NMO
7	CM-007	Pending Actions for Outstanding Allowable Costs on Expired Task Orders	As Required	Within 90 days after Task Order expiration	B-06, Contractor Financing by Letter of Credit (LOC), (b)(11)	Contractor Format	RFO

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
8	EM-001	Five-Year Energy Efficiency and Water Conservation Plan	Once	None Stated for first time	H-09, Energy Management , (a)(6)	Sponsor Format	NMO E&F Manager For Approval
9	EM-002	Update to Five-Year Energy Efficiency and Water Conservation Plan	Every 3 years	Update on a maximum 3-year interval	H-09, Energy Management , (a)(6)	Sponsor Format	NMO E&F Manager For Approval
10	EM-003	Energy and Water Consumption Reports	Quarterly	None Stated	H-09, Energy Management , (a)(10)	Sponsor Format	NETS (ED)
11	EM-004	Plan for Reinvestment of cost Savings from Realized Energy and Water Conservation Measures	Semi-Annually	None Stated	H-09, Energy Management, (a)(13), Reinvestment of Cost Savings	Contractor Format	NMO For Approval
12	EM-005	Draft Outdoor Environment Master Plan (OEMP)	Once	Within 180 days of the effective date of this Contract	H-09, Energy Management, (a)(14), Development of Outdoor Environment Master Plan (OEMP)	Contractor Format	NMO
13	EM-006	Energy and Water Consumption Reports - As Required by any Federal State, Local Regulation, NPD, NPR or Executive Order	As Required	As Required	H-09, Energy Management, (b), Energy and Water Conservation Reports	Contractor Format	NASA
14	EM-007	Office of Management and Budget Circular A-11, Energy and Transportation Efficiency Management Budget Exhibits	Annually	None Stated	H-09, Energy Management (a)(10)	Sponsor Format	NMO
15	EM-008	Energy Management Progress Assessment Report	Annually	None Stated	H-09, Energy Management, (a)(10)	Sponsor Format	NMO

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
16	EV-001	Environmental, Safety and Health System (ESHS) Documentation	Annually	C.O. Will establish dates for submittal, review and comment	H-45, Integration of Environment, Safety and Health into the Contractor's Management System, (d)	Contractor Format	NMO For Approval
17	FA-001	Report on Facilities Leased	Quarterly	None Stated	C-03, Use of Other Facilities and Locations, (d)	Contractor Format	C.O.
18	FA-002	Functional Area Performance Metrics for CoF, Facilities Maintenance, Real Property, Space Utilization, and Environment	Annually	As Requested	C-04, Facilities Management Provisions, (a)(7)	Contractor Format	FED
19	FA-003	Use of Facilities Communications Plan	As Requested	As Requested	H-42, Use of Facilities Communications Plan	Contractor Format	NMO
20	FM-001	Payment of Overtime Premiums	Quarterly	None Stated	H-40, Payment of Overtime Premiums	Contractor Format	NMO
21	FM-002	Caltech Transfers	Quarterly	End of month following reporting quarter	F-05, General Reports and Plans, (8), Caltech Transfers	Contractor Format	NMO
22	FM-003	Estimated Accumulated Post-Retirement Benefits (PRB) Liability - "Initial Baseline"	Once	By August 30, 2012	H-66, Post Retirement Benefits Liability Re-Opener Clause, (a)	Contractor Format	NMO
23	FM-004	Changes to Estimated Accumulated Post-Retirement Benefits (PRB) Liability	Annually	No sooner than March 1st, but no later than May 1st of each calendar year	H-66, Post Retirement Benefits Liability Re-Opener Clause, (b)	Contractor Format	NMO
24	FM-005	Interest on Letter of Credit Payments	Monthly	Due 15 days after month end	B-06, Contractor Financing by Letter of Credit (LOC), (c) Interest	Contractor Format	DHHS

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
25	FM-006	Procedures to Manage the Letter of Credit	Once	Due 60 days after Contract effective date	B-06, Contractor Financing by Letter of Credit (LOC), (b)(12), LOC Management Procedures	Contractor Format	NMO
26	FM-007	Letter of Credit Certifications - Standard Form 425, Federal financial Report	Quarterly	Due 30 days following the end of each Federal fiscal Quarter	B-06, Contractor Financing by Letter of Credit (LOC), (b)(10), LOC Certifications	Sponsor Format	DHHS
27	FM-008	Reconciliation of Expenditures to Letter of Credit Draws	Monthly	None Stated	B-06, Contractor Financing by Letter of Credit (LOC), (b)(8), Monthly Reconciliation	Contractor Format	NMO
28	FM-009	Uncosted Obligations - Phased Costing Plan	As Requested	As Requested	G-02, Cost Segregation and Reporting, (a)(4), Uncosted Obligations	Sponsor Format	NMO
29	FM-010	Annual (Final) Allocated Direct Costs and Forecast Report	Annually	None Stated	G-18, Allocated Direct Cost Reporting, (a), Annual Reports	Contractor Format	NMO
30	FM-011	Allocated Direct Costs Report	Monthly	None Stated	G-18, Allocated Direct Cost Reporting, (b), Monthly Reports	Contractor Format	NMO
31	FM-012	Monthly Contractor Financial Management Report - NF533M	Monthly	Ten (10) working days after the end of the Contractor's fiscal month	G-02, Cost Segregation and Reporting, (a)(6)(i), NASA Contractor Financial Management Report - Monthly NF 533 Reports	Sponsor Format	RFO
32	FM-013	Quarterly Contractor Financial Management Report - NF533Q	Quarterly	Fifteen (15) calendar days prior to the beginning of Contractor's fiscal quarter	G-02, Cost Segregation and Reporting, (a)(6)(ii), NASA Contractor Financial Management Report - Quarterly NF 533 Reports	Sponsor Format	RFO
33	FM-014	Allocated Direct Costs Special Report	As Requested	As Requested	G-18, Allocated Direct Cost Reporting, (c)	Contractor Format	NMO

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
34	FM-015	Public Voucher (No-Pay Voucher)	Monthly	Due 15 working days after the close of the Contractor's fiscal month	I-09, Allowable Cost and Payment (FAR 52.216-7) (JUN 2011) (DEVIATION), (a), Contractor Payments	Sponsor Format	NMO
35	FM-016	Completion Voucher and Final SF1034	Once	Due upon closeout of all task orders under this Contract	I-09, Allowable Cost and Payment (FAR 52.216-7) (JUN 2011) (DEVIATION), (g)(1)	Sponsor Format	NMO
36	HR-001	Wage and Salary Schedules and Non-Academic Policies	As Requested	Within 15 days of written request by the Contracting Officer	H-06, Wages, Salaries and Personnel Data, (a), Wage and Salary Policy and Practice	Contractor Format	NMO
37	HR-002	Workforce Data and Occupational Distribution, Educational Levels, Average Age and Average Rate Ranges	Annually	None Stated	H-06, Wages, Salaries and Personnel Data, (b), Aggregated Data on JPL Work Force	Contractor Format	NMO
38	HR-003	Workforce Reports	Annually	By the 90th day after expiration of the yearly Affirmative Action Plan	F-05, General Reports and Plans, (7), Workforce Reports	Contractor Format	NOE
39	IP-001	Mask Works - Registration and Publication	As Required	Technical report within six months after written disclosure	H-38, Agreement on Establishment of rights, Technology Transfer, and Distribution of Income with Respect to Mask Works, (a)	Contractor Format	NMO
40	IP-002	Shared Royalty Income	Quarterly	None Stated	H-38, Agreement on Establishment of rights, Technology Transfer, and Distribution of Income with Respect to Mask Works, (c)	Contractor Format	NMO
41	IP-003	Tech Transfer Annual Report	Annually	None Stated	F-05, General Reports and Plans, (9)(ii)(D), Tech Transfer Annual Report	Sponsor Format	NTTS (ED)
42	IP-004	NASA Technology Tracking System (NTTS)	Monthly	No later than the 15th of the month for which the data pertains	F-05, General Reports and Plans, (9)(ii)(A), NASA Technology Tracking System (NTTS)	Sponsor Format	NTTS (ED)

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
43	IP-005	Technology Transfer Policy Guidance	Once	None Stated	F-05, General Reports and Plans, (9)(ii)(C), Technology Transfer Policy Guidance	Contractor Format	NMO
44	IP-006	Royalties from Licensing of Intellectual Property Rights on Computer Software Developed	Quarterly	None Stated	H-37, Agreement on Computer Software, (c)	Contractor Format	NMO
45	IT-001	Annual IT Security Awareness Training - Provide Copy to HQ OCIO	Annually	None Stated	I-07, Security Requirements for Unclassified information Technology Resources, NFS 1852.204-76 (JAN 2011) (DEVIATION), (c)(4), Annual IT Security Awareness Training Requirement	Contractor Format	CIO
46	IT-002	Information Technology (IT) Budget Plan	Annually	None Stated	H-56, Requirement for Information Technology Budget Plan, (a)	Contractor Format	CIO
47	IT-003	Assisting NASA by Supplying Data Related to NASA's FISMA Responsibilities	As Requested	None Stated	I-07, Security Requirements for Unclassified information Technology Resources, NFS 1852.204-76 (JAN 2011) (DEVIATION), (f)	Sponsor Format	SOC
48	MS-001	AS9100 Transition Plan	Once	90 days after the effective date of the Contract	E-01, Listing of Clauses Incorporated by Reference, (c)	Contractor Format	C.O.
49	OGC-001	NASA Office of the Inspector General Program Procedures	Once	Within 30 days after the effective date of this Contract	H-47, NASA Office of the Inspector General Programs, (b), Establish and Maintain Procedures for Cooperating with OIG Audits	Contractor Format	OIG
50	OGC-002	Litigation Management Plan Submission	Annually	First one within 90 days after October 1, 2012. Annually thereafter	H-44, Litigation Management Plan, (b)	Contractor Format	C.O.

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
51	OGC-003	Case Assessment and Staffing/Resource Plan - If Requested by the Contracting Officer	As Requested	When requested by the C.O. - within 30 days after responding to complaint	H-44, Litigation Management Plan, (e)	Contractor Format	C.O.
52	PR-001	Property Reporting	Annually	No later than October 30th	G-03, Property Reporting	Sponsor Format	IPO
53	PR-002	Contractor-Held Asset Tracking System (CHATS) Report and Capital Asset Report (CAR)	Monthly	Due the 21st day of the month following the calendar month to be reported	H-58, Monthly Property Financial Reporting, (a)	Sponsor Format	CHATS (ED)
54	PR-003	NASA Property in the Custody of Contractors- NF1018	Annually	None Stated	G-02, Cost Segregation and Reporting, (a)(8), Property, Plant and Equipment and Operating Materials and Supplies	Sponsor Format	NESS
55	SMS-001	Safety and Health Plan	Annually	90 days prior to effective date of Contract. Updates annually thereafter	F-05, General Reports and Plans, (10)(i), Safety, Health and Mission Assurance Reports	Contractor Format	NMO
56	SMS-002	Types of Hazardous Operations Performed	Semi-Annually	90 days after Contract award. Updates no less than semi-annually	F-05, General Reports and Plans, (10)(ii)	Contractor Format	NMO

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
57	SMS-003	Safety and Mission Assurance (SMA) Technical Authority Implementation Plan	Once	Within 60 days after Contract Award	F-05, General Reports and Plans, (10)(iii)	Contractor Format	NMO for Approval
58	SMS-004	Safety and Mission Assurance Annual Operating Agreement	Annually	Submitted no later than 31st October of each year	F-05, General Reports and Plans, (10)(iv)	Contractor Format	NMO
59	SMS-005	Illness, Incident and Injury Experience Report	Quarterly	None Stated	H-07(2), Safety and Health, (D)(i)	Contractor Format	C.O.
60	SMS-006	Ground-Based Pressure Vessels Certification Plan	Once	No later than 90 days after the effective date of the Contract	H-07(2), Safety and Health, (C)(ix)(a)(5), Ground-Based Pressure Vessels: Implement Conditional NASA-STD-8719.17A	Contractor Format	C.O.
61	SMS-007	NASA Incident Reporting Information System	As Required	Within 24 hours of a mishap or close call	H-07(2), Safety and Health, (D)(iii)(b)	Sponsor Format	IRIS (ED)
62	SU-001	Notification to the Contracting Officer of JPL Subcontractor's Material Breach of Its Small Business Subcontracting Plan	As Required	Whenever a JPL Subcontractor fails to comply in good faith with the Plan	G-9, Small Business Subcontracting Plan, (e)	Contractor Format	C.O.
63	SU-002	NASA Small Business Program Report	Semi-Annually	None Stated	Attachment D, Small Business Subcontracting Plan, XII.B. Reporting - NASA Small Business Program Report	Contractor Format	NMO
64	SU-003	Summary Subcontract Report	Semi-Annually	30 days following the end of the reporting period	Attachment D, Small Business Subcontracting Plan, XII.A. Assurances	Sponsor Format	ESRS (ED)
65	SU-004	Individual Subcontract Report (ISR)	Semi-Annually	None Stated	Attachment D, Small Business Subcontracting Plan, XII.A. Reporting - ISR and SSR	Sponsor Format	ESRS (ED)

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
66	SU-005	Institutional Outreach - 45-Day Reports	As Required	45 days after the culmination of Institutional Outreach	Attachment D, Small Business Subcontracting Plan, XII.C. Institutional Outreach - 45-Day Report	Contractor Format	NMO
67	SU-006	NASA Small Business Program Initiatives for the Small Business Improvement Plan (SBIP) Strategy Meeting	Annually	None Stated	Attachment D, Small Business Subcontracting Plan, XII.D. NASA Small Business Program Initiatives for the Small Business Improvement Plan Strategy Meeting	Contractor Format	NMO
68	SU-007	Subcontracting Status Reports	Semi-Annually	None Stated	Attachment D, Small Business Subcontracting Plan, XIII.C. Subcontracting Status Reports	Contractor Format	NMO
69	SU-008	General Provisions in Subcontracts	Once and as Required Thereafter	Within 90 days after the effective date of this Contract	H-27, Clause Flowdown Requirement, Subparagraph (d)	Contractor Format	NMO
70	TE-001	Acquisition and Use of Government-Owned Vehicles Report	Annually	Not later than October 15th of each calendar year	H-51, Transportation Efficiency, (a)(4), Annual Reports	Sponsor Format	FAST (ED)
71	XX-001	Contractor Evaluation	Semi-Annually	Semi-annually submitted at the mid-year point and the end of the fiscal year	B-08, Contractor Evaluation	Contractor Format	C.O.
72	XX-002	Foreign Travel Weekly Report	Weekly	None Stated	Attachment A, Foreign Travel, 2.d.	Contractor Format	OIIR
73	XX-003	Foreign Trip Reports	As Requested	As Requested	Attachment A, Foreign Travel, 2.d.	Contractor Format	OIIR
74	XX-004	Program/Project Management Certification - Requirements for Individuals to be Certified Under the JPL Certification Program	As Requested	As Requested	G-10, Program/Project Management, (b)(2)(II)(a)	Contractor Format	NHQ

Line Item No.	CDRL NO.	TITLE OR DESCRIPTION OF DATA	FREQUENCY	DUE DATE	CONTRACT LOCATION	FORMAT (CONTRACTOR OR SPONSOR)	REQUESTER
75	XX-005	Program/Project Management Certification - Established Procedure for Certification of Individuals Under the JPL Certification Program	As Requested	As Requested	G-10, Program/Project Management, (b)(2)(II)(b)	Contractor Format	NHQ
76	XX-006	Program/Project Management Certification - Assessment of Functional Equivalency to NASA's Program	As Requested	As Requested	G-10, Program/Project Management, (b)(2)(II)(c)	Contractor Format	NHQ
77	XX-007	Program/Project Management Certification - Listing of the Program/Projects that NASA Has Designated Requiring JPL Certification	As Requested	As Requested	G-10, Program/Project Management, (b)(2)(ii)(d)	Contractor Format	NHQ
78	XX-008	Program/Project Management Certification - List of Names Who Have Been Certified Using the JPL Certification Program	As Requested	As Requested	G-10, Program/Project Management, (b)(2)(ii)(e)	Contractor Format	NHQ
79	XX-009	Estimate of Percentage of EPA-Designated Material Used	Once	At end of Contract	I-01, Listing of Clauses, I. Federal Acquisition Regulations, 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products	Sponsor Format	NMO
80	XX-010	Planning, Programming, Budgeting, and Execution (PPBE)	Annually	None Stated	B-04, Budgetary Estimates and Funding, (a)	Sponsor Format	NMD
81	XX-011	Revised Planning, Programming, Budgeting, and Execution (PPBE)	As Required	As Required	B-04, Budgetary Estimates and Funding, (b)	Sponsor Format	NMD

Legend for CDRL No.: CM-Contract Management; EV-Environmental Affairs; FA-Facilities Division; FM-Financial Management; HR-Human Resources; IP-Intellectual Property; IT-Information Technology; MS-Management System; OGC-Office of the General Counsel; PR-Property; SMS-Safety and Mission Success (Other than Environmental); SU-Subcontracts; TE-Transportation Efficiency; XX-Miscellaneous.

Legend for Requester Organizations: C.O. - Contracting Officer; CHATS (ED)- Contractor Held Assets Tracking System (Electronic Data); DHHS - Department of Health and Human Services; ESRS (ED) - Electronic Subcontracting Reporting System (eSRS); FED - Facilities Engineering Division at Headquarters; FAST (ED) - Federal Automotive Statistical Tool (FAST) web-based reporting tool; RFO - Goddard Regional Finance Office; NHQ – NASA; CIO - NASA Chief Information Officer (CIO); NMO E&F Manager – NMO Environmental and Facilities Manager; NMD - NASA Enterprises (Now called NASA Mission Directorates); NETS (ED) - NASA Environmental Tracking System; NOE - NASA Headquarters Office of Education; IRIS (ED) - NASA Incident Reporting Information System; IPO - NASA Industrial Property Officer; OIG - NASA Office of the Inspector General; NHQ - NASA Headquarters; SOC - NASA Security Operations Center; NTTS (ED) - NASA Technology Tracking System (Electronic Data); OIIR - Office of International and Interagency Relations and to HQ Mission Directorates.

END OF MODIFICATION NO. 6

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED: TOP SECRET
b. LEVEL OF SAFEGUARDING REQUIRED: TOP SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

X	a. PRIME CONTRACT NUMBER: NNN12AA01C	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*: 20111213
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [X] YES [ ] NO. If Yes, complete the following:
Classified material received or generated under NAS7-03001 *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
California Institute of Technology Jet Propulsion Laboratory 4800 Oak Grove Drive Pasadena, CA 91109	2D771	

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
N/A		

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
N/A		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
Research and Development (U)

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA	X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	X	
d. FORMERLY RESTRICTED DATA	X	
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)	X	
(2) Non-SCI	X	
f. SPECIAL ACCESS INFORMATION	X	
g. NATO INFORMATION	X	
h. FOREIGN GOVERNMENT INFORMATION	X	
i. LIMITED DISSEMINATION INFORMATION	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*		

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
h. REQUIRE A COMSEC ACCOUNT	X	
i. HAVE TEMPEST REQUIREMENTS	X	
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
l. OTHER *(Specify)*	X	

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE. Adobe Professional 7.0

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through *(Specify)*

Office of Communications
National Aeronautics and Space Administration
Washington, DC 20546

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

All classified materials received or generated in connection with this contract will be handled and safeguarded in accordance with the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M. the highest classification level of information on this contract is Top Secret.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] Yes [ ] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

Clause H-36 of the JPL Contract.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [X] Yes [ ] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

DoD projects have been established in Building 180, Room B-10 and Building 126, Room 153/154. Both areas will not be subject to inspections by the cognizant security office and any other areas developed for Special Programs.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Robert W. Raimond	OPS Director, Security Management Division	202-358-0878

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
Office of Protective Services National Aeronautics and Space Administration Washington, DC 20546	[X]	a. CONTRACTOR
	[ ]	b. SUBCONTRACTOR
	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE (11/4/2011)	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
	[X]	f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

Attachment F

SECURITY CLASSIFICATION CRITERIA FOR CONTRACT NNN12AA01C

Pursuant to the Security requirements clause of the above contract, this is notification of the security classification of assigned work that will be performed and is issued to supplement the basic DoD Contract Security Classification Specification (DD Form 254).

This contract provides funds for the California Institute of Technology (the "contractor") to carry out government funded research and development work associated with the mission of NASA and elements of the Department of Defense. The research and advanced development information supporting this work may include classified information up to and including Top Secret. Therefore, the contract is regarded as being Top Secret from the security regulations point of view. Information obtained or reproduced as a result of such access shall be protected in accordance with its classification at the time of access, or as subsequently revised.

For news information being developed, security classification guidance will be provided by program classification guides, policy directives, or individual letters will provide security classification guides. For those projects dealing with areas of information for which no guidance has been provided or for which security classification cannot be determined in advance, the contractor shall prepare and activate an interim DD Form 254 for each task as required. The Classification Specification assigned shall be in accordance with the provisions of Executive Order 13526, Executive Order 12829 and existing implementing guidelines. Particular attention shall be paid to those achievements which substantially advance "the state of the art" in technology of hardware development or which may have defense support applicability.

The NASA Management Office will review each tentative DD Form 254 to assure appropriate classification and uniformity of classification among programs and will modify if required. The contractor, both for in-house and otherwise controlled activities, which appear to have defense support applicability, shall expeditiously prepare and submit to the NASA Management Office an interim DD Form 254. NASA Headquarters, Office of Protective Services, shall be sent a copy. No release of material on such tasks may be made until NASA Management Office approval of the DD Form 254 is obtained.

Robert W. Raimond
Director, Security Management Division
NASA Office of Protective Services

12/13/2011
Date

ATTACHMENT G

AGREEMENT AND CONDITIONS FOR EVALUATION OF PROPOSALS

(a) The recipient agrees to use proposal information for NASA evaluation purposes only. Additionally, the recipient agrees not to reveal any information concerning the proposal or the evaluation of the proposal to anyone not also participating in the evaluation for three years from the date of disclosure. If information is disclosed to others participating in the evaluation, that disclosure shall only be to the extent that the information is required in connection with the evaluation. Although this limitation does not apply to information that has been previously made available to the public or disclosed publicly, the recipient agrees not to disclose what public information is contained in the proposal for three years from the date of disclosure.

(b) The recipient agrees that the NASA proposal cover sheet notice and any notice that may have been placed on the proposal by its originator, shall be applied to any reproduction or abstracts of any proposal information furnished.

(c) Upon completion of the evaluation, the recipient agrees to return all copies of proposal information or abstracts, if any, to the NASA office that initially furnished the proposal information.

(d) Unless authorized in writing by the NASA official releasing the proposal information, the recipient agrees not to contact either the business entities originating the proposals or any of their employees, representatives, or agents concerning any aspect of the proposal information or extracts covered by this agreement.

(e) The recipient agrees to review his or her financial interests relative to the entities whose proposal information NASA furnishes for evaluation. This duty to review financial interests begins prior to the receipt of the proposal information and continues until the evaluation is completed and the material is sent back to NASA. At any time the recipient becomes aware that he or she or a person with a close personal relationship (household, family members, business partners, or associates) has or acquires a financial interest in the entities whose proposal information is subject to this agreement, the recipient shall immediately advise the NASA official releasing the proposal information, protect the proposal information, and cease evaluation activities pending a NASA decision resolving the conflict of interest.

(f) For purposes of this agreement, financial interests includes, but is not limited to stock ownership, outside employment, spousal employment, profit sharing and actively negotiating for future employment.

_____ _____

Signature of Recipient Date

_____

Printed Name of Recipient

cc: JPL Contract Management Section

NASA Procedural Requirements

JPL NPR 1600
Effective Date:
Expiration Date:

COMPLIANCE IS MANDATORY

Subject: NASA Physical and Program Security

Responsible Office: Office of Protective Services

TABLE OF CONTENTS

PREFACE

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Introduction

1.1 Overview
1.2 Responsibilities
1.3 Best Practices
1.4 Waivers and Exceptions
1.5 Violations of Security Requirements

Chapter 2. Industrial Security

2.1 General
2.2 Department of Defense (DoD) Support

Chapter 3. Physical Security

3.1 Security Control at NASA Centers
3.2 Annual Agency/Center/Program Threat Assessment
3.3 Inspection of Persons and Property
3.4 Security Areas
3.5 Facility Security
3.6 Airfield and Aircraft Security
3.7 Control and Issuance of Arms, Ammunition, and Explosives (AA&E)
3.8 Standards for Secure Conference Rooms
3.9 Design Basis Threat

3.10 Threat and Incident Reporting
3.11 NASA Security Office Special Agent Badges and Credentials (B&C)
3.12 Technical Surveillance Countermeasures (TSCM)
3.13 Protective Services Response to Demonstrations and Civil Disturbances
3.14 NASA National Threat Advisory System NTAS Program
3.15 Hazardous Material Security
3.16 Investigations

Chapter 4. Program Security

4.1 General
4.2 Responsibilities
4.3 NASA Critical Infrastructure (NCI) and Key Resources - NASA Critical Infrastructure Protection Program (NCIPP)
4.4 Operations Security (OPSEC)
4.5 Risk Management Process
4.6 Special Security Programs
4.7 NASA Security Education and Training, and Awareness (SETA) Program
4.8 Self-Inspections

Chapter 5. Training, Certification and Authority of NASA Special Agents, Security Specialists, Contract NASA Security Police Officers and Contract NASA Security Officers

5.1 General
5.2 Applicability
5.3 Responsibility

Appendix A. Definitions
Appendix B. Acronyms
Appendix C. NASA National Threat Advisory System NTAS Actions
Appendix D. NASA Federal Arrest Authority and Use of Force Qualifications and Training
Appendix E. NASA Firearms Qualification Courses
Appendix F.NASA Serious Incident Report Format
Appendix G.Security Area Signs
Appendix H.Identifying and Nominating NASA Assets NASACritical InfrastructureProtection Program (NCIPP)
Appendix I.NASA Security Statistics Format

PREFACE

P.1 PURPOSE

a. This NASA Procedural Requirement (NPR) establishes Agency security and law enforcement services implementation requirements set forth in NASA Policy Directive (NPD) 1600.2, as amended.

b. This NPR prescribes NASA security and protective services procedural requirements for NASA Centers and component facilities in executing the NASA security program to protect people, property, and information. It establishes program specifications necessary to achieve uniformity, standardization, centralization, and decision-making authority where appropriate.

P.2 APPLICABILITY

a. This NPR is applicable to NASA Headquarters and all NASA Centers including Component Facilities, the Jet Propulsion Laboratory and other NASA Contractors, grant recipients, and other partners to the extent specified in their contracts or agreements.

P.3 AUTHORITY

Title 51 U.S.C. §§ 20331, 20332, 20333 and 20334respectively, of the National Commercial and Space Programs Act of December 2010. Public Law 111-314

P.4 APPLICABLE DOCUMENTS AND FORMS

a. 18 U.S.C. § 799, Violation of Regulations of National Aeronautics and Space Administration.

b. 18 U.S.C. § 922 (d) (9) Title 18, USC, Section 922 (d)(9) Update.

c. 42 U.S.C. § 2011 et seq., Atomic Energy Act of 1954.

d. 42 U.S.C. § 13041, Child Care Worker Employee Background Checks.

e. The Homeland Security Act, Pub. L. No. 107-296, Section 2(9).

f. Exec. Order No. 12968, Access to Classified Information, As amended.

g. Exec. Order No. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

h. Exec. Order No. 13526, Classified National Security Information

i. 5 C.F.R. Part 731, Suitability.

j. 5 C.F.R. Part 732, National Security Positions. See 4.8.4.1.1.d

k. Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel, 14 C.F.R. Part 1203 (b).

l. Inspection of Persons and Personal Effects at NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials, 14 C.F.R. Part 1204, subpart 10.

m. Section 4.404(a) of the Federal Acquisition Regulation.

n. National Security Directive (NSD) 63, Single Scope Reliability Investigation.

o. Director of National Intelligence (DNI) Intelligence Community Directive (ICD) Number 705, Sensitive Compartmented Information Facilities (SCIFs), 5/26/2010.

p. National Security Decision Directive (NSDD) 84, Safeguarding National Security Information (Nondisclosure Agreement), 3/11/83.

q. NSDD-298, National Operational Security Program, 1/22/88.

r. Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual, 2/28/06.

s. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection.

t. HSPD-3, Homeland Security Advisory System.

u. HSPD -12, Policy for a Common Identification Standard for Federal Employees and Contractors mm. Department of Justice (DOJ) Report, Vulnerability Assessment of Federal Facilities, June 1995.

v. Homeland Security – Interagency Security Committee Standards (ISC), Physical Security Criteria for Federal Facilities, 2010

w. Homeland Security – ISC Facility Security Level Determinations for Federal Facilities, 2008

x. NASA FAR Supplement 1804.404-70.

y. NPD 1000.3, NASA Organization.

z. NPD 1440.6, NASA Records Management.

aa. NPD 1600.2, NASA Security Policy.

bb. NPR 1441.1, NASA Records Retention Schedules.

cc. NPR 1620.2, Physical Security Vulnerability and Risk Assessments for NASA Facilities and Property.
dd. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

ee. NPR 1660.1, NASA Counterintelligence Program Procedural Requirements.

ff. NPR 2810.1, Security of Information Technology.

gg. NPR 8000.4, Agency Risk Management Procedural Requirements.

hh. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

ii. NPR 8715.3, NASA General Safety Program Requirements.

jj. NPR 8820.2, Facility Project Requirements.

kk. NASA-STD-8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics.

ll. DD Form 254, Contract Security Classification Specification.

mm. SF 31, Agency Information Security Program Data Report.

nn. SF 312, Classified Information Nondisclosure Agreement.

P.5 MEASUREMENT/VERIFICATION

a. Center Directors and Center Chiefs of Protective Services (CCPS) or their designees determine and document compliance by applying a verification approach that is tailored to meet the needs of JPL . The Office of Protective Services (OPS) conducts functional reviews of JPL s and conducts spot-checks and inspections to review Center compliance and implementation.

b. To determine the OPS compliance with the requirements contained in this NPR, internal and external auditors responsible for verifying Headquarters requirements and processes shall evaluate performance against the requirements contained within this NPR.

P.6 CANCELLATION

NPR 1600.1, NASA Security Program Procedural Requirements w/Change 2, dated April 1, 2009. Chapters 6-9 and Appendices D, E, F, G, and H.

/S/
Dr. Woodrow Whitlow, Jr.
Associate Administrator
Mission Support Directorate

Chapter 1: Introduction

1.1 Overview

1.1.1 This NPR establishes Agency-wide program policy and guidance for physical security, industrial security, program security, and NASA Federal Arrest Authority (FAA).

1.1.2 This NPR establishes standards and specifications required to maintain consistency and uniformity for the protection of NASA assets, while considering the unique requirements, circumstances, and environments of individual NASA Centers and locations. During emergencies or periods of increased threat, exigent circumstances may require suspension of certain provisions of this NPR. In that event, immediate coordination with the Assistant Administrator (AA), Office of Protective Services is necessary.

1.1.3 This NPR also presents terminology, definitions, and security measures that are intended to facilitate coordination and support with other U.S. federal agencies such as the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and DoD.

1.1.4 This NPR provides for the assignment and delegation of certain security and protection responsibilities required by law and sound management practice.

1.2 Responsibilities

1.2.1 Security is the direct, immediate, and inherent responsibility of all NASA personnel, contractors, and others who are granted access to NASA Centers, facilities, information and technology. General security responsibilities are set forth in this NPR. Specific policy requirements are cited in this NPR.

1.2.2 The NASA Administrator is responsible for implementing a comprehensive and effective security program for the protection of people, property, and information associated with the NASA mission. The Administrator shall appoint an Assistant Administrator, (AA) Office of Protective Services.

1.2.3 The AA, Office of Protective Services, shall:

a. Oversee Agency implementation, integration of, and compliance with the NASA security program by providing executive management policy direction and ensuring, through Agency advocacy, adequate resources are identified and committed to accomplish the security mission in support of the overall NASA mission, NASA Strategic Plan, and national-level security requirements.

b. Provide functional and operational support for physical, industrial, and program security policy formulation.

c. Serve as the Agency point of contact with the intelligence community for intelligence matters and ensure development and issuance of policy and requirements related to NASA's Counterintelligence and Counterterrorism (CI/CT) program.

d. Ensure law enforcement and investigative activity performed in conjunction with OPS security responsibilities at NASA installations is developed and implemented consistent with authorities granted under the PL 111, 314 and in concert with the NASA Office of Inspector General (OIG), local, state, and Federal law enforcement agencies.

e. Serve as the Agency Critical Infrastructure Assurance Officer (ACIAO) responsible for approving all Center proposals for additions and deletions to the NASA Critical Infrastructure (NCI) Inventory List when such proposals are concurred on by the respective Mission Directorate Associate Administrator.

f. Comply with the requirements of HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection.

g. Effectively collaborate with the Chief Information Officer (CIO) to ensure critical cyber assets are identified and included in the NCI inventory.

h. Establish and implement organizational standards that ensure NASA security programs are appropriately configured, properly staffed with qualified security professionals, and adequately funded to enable each NASA Center to properly and efficiently manage day-to-day security operations while allowing for transition to increased threat environments and emergency scenarios, including appropriate continuity of operations and contingency operations capabilities.

i. Develop and issue, under separate NPR, asset specific physical security vulnerability and risk assessment (RA) requirements including physical and procedural standards to ensure consistency and uniformity in the application of security measures.

j. Establish, disseminate and enforce comprehensive performance standards that address overall security capabilities, training, response to likely emergencies and contingencies, and general compliance with Agency standards. Conduct inspections as well as scheduled and unscheduled audits to ensure compliance and efficiency.

k. Develop and disseminate Agency antiterrorism program standards and procedures necessary to ensure appropriate response to threats and acts of terrorism on NASA installations and component facilities.

l. Implement and manage procedures for certifying and obtaining accreditation of IT resources that process Classified National Security Information (CNSI) and data.

m. Provide overall focus and direction for protecting the NASA workforce, visitors, programs, and infrastructure.

n. Provide central oversight in the development of Agency policy regarding physical security, infrastructure protection, program security, industrial security and law enforcement.

o. Serve as the Agency oversight official for implementation and management of the Agency FAA Program and Use of Force policy in compliance with 42 U.S.C. 2456a, and 14 C.F.R. Part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.

p. Develop and implement Agency policy and procedural requirements to ensure investigation activity is coordinated and/or referred to the NASA OIG, local, state, and Federal law enforcement agencies as defined in appropriate memoranda of agreement (MOA).

q. Establish and maintain a Central Adjudication Facility to adjudicate all Agency requests for security clearances for access to CNSI.

r. Coordinate security and law enforcement policy with the Office of General Counsel.

s. Evaluate compliance with this NPR and overall effectiveness of the NASA security program through periodic site visits.

t. Manage the NASA Critical Infrastructure Protection Program (NCIPP).

u. Develop and implement procedures for managing and safeguarding CNSI.

v. Ensure that the NASA security program operates in compliance with national security policy, applicable DHS program directives, and other national-level regulations.

w. Ensure appropriate physical security and antiterrorism construction standards are developed and published in cooperation with NASA Facilities Engineering Division personnel.

x. Coordinate NASA representation on all security policy development forums and committees.

y. Serve as NASA representative to the DHS Interagency Security Committee.

1.2.4 The Director Jet Propulsion Laboratory (JPL) shall:

a. Provide current and effective security for all JPL and Component Facility personnel, property, facilities, operations and activities.

b. Appoint a qualified and experienced CCPS, in accordance with NPD 1000.3, The NASA Organization. Minimum qualifications include:

(1) Sufficient authority and resources to accomplish national, Agency, and Center security goals and objectives with coordination and concurrence of the AA, OPS.

(2) Relevant experience in the law enforcement, military intelligence, or security professions.

(3) Leadership and managerial experience at a proven level commensurate with the expectations of the CCPS position.

(4) Ability to obtain and maintain a Top Secret security clearance.

c. In accordance with this NPR, establish, fund, and maintain a comprehensive security program through the CCPS. This includes:

(1) Personnel, facilities, and equipment necessary to implement and sustain an effective security program.

(2) Appropriate training and professional certification of security personnel, as established by the AA, OPS.

(3) The development and management of Center-specific security program policy and procedural requirements that implement this NPR's requirements.

d. When recommended by the CCPS and Center Critical Infrastructure Assurance Officer (CIAO), propose NCI and Key Resource assets for inclusion in the NCI Inventory to the Mission Directorate Associate Administrator(s).

e. Act as the Designated Official (DO) and Risk Acceptance Authority (RAA) for Center security program risk management determinations that do not require waiver of national security requirements.

f. Appoint a senior management official to serve as the JPL Critical Infrastructure Assurance Officer (CIAO).

1.2.5 The Director Jet Propulsion Laboratory (JPL) shall:

a. Provide current and effective security for all JPL and Component Facility personnel, property, facilities, operations and activities. Support and strengthen the overall security posture of NASA, including NASA's Counterintelligence (CI) / Counterterrorism (CT) Program.

(1) Support a proactive program to detect, deter, and/or neutralize attempted or probable acts of subversion, sabotage, terrorism, or espionage directed at NASA personnel, technologies, and resources, or the actual, attempted or probable compromise of national security.

(a). Expeditiously notify the servicing NASA CI Special Agent (CISA) of any incidents, events, or circumstances of actual or suspected loss or compromise of sensitive but unclassified information, classified national security information (CNSI), and NASA critical information (NCI).

(b.) Expeditiously notify the servicing NASA CISA of any occurrences of unusual or suspicious contact between NASA employees and foreign nationals.

(c.) Ensure NASA/JPL/Caltech employees expeditiously report to the servicing NASA CISA any information concerning actual or suspected espionage.

(2) Take measures to identify and resolve matters of potential counterintelligence (CI) concern, and promote proactive interaction, communications, and liaison with NASA (e.g., the NMO Chief of Security; NMO Director; NASA OIG), JPL managers (e.g., program/project manager, line managers, and supervisors), JPL operational elements (e.g., export control, NASA technology programs and innovative technology transfer partnerships, launch approval services, JPL Research Network access program for science and foreign personnel community; counterfeit/defective parts avoidance, investigation, and reporting), and JPL application elements (e.g., reimbursable programs; National Space Technology Applications office; International research and development office; JPL Innovation Foundry office; higher and informal education outreach and collaboration).

1.2.6 The JPL CCPS shall:

a. Act as the principal advisor and authority to the JPL Director in all matters relating to the NASA security program, as established and defined in NPD 1600.2. Minimum qualifications for the CCPS include:

(1) Relevant experience in the law enforcement, military intelligence, or security professions.

(2) Leadership and managerial experience at a proven level commensurate with the expectations of the CCPS position.

(3) Ability to obtain and maintain a Top Secret security clearance.

b. Develop, implement, and maintain written JPL-specific security program policy and procedural requirements that implement the requirements of this NPR.

c. Direct, plan, control, and evaluate the overall JPL security program, regardless of the specific security discipline and processes involved.

d. Through periodic assessments, determine the adequacy of physical security, loss prevention, and antiterrorism programs and recommend improvements and associated budget requirements to the JPL Director.

e. Using all available sources of intelligence information (i.e., NASA CI/CT program, local law enforcement, the NASA OIG, and other federal agencies), continuously evaluate Center and program-level criticality and vulnerabilities and local threats, and prepare appropriate countermeasures tailored to the resources requiring protection, specifically identifying Center Critical Infrastructure and Key Resources, in coordination with JPL CIO and CIAO, for inclusion in the NCIPP.

f. Establish priorities for the effective deployment of Center security resources and processes during routine and emergency situations.

g. Integrate and maintain oversight of all Center security activity, including those of tenant organizations to the extent feasible.

h. Establish and maintain annual security awareness and training programs for Center employees.

i. Participate as a principal member of Center teams dealing with resolution of workplace violence and protection issues.

j. Maintain a Center map of the precise jurisdictional boundaries of Center geographical areas, as determined by the NMO and JPL Chief Counsels.

k. Maintain Center security program statistics and provide quarterly reports to the AA, OPS.

l. Establish and maintain all organization informational and operational files pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules.

m. Establishing a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.

1.2.7 JPL Program, Line Managers, and Supervisors shall:

a. Support the CCPS in the implementation of comprehensive security programs and mission-oriented protective services for JPL, along with individual programs and projects.

b. Manage the safeguarding of classified information to include management of personnel holding security clearances.

c. Ensure employment of CCPS recommended security and loss-prevention measures within their programs and/or project or organizations.

d. Report adverse information discovered to CCPS.

1.2.8 Individual JPL employees shall:

a. Report suspicious activity, criminal activity, violations or suspected violations of national security, and other Center security responsibilities to the Security Office.

b. Be aware of and comply with individual responsibilities and roles in maintaining the Agency and Center security program.

c. Protect Government property, CNSI, and sensitive information in accordance with the requirements of this NPR and the NISPOM.

d. Cooperate with Center and Agency security officials during inquiries and investigations.

1.3 Best Practices

1.3.1 The AA, OPS and CCPS shall develop and share “best practices” programs and processes.

1.4 Waivers and Exceptions

1.4.1 Centers may occasionally experience difficulty in meeting specific security program requirements established in NPRs. The process for submitting requests for waivers or exceptions to specific elements of the NASA Security Program is as follows:

a. The asset, program, or project manager and CCPS shall justify the waiver by documenting a security risk analysis that details the following areas: cost of implementation, impact of loss of capability to Center, potential impact/compromise of national security information, injury or loss of life, impact to Center mission and goals, and impact to unique Center capabilities. Justification must also include an explanation of any compensatory security measures implemented in lieu of specific requirements. The waiver request will be submitted to the JPL Director.

b. The JPL Director shall either recommend approval or return the waiver request to the CCPS for further study or closure. Upon concurrence, the JPL Director will forward to the waiver to the Headquarters Associate Administrator responsible for functional oversight.

c. Associate Administrator shall forward waiver requests to the AA, OPS at Headquarters or return proposals to JPL Director for further study or closure.

d. The AA, OPS shall return the waiver request to the appropriate JPL Director with one of three dispositions: approved, for further study, or denial and closure.

1.5 Violations of Security Requirements

1.5.1. Center Directors, Headquarters Operations Director, the AA, OPS, or the CCPS shall order the removal or debarment of any person who violates NASA Security requirements and or whose continued presence on NASA property constitutes a security or safety risk to persons or property. Any determinations to reconsider granting access subsequent to the removal action by these individuals must receive the concurrence, in writing, of the AA, OPS.

1.5.2 The CCPS shall order the temporary removal or debarment of any person who violates NASA Security requirements and whose continued presence on NASA property constitutes a security or safety risk to persons or property.

1.5.3. Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA Security program is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. 799, that provides for fines or imprisonment for not more than 1 year, or both.

Chapter 2. Industrial Security

2.1 General
2.1.1 This chapter provides procedural requirements for implementation of the industrial security program in accordance with the National Industrial Security Program Operating Manual (NISPOM). The NISPOM applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States and its territories.
2.1.2 Industrial security pertains to, but is not limited to, the requirement to review all programs/projects in accordance with associated regulations, classified contract administration rules and requirements, and the processing and control of classified visits for cleared Government and contractor employees.
2.1.3 This chapter is applicable to contracts, grants, cooperative agreements, and other binding transactions in which performance shall require access to CNSI by the contractor, supplier, grantee, or its employees. It does not apply to agreements with other Federal agencies.
2.1.4 The processing and control of classified and unclassified visits to a Center in relation to classified contracts is the responsibility of the CCPS and shall be covered in written local security procedures tailored to that Center.
2.2 DoD Support
2.2.1 The Defense Security Service (DSS) administers the National Industrial Security Program on behalf of NASA. This support extends to contractor sites. The CCPS is responsible for oversight of industrial security services of contractors on NASA Centers and facilities, excluding personnel security clearances.
2.2.2 The standard security provisions of NASA classified contracts require the contractor to possess a facility security clearance and be assigned a Cage Code, execute a DoD Contract Security Specification (DD Form 254), and complete other applicable industrial security forms that require the contractor to comply with the NISPOM for industrial security matters.
2.2.3 NASA exercises the right to inspect JPL contractor operations located on NASA property that are involved in accessing and safeguarding classified information in accordance with the NISPOM and applicable NASA Security NPRs.

Chapter 3. Physical Security

3.1 Security Control at NASA Centers

3.1.1 The OPS has programmatic responsibilities for managing information technology with the CIO's Office to properly manage identity, credential, and access management (ICAM) services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration. In order to meet Federal requirements established by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), and documented in the Federal ICAM Roadmap and Implementation Guidance, NASA Procedural Requirement (NPR) 2841.1 establishes Agency-wide enterprise services that all Centers and applications shall use. All NASA Centers shall follow this NPR and manage their physical security programs in compliance with NPR 2841.1.

3.1.2 JPL shall apply and maintain appropriate physical security measures necessary to provide for protection of persons, missions, information, and property.

3.1.2.1 JPL shall be financially responsible for the lifecycle management of all Center Premise Access Control Equipment, integrated intrusion detection, closed-circuit video equipment, and any peripheral equipment. 3.1.3 Procedures shall be established to ensure only authorized personnel are admitted to NASA Headquarters and Centers.

3.1.3 Positive access controls to JPL shall be implemented at all entry points by armed., uniformed Security Officer/Security Police personnel and additional access controls, including armed personnel may be established at individually designated security areas and facilities within JPL to preclude unauthorized access to critical areas, information, or personnel. Security Officers/Security Police will be used throughout JPL to provide traffic safety, detect and deter criminal conduct, enforce security rules and policies, detect unauthorized personnel, act as first responders to critical incidents, establish emergency or temporary control points, respond to calls for assistance, and perform other duties as determined by the CCPS.

3.2 Denial of Access

3.2.1 The CCPS shall temporarily deny access to JPL facilities any person who violates NASA Security requirements and whose continued presence on NASA property constitutes a security or safety risk to persons or property. This temporary denial of access shall become permanent after 10 working days unless:

a. The CCPS reverses the decision to deny access upon receipt of additional information.

b. The non-NASA employee requests an appeal and the appeal panel reverses the denial of access.

3.3.1 Reserved

3.3.2 Reserved

3.3.3 Non-NASA Employee Denial of Access Appeal Process

3.3.4 Upon temporary denial of access by the CCPS, the Non-NASA employee denied access either personally or through their Government Sponsor, may appeal to the CCPS, seeking review of the decision only as follows.

3.3.5 Within 10 working days of being notified of the denial of access, the removed non-NASA employee must submit a written request for review of the denial of access, and include any and all written materials as he/she desires to be considered on that review. An additional 5 working days for an individual's submission shall be granted on written request, but only if the individual has made the initial request within the first 10 working days following notification of the denial of access. If the individual supplies new information, the CCPS may augment any written submission on the individual.
3.3.6 Upon submission of the individual's written materials, the JPL Director shall convene a three (3) person access appeals panel to review the CCPS determination. The access appeals panel shall consist only of Federal employees. It shall include (1) an attorney from JPL Office of

General Counsel; (2) a disinterested employee from JPL management, and (3) an employee from Center Protective Services.

3.3.7 The Access Appeals Panel will assess the CCPS denial determination in terms of compliance with access standards as promulgated by 5 C.F.R. §731.202. The Panel will submit a written statement briefly setting forth their conclusions and decision. The Panel may (1) uphold the denial of access, (2) reverse the denial of access, or (3) return to the matter for additional and specified processing. Returning a matter without specific guidance is discouraged. A minority report may be submitted, and should be succinct as to reasons for disagreement with the majority. The Access Appeals Panel shall accomplish its review within 5 working days of the individual making a written submission. The JPL Director may extend the appeal period an additional 5 working days if circumstances warrant.

3.3.8 The decision of the panel is final, and further review of the Access Appeals Panel decision is not provided for. The NASA Administrator, however, reserves the right and authority to direct that any grant or denial of access decision (including subsequent appeal) be held in abeyance pending additional discretionary review by HQ. This reservation of authority by the Administrator does not convey any substantive right to affected individuals.

3.3.9 If the individual denied access declines to appeal, either through communicating in writing or time for the appeal has expired, the original determination will be final. During this appeal process the individual is not granted access to any NASA facility.
3.3.10 Upon employee resignation, termination of employment , or release of the non-NASA employee by his/her employer or sponsor, the appeal process shall stop and the denial of access decision by the CCPS shall become final.

3.4 Annual Agency/Center/Program Threat Assessment

3.4.1 The Director NASA Counterintelligence/Counterterrorism Division shall publish and disseminate an annual NASA Threat Assessment. Additionally, Center and program specific threat assessments will publish an annual NASA CI/CT Threat Assessment that provides a comprehensive evaluation of those threats under the CI/CT investigative purview.

3.5 Inspection of Persons and Property

3.5.1 General.

3.5.1.1 Consistent with NASA's requirement to ensure appropriate protection for personnel, property, and facilities, NASA reserves the right to conduct an inspection of any person and property in his possession as a condition of admission to, or continued presences on, or upon exit from, any NASA facility. Requirements, policy, and procedures for all aspects of this program are contained in 14 C.F.R. Part 1204, subpart 10.

3.5.1.2 All NASA entities must adhere to these requirements in the implementation of this program.

3.5.2 Requirements. Consistent with 14 C.F.R. Part 1204

3.5.2.1 All entrances to NASA real property or installations shall be conspicuously posted with the following notices:

a. “CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from, this installation is contingent upon your consent to inspection of person and property.”

b. “UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you may not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property.”

3.5.3 The CCPS is responsible for this program. Security Officers/Security Police may use inspection tools and detection devices (mirrors, x-ray, and other sensing devices) and/or canines as necessary.

3.5.3.1 Training for security personnel conducting searches shall include:

a. Appropriate search techniques for the type of vehicle being searched.

b. Key locations where devices or other contraband may be secreted.

c. Procedures for confiscating illegal or dangerous items, detaining of individuals and referring incidents to appropriate external law enforcement.

3.5.3.2 Such inspections shall be conducted in accordance with the following guidelines:

a. Consent to Inspection Notices shall be prominently posted at entrances to NASA Centers and Facilities. Language for these notices is contained in 14 C.F.R. §1204.1003, Subpart 10.

b. Only NASA security personnel or members of the installation’s uniformed security force will conduct inspections. Such inspections will be conducted in accordance with guidelines established by the AA, OPS.

c. Security personnel shall present appropriate NASA credentials to the subject of the inspection.

d. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of JPL (weapons, drugs, and explosives), the items shall be confiscated, the individual will be denied admission to, or be escorted from, JPL; or detained at the scene. The appropriate law enforcement authorities will be notified immediately.

e. If, during an inspection conducted pursuant to this subpart, an individual is in possession of U.S. Government property without proper authorization, that person will be required to relinquish the property to the security representative pending proper authorization for the possession of the property or its removal from the installation. The individual relinquishing the property will be provided with a receipt for the property.

3.6 Security Areas Rewrite

3.6.1 Types of Security Areas.

3.6.1.1 Controlled Area (formerly Restricted Area). An area in which security measures are taken to safeguard and control access to property and hazardous materials, or other sensitive material or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. The Controlled Area shall have a clearly defined perimeter, but permanent physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All material in question will be secured during non-working hours in approved storage repositories or secured using other methods approved by the CCPS.

3.6.1.2 Limited Area. An area in which security measures are taken to safeguard or control access to classified material or unclassified property warranting special protection or property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. A Limited Area shall also have a clearly defined perimeter but where it differs from a Controlled Area is that permanent physical barriers and access control devices, including walls and doors with locks or access devices are implemented to assist the occupants in keeping out unauthorized personnel. During working hours, personnel within the area will be responsible for challenging all persons who may lack appropriate access authority. Sensitive material, property and hazardous material can be stored in this area in approved containers. All CNSI material will be secured during non-working hours or when no cleared personnel are present in GSA approved security containers or other methods approved by the CCPS. When the Limited Area is not in use, access to the access control devices (i.e., keys, combinations to mechanical/electronic cipher locks, badge reader control) will be limited to authorized personnel. To prevent unauthorized access to such property, visitors will be escorted or other internal restrictions implemented, as determined by the CCPS. All facilities designated as NASA Critical Infrastructure (NCI) or key resource will be designated as, a minimum, “Limited” areas.

3.6.1.3 Exclusion Area (formerly Closed Area). An area that is a permanent facility dedicated solely for safeguarding and use of CNSI and it is used when vaults are unsuitable or impractical and where entry to the area alone provides visible or audible access to classified material. .

3.6.2 Establishment, Maintenance, and Revocation.

3.6.2.1 Establishment. Center Directors; JPL Director; Director, Headquarters Operations; the AA, OPS; and the CCPS shall establish, maintain, and protect such areas designated as Controlled, Limited, or Exclusion depending on the rationale for the establishment of the area and the area’s vulnerability to unauthorized access. Only the AA, OPS or the CCPS will establish an area functioning for the protection and use of CNSI. Only a coordinating office in AA, OPS will establish a Special Access Program Facility (SAPF) or SCIF based on legal authority or Memorandum of Understanding (MOA) with the Cognizant Security Authority.

3.6.2.2 Maintenance. Security measures shall vary according to individual situations; however, the following minimum-security measures will be taken in all security areas:

a. Post appropriate signs at entrances and at intervals along the perimeter of the designated area, for the facility, to provide reasonable notice to persons that the area is a security area. SAPFs and SCIFs are not required to use identifying signs due to Operations Security (OPSEC) concerns.

b. Signs must read as shown in Appendix G.

c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

3.6.2.3 Revocation. Once the need for a security area no longer exists, the area must return to normal procedures as soon as practical.

3.6.3 Access. Only those NASA employees, contractors, and visitors who need access and who meet the following criteria shall enter a security area unescorted. All other individuals requiring access must be escorted by an authorized NASA employees or NASA contractors.

3.6.3.1 To enter a Controlled Area unescorted, individuals must undergo the appropriate investigation or procedures required for that area as established by the individual Center; when an investigation is required, it shall be, at a minimum, a National Agency Check with Inquiries for civil service employees and for non-NASA personnel.

3.6.3.2 To enter a Limited Area, unescorted individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a National Agency Check with Inquiries for unclassified information and material.

3.6.3.3 To enter a Exclusion Area, unescorted individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

3.6.3.4 Center Directors and the AA, OPS shall rescind previously granted authorizations to enter security areas when an individual's clearance and need-to-know is no longer justified, their presence threatens the security or safety of the property, or when access is no longer required for official purposes.

3.6.4 The CCPS will implement and enforce the following:

a. JPL Protective Services Office shall conduct a continuing review of JPL facilities to ascertain the locations of sensitive activities or functions requiring protection.

b. Centers must have written security plans to accomplish the protection of Limited and Exclusion Areas. Copies of those plans shall be maintained in JPL Protective Services Office, and a copy must be available within the protected area at all times. Plans must include, as a minimum, the following items:

(1) The method used to alert and educate affected employees.

(2) Details on how the policy shall be enforced, including how devices such as cell phones, cameras and other electronic equipment will be controlled.

(3) Procedures for conducting an unannounced spot-check.

3.7 Facility Security

3.7.1 NASA Buildings and Facilities.

3.7.1.1 Facilities and buildings shall be provided the level of security commensurate with the level of risk as determined by conducting a risk assessment consistent with NPR 1620.2:

a. Physical security enhancements for existing facilities shall be established based on an assessment of the type of vulnerability (ies) identified during a security risk assessment, development of strategies to address identified vulnerabilities, and implementation of selected security measures, both physical and procedural.

b. Minimum physical security requirements shall be incorporated into construction of facilities projects in accordance with the requirements established by NPRs, Facility Engineering, and the Interagency Security Committee (ISC), Physical Security Criteria for Federal Facilities.

c. Procedural security measures shall be developed, implemented, and properly disseminated to ensure awareness, adherence, and compatibility with implemented physical security measures.

3.7.2 Security Fencing. Minimum standards for NASA perimeter fencing are established in NPR 1620.3.

3.7.2.1 Selection and placement of security fencing shall be in accordance with the requirements established in NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

3.7.2.2 When used properly and in conjunction with other physical and procedural security measures, fencing provides a cost-effective method for delineating U.S. Government property boundaries, establishing clearly visible protected borders, and serving as a deterrent to most would-be trespassers.

3.7.3 Keys, Locks, Locking Devices (hasps and chains), and Protective Seals.

3.7.3.1 Center Security Officials shall establish key and lock control policies and procedures in accordance with . NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

3.7.4 Minimum Protection Considerations for NCI Facilities or areas housing NCI assets.

3.7.4.1 Centers shall designate a Facility Security Manager or equivalent for each facility. The Facility Security Manager shall ensure that security training is provided to employees with access to the NCI asset and that program management implements and enforces the security requirements developed for the asset.

3.7.4.2 The NASA Enterprise Physical Access Control System shall be employed at all times.

3.7.4.3 Based on a risk assessment, Intrusion Detection Systems (IDS) and other surveillance systems shall be appropriately monitored and receive appropriate response by armed mobile security personnel capable of responding within locally established time limits, not to exceed 5 minutes. Unannounced response tests are to be performed at a minimum of twice in a calendar year.

3.7.4.4 Security fencing shall be installed when the need is identified by the security risk assessments.

3.7.4.5 Security lighting shall be installed at key areas around the facility to facilitate, to the extent possible, detection of intruders and will follow the current Guidelines for Security Lighting for People, Property, and Public Spaces from the Illuminating Engineering Society of North America.

3.7.4.6 All personnel requiring unescorted access to the NCI shall have been investigated in accordance with NASA personnel security investigation requirements. All personnel not meeting investigative requirements will be escorted.

3.7.4.7 Personnel shall properly display issued photo-ID. The badge will be worn at all times while on Center, in plain sight, picture side out, above the waist, and below the head. Exceptions to this method of display may occur for safety reasons such as in laboratories. .

3.7.4.8 NCI shall be designated and properly posted as a NASA “Limited” Area, at a minimum. See Chapter 3.4 for criteria regarding designation of NASA Security Areas.

3.7.4.9 After completion of an initial security RA upon designation as an NCI asset, reassessments shall be conducted every 3 years at a minimum, or more frequently as circumstances warrant.

3.8 Childcare Centers

3.8.1 Childcare centers established under the auspices of NASA sponsorship shall, with coordination and approval of the CCPS:

a. Establish positive measures to ensure the proper identification of authorized parents and others authorized to pick up children.

b. Establish physical and procedural security measures necessary to separate and control childcare areas from visitor reception areas.

c. Install duress system buttons at key locations in accordance with Center Protective Services specifications.

d. Install closed circuit television (CCTV) capability in key locations in accordance with Center Protective Services specifications.

e. Ensure adequate mechanisms are in place for emergency notification and response.

f. Ensure appropriate security lighting is installed at key areas around the facility to enable detection of would-be intruders.

g. Ensure that a Childcare National Agency Check with Inquiries is performed on all employees of the Childcare Center.

3.8.2 Minimum physical security and antiterrorism construction standards for new NASA Childcare Centers shall be incorporated into construction of facilities projects in accordance with the requirements established in NPR 8820.2E, NASA Facility Project Implementation Guide, Interagency Security Committee (ISC) “Physical Security Criteria for Federal Facilities,” and the ISC “Child-Care Centers Annex 1” to Physical Security Criteria for Federal Facilities.

3.9 Visitor Centers and Outdoor Displays

3.9.1 NASA Visitor Centers and outdoor displays traditionally house one-of-a-kind, irreplaceable items of historical significance. The physical security requirements of this NPR apply to locations under NASA control and jurisdiction. When NASA property or artifacts are on loan or display outside a NASA controlled facility, loan agreements shall detail the physical security measures to be taken to safeguard NASA property.

3.9.2 The degree of protection necessary must be determined locally and in partnership between the Visitor Center curator, CCPS, and supporting facility engineers.

3.9.3 Visitor Center buildings and apertures providing access to the building must be modified or constructed so as to delay a determined intruder long enough for a security force to respond.

3.9.4 Interior and exterior security lighting shall be provided in all Visitor Center buildings in which sensitive property is located.

3.9.5 Viewing surfaces of exhibit or display cases shall be constructed of materials resistant to breakage and must be securely fastened into frames or into the container.

3.9.6 Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.

3.9.7 Pilferable component parts shall be secured to the display or removed at the close of each business day.

3.10 IDS, CCTV, and Electronic Access Control System Minimum Standards and Integration.

3.10.1 IDS, CCTV, and Electronic Access Systems are the responsibility of the CCPS. These systems provide an effective means to enhance any organization’s physical security program. If employed correctly and managed appropriately, these systems offer a wide range of coverage options.

3.10.2 The CCPS shall:

a. Determine, in coordination with facilities engineering personnel with the appropriate expertise in security systems design, integration, and operation overall performance requirements for IDS, CCTV, and the Electronic Physical Access Control Systems.

b. Establish and operate a 24-hour monitoring site where emergency response can be dispatched upon need.

3.10.3 Individual, stand alone systems offering no centralized monitoring oversight and alarm response capability (including internally-monitored systems) are not authorized.

3.10.4 For those facilities protected under the National Preservation Act of 1966, implementation of security measures shall be those measures allowable under the Act, to the extent necessary and practical. See NPR 1620.3

3.11 Control and Issuance of Arms, Ammunition, and Explosives (AA&E)

3.11.1 Authority.

3.11.2 The AA, OPS is the approval authority for the CCPS to carry firearms. The AA, OPS may withdraw weapons carry authority for any NASA Special Agent, Security Specialist, or Armed Security Officer if deemed in the best interest of the Agency.

3.11.3 Center CCPS shall direct or grant approval for their Center's NASA SA and designated NASA Security Specialists and Contractor security personnel to carry firearms.

3.12 Responsibilities.

3.12.1 NASA certifying officials, described in APPENDIX A. Definitions, shall ensure compliance with the requirements of this section.

3.12.2 NASA employees and contractors to whom firearms are issued are responsible for strict compliance with all the conditions regarding the carrying and use of firearms as established herein and set forth at 14 C.F.R. Part 1203b, Security Programs, Arrest Authority and Use of Force by NASA Security Force Personnel.

3.12.3 NASA security personnel and contractors shall not carry firearms outside the 50 States, the District of Columbia, and U.S. territories (Puerto Rico, Guam, U.S. Virgin Islands, American Samoa) without the advance approval of the AA, OPS.

3.13 Reserved

3.14 Reserved

3.15 Firearms Instruction.

3.15.1 The certifying official shall designate a firearms instructor, who will inform the certifying official in writing of an individual's knowledge of the rules of firearm safety and the content of this NPR.

3.15.2 In cases involving a contractor Security Officer force, the firearms instructor may be appointed from the Security Officer force complement.

3.15.3 Minimum standards shall be met before a firearms instructor or certifying official will consider an individual qualified to carry firearms.

3.15.4 Recent firearms training and experience during prior employment, such as the FBI, Secret Service, police, military, or other significant and qualifying experience, shall meet NASA standards if the individual has qualified under all provisions of this chapter within the past 30 days.

3.15.5 These qualifications shall be verified by a review of employment and training history either through an interview with previous management or visual inspection of documented training history.

3.15.6 Appropriate NASA training, including firearm safety procedures and use of deadly force, followed by obtaining a qualifying score on a recognized course as specified in paragraph *3.16.2* below, shall also be required.

3.16 Reserved

3.17 Reserved

3.18 Records.

3.18.1 The law enforcement training originator shall maintain records of personnel certified to carry firearms, including the basis for qualification, qualifying scores, rounds fired, and all other pertinent data. Records are to be destroyed 5 years after employee separation.

3.18.2 Records shall be destroyed 5 years after employee separation.

3.19 Firearms Standards.

3.19.1 CCPS shall utilize only firearms listed in the NASA Approved Firearms List (AFL) to arm their civil service and contractor security staff.

3.19.2 The AFL is approved by the AA, OPS and maintained by the NASA Federal Law Enforcement Training Academy (NFLETA). The AFL may be waived or modified only by the AA, OPS.

3.19.3 Training, qualifications, and certification for all approved firearms shall be *documented per paragraph 3.7.10.*

3.20 Modifications.

3.20.1 No modifications to the operating system, firing mechanism, and/or trigger groups shall be made to any NASA approved firearms.

3.20.2 Only Center armorers will modify grips, sights, and control levers to best suit individual users.

3.21 Handguns.

3.21.1 NASA Contractors shall only carry NASA issued and approved rifles, shotguns, and semi-automatic pistols in calibers., 9mm or .40.

3.21.2 Uniformed contractors at JPL must be armed with the same make and model handgun.

3.21.3 Emergency Response Teams/ERT teams may carry a different make and model.

3.21.4 NASA Civil Service personnel shall carry the same make and caliber, but may vary the model to suit individual users.

3.21.5 Handguns must always be worn in standard, commercially available holsters; uniformed officers must use holsters with a retention device.

3.21.6 Patrol Rifles. At the discretion of the CCPS, contractors shall be armed with semi-automatic or select fire patrol rifles.

3.22 Patrol Shotguns.

3.22.1 At the discretion of the CCPS, contractors and Civil Service personnel shall be armed with semi-automatic or pump action 12 gauge shotguns.

3.22.2 Shotguns used to employ “less-lethal” ammunition shall be solely dedicated for this use and be clearly identified as less-than-lethal weapons.

3.22.3 Submachine guns. At the discretion of the CCPS, contractor security force may be armed with submachine guns.

3.22.4 Other approved firearms. At the discretion of the CCPS, and with the consent of the AA, OPS, other firearms may be utilized to meet Center security requirements.

3.22.5 The user of any NASA approved firearm must meet the training and certification requirements of paragraph 3.7.8.

3.22.6 The use or carrying of a firearm is limited to the approved weapons with which the individual is currently qualified with.

3.23 Ammunition.

3.23.1 Only premium, commercially manufactured, duty ammunition shall be issued.

3.23.2 Duty ammunition shall be expended at training sessions at least once every 12 months to ensure use of fresh duty ammunition.

3.23.3 Normal training ammunition shall be commercially manufactured “lead-free” training ammunition designed for range use.

3.24 Firearm maintenance.

3.24.1 All firearms shall be periodically inspected and kept in good working order by a qualified gunsmith/armorer.

3.24.2 Ammunition, holsters, and related equipment shall be periodically inspected for deterioration and kept in good working order.

3.25 Accountability of AA&E.

3.25.1 The control and custody of all AA&E within a Center shall be under strict accountability at all times and is the ultimate responsibility of the CCPS.

3.25.2 The CCPS shall appoint a custodian for all AA&E within Center Protective Services, within each contractor security force, and within each non-security organization using any type of AA&E, including explosives, propellants, or ammunition, for research or testing purposes.

3.25.3 Each custodian shall maintain an ongoing inventory of all AA&E. The inventory will indicate:

a. The date and method of acquisition of all firearms and ammunition.

b. Full identifying data, the caliber, make, and serial number of each firearm.

c. Amounts of basic load and training ammunition on-hand.

d. Types and amounts of explosives, (fragmentary, flash-bang grenades, C/S, pepper spray).

3.25.4 The CCPS shall report all Center AA&E data to the AA, OPS on an annual basis the third week after the end of the fourth quarter of each fiscal year.

3.25.5 Current contractor firearm data shall be maintained and made available to Center Protective Services Office upon request.

3.25.6 A receipt system for recording the issuance, transfer, and return of all firearms, ammunition, and explosives, shall be maintained by the custodian. Receipts will include the following details:

a. Dates of issuance, transfer, or return to custody.

b. Serial numbers of firearms.

c. Numbers and types of assigned explosives.

d. Types and numbers of ammunition on-hand.

e. Signatures of recipients.

f. Signatures of custodians upon return of the firearms and explosives. (NOTE: Both NASA personnel and contractor receipts shall be retained by JPL for 1 year.)

3.25.7 Lost, stolen, or missing AA&E shall be reported immediately, but no later than 24 hours after discovery, to the AA, OPS.

3.25.8 This preliminary report shall include all available details concerning the event with a complete description of the weapon or other lost AA&E item(s).

3.25.9 This preliminary report shall not be delayed pending a complete report of the circumstances.

3.25.10 A description of the lost, stolen, or missing AA&E shall also be entered into the National Criminal Information Center database by local or federal law enforcement personnel.

3.25.11 Security Services contract personnel issued AA&E shall only be armed to perform their mission, if approved by the CCPS.

3.25.12 Non-security personnel having NASA mission related uses for AA&E items shall:

a. Ensure control, storage and accountability of authorized AA&E are in accordance with the provisions in paragraph 3.7.21 and the requirements established in NPR 8715.3, NASA General Safety Program Requirements, and NASA-STD-8719.12, Safety Standard for Explosives, Propellants, and Pyrotechnics.

b. Maintain appropriate and current inventories of issued and maintained AA&E pursuant to paragraph 3.7.17 and provide a copy of the inventories to the CCPS as changes occur.

3.26 Storage and Exchange of AA&E.

3.26.1 When not in use, all issued firearms and ammunition shall be securely stored per local policy.

3.26.2 Non-issued firearms and shoulder-fired weapons shall be stored in an arms room or a security container with a built-in 3-position combination lock and issued only as required.

3.26.3 Non-issued ammunition shall be stored in either a suitable lockable container or an arms room.

3.26.4 Explosives shall be stored in separate secure containers, specifically designed for the purpose of storing explosive materials.

3.26.5 Firearms or ammunition shall not be stored in containers with money, drugs, precious materials, evidence, or CNSI. They will be stored separately.

3.26.6 NASA Headquarters and Centers shall adopt procedures for the maintenance of records with respect to the issuance of AA&E and access to firearms and ammunition storage areas and containers.

3.26.7 Weapons shall not be exchanged on a Security Officer post. Any exchange or inspection of firearms will be done only in an area where a “clearing barrel” is available and/or under proper supervision.

3.27 Standards for Secure Conference Rooms

3.27.1 When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in Director National Intelligence (DNI) Intelligence Community Directive (ICD) Number 705.

3.27.2 The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with ICD 705.

3.27.3 Meetings shall be limited to collateral Secret or below. Meetings shall not be regularly scheduled or be re-occurring meetings.

3.27.4 Positive access control shall be implemented.

3.27.5 A Security Officer shall conduct a visual inspection and establish security procedures for the meeting.

3.27.6 Special Cases.

3.27.7 The preceding specifications do not apply to conference areas in which the level of security exceeds the collateral Secret level.

3.27.8 For these areas, guidance on additional requirements will be provided by the CCPS on a case-by-case basis.

3.27.9 The AA, OPS or CCPS shall be contacted for any interpretation of these specifications.

3.28 Design Basis Threat

3.28.1 The ISC's interim Design-Basis Threat (DBT) Report is a stand-alone threat analysis to be used in conjunction with the Agency physical security criteria. The DBT document establishes a profile of the type, composition, and capabilities of adversaries. It is designed to correlate with the countermeasures contained in the compendium of standards and to be easily updated as needed. The DBT is an estimate of the threat facing federal facilities across a range of undesirable events and is based on the best intelligence information, reports, assessments, and crime statistics available. DBT shall be used to plan protection for NASA Critical Infrastructure (NCI).

3.28.2 The CCPS shall use the DHS Design Basis Threat in developing a localized threat statement for their Center.

3.29 Physical Security Vulnerability Assessments.

3.29.1 Centers shall conduct physical security vulnerability assessments to define, identify, and analyze their security vulnerabilities consistent with NPR 1620.2 and NPR 1620.3.

3.29.2 CCPSs shall conduct a periodic RA for signature by the JPL Director. The RA will be forwarded to the AA, OPS. The RA may or may not be classified.

3.29.3 NASA shall employ a sound and comprehensive security program that includes security awareness training and the development and implementation of Center security plans to mitigate risks.

3.29.4 To ensure an Agency-wide standard for reacting to periods of increased security threats, the threat conditions established in section 3.17 below shall be employed as directed by NASA Headquarters or as determined by local events and authorized by the JPL Director.

3.30 Threat and Incident Reporting

3.30.1 General.

3.30.1.1 All Centers shall implement a threat and incident reporting system as required by NPD 1600.2, NASA Security Policy.

3.30.1.2 The system's purpose is to keep the Agency senior management officials advised on a timely basis of serious security-related incidents or threats that may affect the NASA mission.

3.30.1.3 After advising Center senior management officials, CCPS reports shall be forwarded expeditiously to the AA, OPS . Refer to APPENDIX F for a sample of the Serious Incident Report format.

3.30.2 The CCPS ensures that incidents are reported to the AA, OPS and followed up with a detailed situation report that describes the incident.

3.30.3 Any type of incident that might have Agency security implications shall be reported to the AA, OPS in a timely manner, including but not limited to the following:

a. All crimes or incidents at a Center requiring notification of NASA OIG, or, the FBI, Drug Enforcement Agency (DEA), Bureau of Alcohol Tobacco Firearms and Explosive (ATF), or local law enforcement.

b. Suspected Espionage (Reported through Center CI channels via the NASA Secure Network (NSN).

c. Suspected Sabotage (Reported through Center CI channels via the NSN).

d. Suspected terrorist activity (surveillance, photography, attempted penetrations, and unusual requests for information). (Reported through Center CI channels via the NSN).

e. Bombing incidents, including bomb threats that severely impact Center activities.

f. Actual or planned demonstrations or strikes.

g. All weapons discharges, including unintentional discharges, or other violent acts. Planned and pre-approved scientific or experimental discharges do not require reporting.

h. All incidents which involve the need for professional medical attention or damage to NASA facilities or equipment shall also be reported in accordance with NPR 8621.b, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

i. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on NASA property may also require reporting to and through the NASA Safety Program channels in accordance with NPR 8621.b).

j. A security-related incident that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities and/or in which the media has become involved and publicity is anticipated.

k. An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incidents shall include unauthorized access, theft, interruption of computer/network services or protective controls, damage, disaster, or discovery of a new vulnerability.

l. Threats against NASA property.

m. Physical threats to the infrastructure that support NASA missions.

n. Threats against NASA personnel.

o. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.

p. Information concerning individuals who are perceived to be acting irrationally in their efforts to make personal contact with high Government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American and anti-U.S. Government demonstrations in the United States, involving serious bodily injury or destruction of property; or an attempt or credible threat to commit such acts to further political, social, or economic goals through intimidating and coercive tactics.

3.31 The CCPS will maintain statistics for areas identified in Appendix I. This information will be sent to the AA, OPS in December of each year and/or as requested.

3.32 NASA Protective Services Office SA and Security Specialist Badges and Credentials (B&C)

3.32.1 *NASA Credentials will be issued only to those civil service security employees who are required to present proof of their authority in the performance of their official duties.*

3.32.1.1 Credentials are sequentially numbered and accountable security items. Their issue, use, and accountability shall be monitored by the AA, OPS and the CCPS.

3.32.2 Issuance, Use, and Return.

3.11.2.1 Credentials identify NASA SA and Security Specialist authorized, under NASA FAA, to carry firearms, to conduct investigations and inspections and to perform other duties that shall be assigned by virtue of the PL 111-314. NASA SA must maintain their qualifications within the NASA training programs.

3.32.2.2 The AA, OPS shall create, authenticate, and issue credentials and procure metallic badges at the request of the CCPS.

3.32.2.3 Security Specialists whose official duties do not require routine investigative work and/or frequent liaison with Federal, State, or local law enforcement authorities shall only be issued Security Specialist Credentials appropriate for the position occupied.

3.32.2.4 The CCPS shall ensure that SA Credentials or Security Specialist Credentials no longer required for official duties will be returned to the AA, OPS.

3.32.2.5 The CCPS shall ensure that Credentials are not misused and will withdraw them immediately upon any report of misuse, pending investigation of the allegation.

3.32.2.5.1 A report outlining the circumstances of any withdrawal of Credentials shall be forwarded to the AA, OPS within 72 hours.

3.32.2.5.2 A report on the final disposition of the incident, including the results of a Return To Duty assessment and recommendation, shall also be furnished to the AA, OPS for review and final determination.

3.32.2.6 Lost or stolen Credentials must be reported immediately. The appropriate CCPS shall forward a report outlining all pertinent facts to the AA, OPS no later than 2 days after the loss.

3.32.2.7 Security Specialists and SA must surrender credentials when requested by the issuing authority or when relieved of security duties by transfer, termination, or retirement. Upon termination of security duties, requests by retiring personnel to keep credentials shall be addressed as follows:

a. Employee must have been employed by NASA and leave the Agency with a satisfactory performance record.

b. Credentials shall be sent, along with a letter requesting retention of “voided” credential, for the individual concerned to the AA, OPS for approval.

c. Retirement and presentation of the NASA metal badge shall be considered based on the following prerequisites:

(1) Employee must be retiring from Federal service under honorable circumstances.

(2) Badges must be mounted in a Lucite award block, which shall be funded by the retiree.

(3) Individuals or organizations shall submit to the OPS a written request containing the individuals name, position, and length of service with NASA, along with a personal check in the amount required at that time, made out to the OPS selected vendor.

3.32.2.8 Credentials may be returned to the AA, OPS double wrapped by NASA pouch mail, or they may be hand-carried.

3.33 Technical Surveillance Countermeasures (TSCM)

3.33.1 TSCM Program.

3.33.1.1 The AA, OPS is responsible for the NASA TSCM program. The program shall be consistent with national policy issued by the U.S. Security Policy Board. All matters pertaining to the conduct of TSCM activities throughout the Agency will be directed and coordinated through the AA, OPS.

3.34 Protective Services Response to Demonstrations and Civil Disturbances

3.34.1 The primary objectives in dealing with demonstrations are to restrict demonstration activity to areas outside Centers and to preserve peace while protecting the rights of demonstrators to assemble peacefully and exercise free speech.

3.34.2 The CCPS for JPL shall make reasonable efforts to safely manage crowds who have assembled to demonstrate.

3.34.3 If demonstrators trespass onto NASA property, the CCPS will protect NASA personnel, property, and information in accordance with the law.

3.34.4 Ensure that the Statement of Work for the contract security force requires training in dealing with demonstrators as annual in-service training, and as refresher training immediately prior to a demonstration, when possible.

3.34.5 Ensure that NASA Special Agents, Security Specialists, and contract security officers/police receive training in dealing with demonstrators during in-service training and as refresher training prior to a demonstration, when possible.

3.34.5.1 The CCPS will maintain an event log, commencing at the time information is first received, of a demonstration and detailing thereafter all significant events, times, places, and actions with the name of the NASA official authorizing such actions.

3.35 Threat Conditions (THREATCONS) Program

3.35.1 General.

3.35.1.1 The protection of NASA employees and assets from acts of terrorism at NASA-owned or leased property in the United States or abroad shall be given priority, especially during periods of heightened threat.

3.35.1.2 Although absolute protection against such acts is not possible, protective procedures shall be based on the threat level and reflect a balance among the degrees of protection required, the resources available, Agency mission requirements, and other pertinent factors.

3.35.1.3 In addition to assistance from OPS , JPL shall obtain support from representatives such as the FBI, Department of State, NASA OIG, and state and municipal law enforcement agencies.

3.35.2 THREATCONS.

3.35.2.1 This section explains the establishment of the NASA THREATCON program designed to meet the requirements of the National Terrorism Advisory System (NTAS) developed and implemented by the DHS.

3.35.2.2 NASA Centers hosting military organizations as tenants, residing as a tenant on a military installation, or situated contiguous to a military installation, shall establish mutually agreed upon notification systems for ensuring DoD's use of ALPHA designators under the DoD Force Protection Condition concept are understood and integrated into JPL 's threat condition warning system. NASA utilizes the DHS National Terrorism Advisory System. .

3.35.2.3 The warning system ranges from NASA's basic, everyday security policy, Imminent Threat Alert and elevated Threat Alert.

3.35.2.4 The warning system is intended to standardize terms and establish standardized security measures that can be initiated by the AA, OPS and Center Directors through the Agency-wide emergency notification system.

3.35.2.5 Every Government agency is required to use this NTAS that provides for a greater consistency to threat reactions at both the national and Agency-level.

3.35.2.6 The AA, OPS shall initiate, and will change, or rescind NASA-wide THREATCONS.

3.35.2.7 Center Directors shall implement threat mitigation measures initiated by the AA, OPS and may implement additional measures for their Center based on the local threat situation. They will not lower or rescind a threat mitigation action initiated by the AA, OPS.

3.35.2.8 The AA, OPS shall monitor the threat status in the Agency and maintain close liaison with the DHS and National-level intelligence and security agencies for timely and accurate threat information.

3.35.2.9 The CCPS shall maintain close liaison with the local FBI offices and local law enforcement agencies for threat information.

3.35.2.10 NASA NTAS and associated actions are outlined in APPENDIX C, NASA NTAS Actions.

3.36 Hazardous Material Security

3.36.1 NASA programs use many different hazardous materials in meeting mission objectives. It is imperative that the use, storage, and protection of these materials be given the highest priority necessary to ensure the safety of NASA personnel and the general public.

3.36.2 In coordination with Center safety, logistics, environmental, and transportation officials, Center Protective Services Offices shall develop and implement security plans specifically designed to provide maximum protection in the transportation, receipt, access, use, storage, and accountability of hazardous materials used by NASA. Security Plans will include:

a. Review of shipping/transportation procedures to ensure appropriate precautions are in place. Recommend changes/adjustments.

b. Appropriate sharing of threat information associated with the targeting of hazardous materials.

c. Establishment of Center-specific receipt, escort, and hand-off procedures.

d. Establishment of security procedures for permanent and temporary storage/holding areas.

3.36 Investigations

3.36.1 The investigative component of Protective Services is directly related to the security and protection mission and may include such matters as threats of workplace violence, harassment, missing or stolen property, misuse of government property, and other violations of NASA and Center security policies.

3.36.2 The CCPS shall closely coordinate investigative activity with the appropriate external organizations (OIG, CIO, Office of Human Capital, Office of the Chief Counsel, FBI, ATF, DOD, local and state police) to ensure that cases are referred to the appropriate organization for follow-up when this is required.

3.36.3 Reports of Investigation shall be thoroughly documented. HQ, OPS will be notified of investigations of security incidents as prescribed in paragraph 3.10 of this NPR.

Chapter 4. Program Security

4.1 General

4.1.1 This chapter provides the requirements for establishing a system security approach in the development of a NASA program or in enhancing the protection level of an active program.

4.1.2 The objective is to identify security provisions as early as possible in system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

4.2 Responsibilities

4.2.1 The CCPS for JPL is responsible for the following:

4.2.1.1 Establishing a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.

4.2.1.2 Incorporating appropriate security measures, outlined in the various Chapters of this NPR, into project plans, facility plans, and requests for proposals.

4.2.2 Project and program managers at NASA Centers are responsible for ensuring provisions contained in NPR 7120.5D NASA Space Flight Program and Project Management Requirements are appropriately addressed with the CCPS.

4.2.3 The AA, OPS shall compile and maintain the NASA Critical Infrastructure (NCI) Inventory of NASA mission essential infrastructure assets. The list will consist of:

a. critical or key asset description (cyber, physical or both)

b. owning center/program

c. physical location

d. responsible enterprise

e. whether part of the Agency continuity of operations planning program

f. Develop contingency plans to ensure sufficient redundancies exist for key systems and infrastructure elements. Plans should be reviewed/vetted through all key stakeholder organizations.

4.2.4 Center program/project managers shall ensure that critical programs or assets are identified for inclusion on the consolidated inventory and that program planning includes security provisions and funding.

4.2.5 Project and program managers at NASA Centers are responsible for reporting incidents or perceived incidents involving loss of sensitive mission information to JPL Security Office.

4.3 NCI and Key Resources – NCIPP

4.3.1 HSPD-7 “Critical Infrastructure Identification, Prioritization, and Protection,” directs every Government agency to establish a program to identify critical essential infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as NCI to better facilitate designation of vital “mission oriented” critical infrastructure and key resources.

4.3.2 An effective critical asset protection program provides affordable, practical, and responsible protection, within acceptable risks, to those vital NASA resources that cannot reasonably be replaced or that have unique capabilities to support NASA goals.

4.3.3 Designated NCI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate security risk assessment.

4.3.4 NCI may include IT resources managed under the “Special Management Attention” designator; critical components; communication, command, and control capability; Government-owned flight or experimental flight vehicles, shuttles, International Space Station and apparatus; and one-of-a-kind irreplaceable facilities.

4.3.5 Supporting infrastructure called “interdependencies” shall not be designated as NCI.

4.3.5.1 “Interdependencies” includes those external and internal commercial elements that JPL NCI depends on to operate; electrical power, gas, communications hubs, local area networks, telephone systems.

4.3.5.2 “Interdependencies” must nevertheless be evaluated for their vulnerability and assessed for their impact if lost, especially if they are “single points of failure.” Vulnerability mitigation activity regarding NASA assets designated as “interdependencies” must also take the “single point of failure” aspect into account when developing their mitigation plans.

4.3.6 Policy and procedures shall be developed and implemented at JPL that accurately reflect Agency requirements for assessing NCI as outlined in this and other Agency-wide requirements. This ensures Agency-wide uniformity and consistency in the approach to performing the appropriate security risk assessments for each identified NCI.

4.3.7 Criteria and procedures NASA Centers shall use in identifying NCI are contained in Appendix H, Identifying and Nominating NASA Assets for the NCIPP.

4.3.8 Minimum security requirements for NCI facilities or facilities housing NCI assets are provided in this Chapter 3.5.4 of this NPR as well as NPR 1620.3.

4.4 OPSEC

4.4.1 NSDD 298 establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program.

4.4.2 Agencies with minimal activities affecting national security are not required to establish a formal OPSEC program; therefore, NASA does not require a formal Agency-level OPSEC program, although some Centers have programs that do require OPSEC application.
4.4.3 The NASA minimum security standard is to employ OPSEC measures on all classified programs.

4.4.4 If OPSEC planning is warranted, program and project managers, in coordination with JPL Physical Security Officer, shall develop and implement a project OPSEC plan that will identify critical information or activity, analyze threat(s) and vulnerability(ies), assess risk, and apply appropriate countermeasures.

4.5 Risk Management Process

4.5.1 NASA has adopted a Risk Management approach, using requirements established in NPR 8000.4A, Agency Risk Management Procedural Requirements and NPR 1620.3 in which the risk of loss must be weighed against the cost and operational impact of implementing established minimum-security standards.

4.5.2 Risk management provides a mechanism that allows security and program/project managers to recommend waivers to security standards based upon a threat and vulnerability assessment and the resulting risk determination.

4.5.3 Risk management is an integrated process of assessing the threat, vulnerabilities, and value of the resource and then applying appropriate safeguards and/or recommending the assumption of risk.

4.5.4 The CCPS shall ensure that security standards, established in this and other NPR, are met or that appropriate requests for waivers are submitted and approved by the AA, OPS.

4.5.4.1 JPL Director is designated as the Designated Official (DO) for JPL .

4.5.4.2 The DO shall make the final determination on requests for waivers to security standards when the CCPS has determined that the waiver will pose a serious risk on the program. The DO will accept security risk and forward a waiver as described in Waivers and Exceptions section 2.3 of this NPR to describe their decision to deviate from the NPR.

4.5.5 AA, OPS in coordination with the various stakeholders shall establish and implement an Enterprise Security Risk Management Program that enhances operational readiness and mission success by providing security support to program/projects throughout the life-cycle of a system or activity that is commensurate with the risk and helps ensure mission critical information, technologies, and/or assets are appropriately protected.

4.7 NASA Security Education and Training, and Awareness (SETA) Program

4.7.1 General.

4.7.1.1 The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them.

4.7.1.2 Management and employee involvement is essential to an effective security program.

4.7.1.3 An integral part of the overall NASA Security Program relies on the education and training of individuals regarding their security responsibilities.

4.7.2 Responsibilities.

4.7.2.1 As a minimum, the JPL Director shall ensure that adequate procedures are in place whereby all JPL employees and contractor personnel, regardless of clearance status, are briefed annually regarding Center security program responsibilities.

4.7.2.2 The CCPS for JPL shall ensure that appropriate and knowledgeable security personnel provide and receive the applicable types of briefings or training as described in paragraph 4.7.3 below and as required by the NISPOM.

4.7.2.3 NASA supervisors shall ensure job-related, facility-oriented security education, and awareness instruction or training for newly assigned personnel are timely and properly coordinated with the CCPS.

4.7.3 Required Briefings and Training.

4.7.3.1 Initial orientation briefings are given by security personnel (i.e., NASA and/or security services contractor) to acquaint new employees with local security procedures and employee responsibilities to protect personnel and Government property from theft, loss, or damage.

4.7.3.2 Security orientation briefings are given by the responsible supervisor or designee to each new employee and shall include all security requirements and procedures for which the employee is to be specifically responsible.

4.7.3.3 The CCPS shall ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance and prior to being granted access to classified information.

4.7.3.3.1 This briefing shall include:

a. Execution of Classified Information Nondisclosure Agreement (SF 312) and/or SCI NDA 4414, where appropriate) as required by the NISPOM.

b. General security aspects affecting employment and a summary of restrictions and obligations associated with access to classified information that are imposed by statute or executive order.

c. Employee reporting obligations.

d. Security procedures with regarding proper to handling of classified information and documents, classified meetings and discussions, and how to apply Need-to-Know.

e. Standards of behavior expected of persons in sensitive positions and the responsibility of security clearance holders to report behavior and adverse information that will disqualify an individual from security clearance eligibility.

4.7.3.3.2 The security person giving the briefing shall ensure that the employee is made aware of the most current executive order number if the briefing form has not been revised to reflect that change.

4.7.3.3.4 Annual briefings are required for all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Initial and annual briefings are also required for individuals granted accesses to certified National Security Systems that process classified information. Clearances may be suspended or revoked for failure to complete annual training.

4.7.3.4 Classified custodians and any other custodians responsible for CNSI safes, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

4.7.3.5 Security personnel shall give other special security training or briefings to employees related to SAP's, SCI, and NCI.

4.7.3.6 Security personnel shall conduct foreign travel briefings to JPL travelers to enhance their awareness of potential hostile intelligence, terrorist, and criminal threats in the countries to which they are traveling. These briefings must also provide defensive measures and other practical advice concerning safety measures.

4.7.3.7 Security personnel shall conduct security termination briefings to employees whose personnel security clearances are being terminated due to termination of employment, transfer to another Center, or other reasons. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their life-long responsibilities and penalties for unauthorized disclosure of CNSI even after termination of the clearance or employment.

4.7.4 The Program Protection Officers at JPL shall provide both security awareness and guidance to projects and programs regarding protection of unclassified sensitive mission information or technologies. The information provided to programs and projects will be based on industry best practices and real-life lessons learned with the Agency.

4.8 Self-Inspections

4.8.1 This section sets standards for establishing and maintaining an ongoing NASA/OPS Functional Review Program, which shall include the periodic review and assessment of the Information, Industrial, Personnel, Identity Management, Physical and Program Security at all NASA Centers and the JPL.

4.8.2 The objective is to ensure that JPL is implementing their security program in accordance with all applicable NASA and Federal regulations and to identify areas that need to be addressed that are not in compliance with appropriate rules and regulations. The review will also pinpoint commendable areas of each security operation and identify areas that need additional support to complete their mission.

4.8.3 Responsibilities.

4.8.3.1 The AA, OPS is responsible for the NASA/OPS's Functional Review Program. The AA, OPS shall designate agency personnel to assist in carrying out this responsibility. The means and methods for the conduct of functional reviews may include:

a. A review of relevant Protective Services directives, guides, training material and instructions.

b. Interview with Protective Services representatives and customers.

c. Review of Information, Industrial, Emergency Management, Identity Management, Personnel and Physical Security Programs.

d. Review of various files and documents pertaining to day-to-day operations.

4.8.3.2 A standard functional review guide/checklist will be used by the inspectors conducting the review. JPL will be inspected at least every 3 years. The format for documenting findings will be set by the AA, OPS. The AA, OPS, in its oversight capacity, may schedule reviews of Centers on an as needed basis.

4.8.4 Coverage of Functional Reviews

4.8.4.1 Each review may be adjusted to meet the coverage of the security programs in place at that particular center.

Chapter 5. Training, Certification and Authority of, Contract NASA Security Police Officers and Contract NASA Security Officers

5.1 General

5.1.1 42 U.S.C. 2456a authorizes the NASA Administrator to prescribe security regulations in support of these regulations and as approved by the Attorney General of the United States. The NASA Administrator also prescribes statutory FAA. Those regulations are set forth in 14 C.F.R. Part 1203b. This chapter identifies the requirements for granting FAA. NASA contract Security Police and Security Officers are required to be trained and certified to the standards described in this chapter.

5.2 Applicability

5.2.1 This chapter applies to all NASA Special Agents, Security Specialist and contractors assigned as NASA Security Police Officers and NASA Security Officers.

5.3 Responsibility

5.3.1 The AA, OPS is the designated Senior Agency Official for the NASA security and law enforcement training which includes NASA Federal Arrest Authority Training and NASA Security Officer Fundamentals Training. These responsibilities include:

5.3.1.1 Directing the FAA Program in accordance with applicable laws, NASA regulations, and directives.

5.3.1.2 Reviewing and approving nominations of all civil servants to be NASA SA and issuing credentials.

5.3.2 The Deputy AA/OPS is designated the NOPST Academy Program Manager. The Deputy AA/OPS is responsible for:

a. Informing the Senior Agency Official for FAA of any areas of interest in which FAA requirements are lacking and any other matters likely to impede NASA objectives in meeting FAA requirements.

b. Periodically reviewing the FAA Program and recommending to the Senior Official any changes necessary.

c. Recommending to the Senior Official adequate internal safeguards and management procedures.

d. Review and Approve all NOPS Academy training curriculum and courses.

e. Coordinate matters pertaining to FAA Program with the OGC and/or Department of Justice.

f. Approve NASA curriculum and certification procedures for Security Officer Fundamentals Certification (SOFC) training which is required for all NASA Security Specialist and contract Security Officers who are armed but do not require FAA.

5.3.3 Center Directors have the following responsibilities:

a. Through the CCPS and with the advice of NASA NMO Chief Counsel implement and maintain the NASA FAA program at their respective Center. Essential to implementing and maintaining a viable NASA FAA at JPL level is ensuring that adequate numbers of qualified contract security force personnel are identified, selected, and properly trained under NASA FAA requirements pursuant to Appendix D, NASA FAA and Use of Force Qualifications and Training. This will be accomplished by:

b. Reserved

c. Upon notification, immediately suspend from duty with pay or reassign to duties not requiring FAA, any person with FAA accused of violating FAA procedures or instructions. This suspension will remain in effect until completion of an internal investigation. Suspensions will be immediately reported to OPS.

d. Special Response Teams, K-9 Teams, other LE emergency response teams.
Centers that utilize specialized contractor security teams, such as; SRT, and K-9 shall utilize standardized selection criteria that will include a physical fitness test, an oral interview, a job specific physical test, a written test, and a review of employment files (to ensure the officer has completed probationary periods and to confirm that the officer is not under any disciplinary action.) JPL may develop their own specific details on what to include within these criteria but, as minimum, must include the requirements identified in Section 2.4.

5.3.4 The CCPS shall determine and establish operational procedures and arrangements for providing essential, timely, consistent and effective security and law enforcement response capability. The CCPS will implement the NASA FAA program after evaluating types of Center jurisdiction, availability and capability of federal, state and local law enforcement, and other factors that may impact Center security.

5.3.4.1 Prior to implementation of FAA, the CCPS shall coordinate with their Office of Chief Counsel for consultation with the U.S. Attorney regarding procedures for the appropriate and timely transfer of arrested persons.

5.3.5 In consultation with JPL NMO , the CCPS shall develop appropriate chain of custody procedures and establish the necessary relationships with local law enforcement and Federal law enforcement agencies to ensure issuance and execution of necessary arrest warrants.

APPENDIX A: Definitions

A.1 Access – the ability, opportunity, and authority, to gain knowledge of classified information or gain authorized entry onto a NASA classified IT resource.

A.2 Access Control System – Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

A.3 Accreditation – Formal declaration by a DAA that an information technology system is approved to operate in a particular security mode for the purpose of processing CNSI, using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

A.4 Adjudication – According to E.O. 13467 of July 2, 2008 Adjudication is the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: suitable for Government employment; eligible for logical and physical access; eligible for access to classified information; eligible to hold a sensitive position; or fit to perform work for or on behalf of the Government as a contractor employee.

A.5 Arrest Authority – the power to execute arrests, without a warrant, and to conduct searches incident to an arrest, granted to designated NASA Security Officials and Security Services Contractors, pursuant to Section 104(f) of the National Aeronautics and Space Act of 1958, as amended, and 14 CFR Part 1203b.

A.6 Asset – a system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

A.7 Center Chief of Protective Services (CCPS) – the senior Center security official responsible for technical management and day-to-day operations of the JPL security program.

A.8 Certification – a formal process used by the Certifying Official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

A.9 Certifying Authority (CA) – individual responsible for ensuring and certifying, to the DAA, that requisite security measures are implemented for IT Systems identified for processing of classified information.

A.10 Certifying Officials – the AA/OPS or the CCPS who are, by virtue of this NPR, are authorized to certify that an individual has met established requirements (training, firearms qualification), can perform those security functions designated in their position description, and can carry a firearm in performance of their security duties. They can also approve the use of a security room, vault, or container for storage of CNSI.

A.11 Classification Category – the specific degree of security classification that has been assigned to CNSI to indicate the extent of protection required in the national interest:

a. Confidential Information – the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

b. Secret Information – the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

c. Top Secret Information – the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

A.12 Classified information.- Information that has been determined pursuant to Executive Order 13526 of., or a successor or predecessor order, or the Atomic energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

A.13 Classified Material.-Any physical object on which is recorded, or in which is embodied, CNSI that shall be discerned by the study, analysis, observation, or other use of the object itself.

A.14 Classified National Security Information (CNSI) - Information that must be protected against unauthorized disclosure IAW Executive Order 13526, “Classified National Security Information,”. And is marked to indicate its classified status when in documentary form. See definition for “Classification Category” above.

A.15 Compromise - The improper or unauthorized disclosure of or access to classified information.

A.16 Contractor -Under E.O. 13467, July 2, 2008 Contractor is an expert or consultant (not appointed under section 3109 of title 5, United States Code) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of NASA (but not a federal employee).

A.17 Counterintelligence (CI) - Information gathered and activities conducted to protect against espionage and sabotage and other intelligence activities conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document, or communications security.

A.18 Critical Infrastructure -Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Public Law 107-56, U.S. Patriot Act Section 1016 (e))

A.19 Debarment - Official determination made in writing by the JPL Director or CCPS that bars, for cause, an individual from accessing NASA property.

A.20 Declassification - The authorized change in the status of information from classified information to unclassified information.

A.21 Denial -The adjudication that an individual's initial access to classified information would pose a risk to National security, after review procedures set forth in E.O. 12968 have been exercised.

A.22 Designated Approving Authority (DAA) - Official who formally assumes responsibility for operating an ITS or network at an acceptable level of risk.

A.23 Director, Security Management Division - Official assigned to OPS responsible for Agency management of physical security, personnel security, industrial security, and program security.

A.24 Escort -The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access JPL , where the individual may go, whom the individual is to meet, and authorized topics of discussion.
A.25 Exclusion Area - A space in which security measures are applied primarily to safeguard CNSI and material with entry to that space being equivalent to access to such classified information and material.

A.26 Executive Order (E.O.) - Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

A.27 Federal Arrest Authority (FAA) - The arrest authority granted under 14 CFR, Section 1203b.103 to NASA security personnel.

A.28 Infrastructure - A collection of assets. See definitions for asset and system.

A.29 Intelligence Community - The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; offices within the DoD for the collection of specialized national foreign intelligence through reconnaissance programs; the Bureau of Intelligence and Research of the Department of State; intelligence elements of the military services; the Federal Bureau of Investigation; the Department of Homeland Security; the Department of the Treasury; the Department of Energy; and staff elements of the Office of the Director of Central Intelligence.

A.30 Intrusion Detection System (IDS) -A security alarm which consists of one or more various types of components used to detect, assess, and notify of unauthorized access into a protected area.

A.31 Key Resources. Publicly or privately controlled resources essential to the minimal operations of the economy and government (Public Law 107-296, The Homeland Security Act, Section 2(9)). Key resources include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

A.32 Lautenberg Amendment. The Lautenberg Amendment to the Gun Control Act of 1968 became effective 30 September 1996. The Lautenberg Amendment makes it a felony for anyone convicted of a misdemeanor crime of "domestic violence" (assault or attempted assault on a family member) to ship, transport, possess, or receive firearms or ammunition. There is no exception for law enforcement or security personnel engaged in official duties. The Amendment also makes it a felony for anyone to sell or issue a firearm or ammunition to a person with such a conviction. This includes NASA personnel and contractors who furnish weapons or ammunition to persons knowing, or having reason to believe, they have qualifying convictions.

A.33 Limited Area. A space in which security measures are applied primarily for the safeguarding of classified information and material or unclassified property warranting special protection and in which the uncontrolled movement of visitors would permit access to such classified information and material or property. But within such space, access shall be prevented by appropriate visitor escort and other internal restrictions and controls.

A.34 NASA Critical Infrastructure (NCI). Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations. .

A.35 NASA Critical Infrastructure Protection Program (NCIPP). The planning and implementation, of an enhanced protection level for Agency key resources identified by an NASA organization to be so crucial to the success of NASA missions as to warrant protection over that which would be routinely provided to NASA assets.

A.36 NASA Employee. NASA Civil Service personnel.

A.37 NASA PHOTO-ID. Refers to the NASA photo-ID that has any number of imbedded and external technologies capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded “smart card” chip.

A.38 NASA Policy Directive (NPD). NPDs are policy statements that describe what is required by NASA management to achieve NASA’s vision, mission, and external mandates and who is responsible for carrying out those requirements.

A.39 NASA Procedural Requirements (NPR). NPRs provide Agency requirements to implement NASA policy as delineated in an associated NPD.

A.40 National Agency Check (NAC). The NAC is a search of the following four indices:

a. U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.

b. FBI Identification Division contains a fingerprint index and name file.

c. FBI Records Management Division contains files and records of all other investigations (background, criminal, loyalty, intelligence); and

d. Defense Clearance and Investigations Index contains investigations, including criminal investigations, conducted on civilian and military personnel in the DoD.

(Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)
A.40 National Agency Check with Inquiries(NACw/I).

A.41 National Security Positions. Positions that have the potential to cause damage to the national security. These positions require access to classified information and are designated by the level of potential damage to the national security:

a. Confidential. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to National security that the Original Classification Authority (OCA) is able to identify or describe.

b. Secret - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to National security that the OCA is able to identify or describe.

c. Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to National security that the OCA is able to identify or describe.

A.42 Nondisclosure Agreement. Standard Form 312 (SF 312) is a non-disclosure agreement required under E.O. 13526 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the Information Security Oversight Office of the National Archives and Records Administration and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. The SF 312 replaces the earlier forms SF 189 or the SF 189-A. Enforcement of SF-312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion or removal, in addition to the likely loss of the security clearance."

A.43 Non-NASA Employee. Any paid worker who is not a NASA Civil Service employee.

A.44 Open Storage. Storage of CNSI in a security container or vault that does not incorporate secondary level storage in security containers.

A.45 Original Classification Authority (OCA). An individual authorized in writing, either by the President or by agency heads or other senior Government officials designated by the President, to classify information in the first instance.

A.46 Controlled Area. A space in which security measures are applied to safeguard or control property or to protect operations and functions that are vital or essential to the accomplishment of the mission assigned to a Center or Component Facility.

A.47 Revocation. The removal of an individual's eligibility to access classified information based upon an adjudication that continued access to classified information poses a risk to national security and after review procedures set forth in E.O. 12968 have been exercised.
A.48 Risk Acceptance. An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate the risk.

A.49 Risk Acceptance Designated Authority (RADA). An individual designated in writing who makes the final determination on waivers to security standards and requirements when a security deficiency has been determined to pose a serious risk to a program.

A.50 Risk Assessment (RA). The process of identifying internal and external threats and security vulnerabilities, identifying the likelihood of an event arising from the combination of such threats and vulnerabilities. Further, the RA defines the critical security countermeasures necessary to continue an organization's operations, defines the controls in place or necessary to reduce risk, and evaluates the cost for such controls.

A.51 Risk Management. A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

A.52 Sensitive Compartmented Information (SCI). Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

A.53 Security Clearance. A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to National security.

A.54 Security Police Officer. A uniformed and armed NASA security officer who has completed all required NASA Federal Law Enforcement training and is authorized to perform certain law enforcement duties as prescribed by 42 U.S.C. SS 2456a and this NPR.

Security Officer

A.55 Security Specialist. A qualified and trained NASA civil servant assigned to perform certain security duties such as physical, personnel, and program security functions.

A.56 Security Survey. A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

A.57 Security Violation. An act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (including the loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; security area violations). (NOTE: Does not include incidents of criminal activity; such as theft, assault, DUI).

A.58 Special Access Program (SAP). Any program established and approved under E.O. 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

A.59 Special Agent. A qualified and credentialed NASA civil servant assigned to perform specialized security, arrest, investigative or enforcement duties authorized by law and this NPR.

A.60 Suitability. Refers to identifiable character traits and past conduct, which are sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of a Federal job. Suitability is distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities. See 5 CFR Part 731

A.61 Suspension. The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

A.62 Technical Surveillance. Covert installation or modification of equipment to monitor (visually or audibly) activities within target areas or to acquire information by specialized means.

A.63 Threat Assessment. A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets. Used in conjunction with a Vulnerability Assessment to prepare a Risk Assessment.

A.64 Unauthorized disclosure (E.O. 13526). A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access or may also be the result of inadvertent disclosure.

A.65 Unclassified Controlled Nuclear Information (UNCI). Sensitive unclassified Government information concerning nuclear material, weapons, and components, whose dissemination is controlled under Section 148, of the Atomic Energy Act.

A.66 Vulnerability Risk Assessment. A formal evaluation, conducted by security professionals, of a critical asset's (facility, person, equipment, aircraft, spacecraft) vulnerability to theft, sabotage, death, or destruction, resulting in a determination of level of vulnerability and subsequent development and implementation of security measures (physical and procedural) designed to negate or eliminate those vulnerabilities. Used in conjunction with a Threat Assessment to prepare a Risk Assessment.

A.67 Waiver. The approved continuance of a condition authorized by the AA, OPS that varies from a requirement and implements risk management on the designated vulnerability.

APPENDIX B: ACRONYMS

AA – Assistant Administrator
AA&E - Arms, Ammunition, and Explosives
AFL - Approved Firearms List
ATF Bureau of Alcohol Tobacco Firearms and Explosive
CA - Certifying Authority
CCPS - Center Chief of Protective Services
CI - Counterintelligence
CIAO - Critical Infrastructure Assurance Officer
CIO- Chief Information Officer
CIPP - Critical Infrastructure Protection Program
CNSI - Classified National Security Information
CO - Contracting Officer
DAA - Designated Approving Authority
DCID - Director, Central Intelligence, Directive
DEA - Drug Enforcement Agency
DHS - Department of Homeland Security
DNI – Director of National Intelligence
DoD - Department of Defense
DSS - Defense Security Service
E.O. - Executive Order
FAA - Federal Arrest Authority
FBI - Federal Bureau of Investigation
FGI - Foreign Government Information
FLETA - Federal Law Enforcement Training Academy
HSPD - Homeland Security Presidential Directive
IDS - Intrusion Detection System
NAC - National Agency Check
NACI – National Agency with Inquiries
NASA-STD - NASA Technical Standard
NCI - NASA Critical Infrastructure
NCIPP - NASA Critical Infrastructure Protection Program
NPSTA - NASA . Protective Services Training Academy
NISPOM - National Industrial Security Program Operating Manual
NPD - NASA Policy Directive
NPR - NASA Procedural Requirements
NSDD - National Security Decision Directive
NSN - NASA Secure Network
NSS – National Security System
NTAS-National Terrorism Advisory System
OCA - Original Classification Authority
OGC - Office of the General Counsel
OIG - Office of Inspector General
OPSEC - Operations Security
PDD - Presidential Decision Directive
PPO - Program Protection Office
RA - Risk Assessment

RAA - Risk Acceptance Authority
SA - Special Agent
SAP - Special Access Program
SAPF - Special Access Program Facility
SCI - Sensitive Compartmented Information
SCIF - Sensitive Compartmented Information Facility
SOFC - Security Officer Fundamentals Certification
SOFCC - Security Officer Fundamentals Certification Course
SPB - Security Policy Board
.
TSCM - Technical Surveillance Countermeasures

APPENDIX C: NASA NTAS Actions

The National Terrorism Advisory System, or NTAS, replaces the color-coded Homeland Security Advisory System (HSAS). This new system will more effectively communicate information about terrorist threats by providing timely, detailed information to the public, government agencies, first responders, airports and other transportation hubs, and the private sector.

The NTAS Alerts will be based on the nature of the threat: in some cases, alerts will be sent directly to law enforcement or affected areas of the private sector, while in others, alerts will be issued more broadly to the American people through both official and media channels.

NTAS Alerts contain a sunset provision indicating a specific date when the alert expires - there will not be a constant NTAS Alert or blanket warning that there is an overarching threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS Alert. All changes, including the announcement that cancels an NTAS Alert, will be distributed the same way as the original alert.

C.1 NTAS-No Alert Minimum Actions:

C.1.1 Definition: Low risk of terrorist activity against the United States or NASA facilities or personnel.

C.1.1.2 Threat condition (NO ALERT) employs every day, routine security measures determined by the CCPS and endorsed by the JPL Director as being appropriate for the optimum protection of NASA assets at that Center.

C.1.1.3 The program shall include antiterrorism measures such as ID checks for entry, enforcing NASA policy on the wearing and display of the NASA photo-ID badge, random vehicle inspections, consistent and current mandatory security training, exercising emergency response capability; to include response to increase in threat condition, periodic security assessments of individual Centers and facilities to ensure all reasonable measures are taken to mitigate vulnerabilities.

C.1.2 NTAS-Elevated Threat Alert Minimum Mitigation Considerations:

C.1.2.1 Definition: Warning of a credible. terrorist threat against the United States .

C.1.2.2 Advise continuously all employees of the condition, through training, briefings, and other mediums;

C.1.2.3 Increase general security awareness, through training, briefings, and other mediums;

C.1.2.4 Secure buildings, rooms, and storage areas not in regular use;

C.1.2.5 Increase security inspections of packages;

C.1.2.6 Check all deliveries at mailrooms and shipping and receiving departments;

C.1.2.7 Periodically test emergency communications capability with command locations;

C.1.2.8 Review and update emergency response plans;

C.1.2.9 Keep Center personnel updated.

C.1.3.3 Conduct random vehicle and package inspections;

C.1.3.4 Monitor visitors;

C.1.3.5 Curtail special events and visitors;

C.1.3.6 Increase surveillance of critical locations;

C.1.3.7 Coordinate with local law enforcement and emergency response agencies, as required;

C.1.3.8 Assess the threat characteristics for further refinement of established/planned protective measures;

C.1.3.9 Review and implement as necessary contingency, Continuity Of Operations, and emergency response plans.

C.1.4 Imminent Threat Alert Minimum mitigation considerations

C.1.4.1 Definition: Warning of a credible, specific, and impending...terrorist threat against the United States C.1.4.2 Continue all imminent threat measures;

C.1.4.3 Inspect all incoming packages at a centralized receiving point;

C.1.4.4 Admit only essential visitors under escort;

C.1.4.5 Establish random Center checkpoints;

C.1.4.6 Cancel special events;

C.1.4.7 Limit number of entry and exit points;

C.1.4.8 Perform a consent search on all entering vehicles and conduct random searches of exiting vehicles;

C.1.4.9 If necessary, cancel vacations for security personnel;

C.1.4.10 Establish additional 24-hour patrols as necessary;

C.1.4.11 Coordinate with local law enforcement agencies.

C.1.5.3 Close JPL to all visitors;

C.1.5.4 Limit entry and exit to a single point;

C.1.5.5 Augment security forces as necessary to ensure adequate response capability;

C.1.5.6 Minimize all administrative journeys and visits;

C.1.5.7 Frequently check the exterior of buildings and parking areas for suspicious items and activity.

APPENDIX D: NASA Federal Arrest Authority and Use of Force Qualifications and Training

D.1 General

D.1.1 42 U.S.C. 2456a, Section 304(f) of the Public Law 111-314 , and 14 CFR Part 1203b--Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel authorizes the Administrator to implement an Agency FAA and Use of Force to ensure appropriate protection for NASA employees and contractors, facilities, information, and missions.

D.1.1.2 The Agency FAA shall be managed in strict compliance with the requirements established by the Attorney General of the United States and the direction provided in the following paragraphs.

D.1.1.3 Failure to maintain qualification, training and certification requirements established under this NPR shall result in denial of Center authorization to arm personnel.

D.1.2 FAA Program

D.1.2.1 Qualifications. FAA shall not be performed unless the JPL Director has the following assurances:

a. All FAA candidates must meet the physical fitness standards prescribed by the NASA Office of Protective Services Training (NOPST) course curriculum in order to graduate.

b. NASA civil service supervisors shall insure that all civil service employees and security contractor personnel nominated for FAA are physically and emotionally stable.

c. FAA authorization shall be withheld or suspended pending an assessment of a FAA candidate’s physical and mental health by a qualified physician.

d. That the candidate is currently a certified graduate in accordance with the training described in, but not limited to this Appendix.

D.1.2.2 Attendance at the full FAA basic training course may be waived for civil service candidates only, under the following circumstances:

a. The candidate is a retired or former law enforcement officer who has met all imposed hiring criteria and who has graduated from an appropriate Federal Law Enforcement Training Program (including FLETC, FBI Academy, Military, or other similar programs). Under these circumstances, a waiver detailing the candidates training history will be submitted to the AA, OPS for approval. Upon approval the candidate must only attend the FAA refresher course, and;

b. The candidate must complete required in-service Use of Force training, intermediate to lethal force; semiannual qualification with assigned firearm (Appendix E); judgmental shooting and NASA regulations and Center implementing instructions and training concerning FAA, or;

c. The candidate is not identified as requiring FAA and therefore, must attend and graduate from the NASA Security Officer Fundamentals Certification Course (SOFCC).

D.1.2.3 Selection and Attendance at NASA FAA Training.

D.1.2.3.1 Attendance at FAA training is required for all Civil Service personnel (CS) tasked with operational control of those performing duties related to:

a. Investigations.

b. Frequent duty related interactions with outside law enforcement.

c. VIP and special event protection details.

d. Emergency Response Team (ERT), K-9 and other LE emergency response members.

D.1.2.3.2 Attendance at FAA training for security services contractor personnel shall be determined by the CCPS. At a minimum, those performing the following duties will attend FAA:

a. Shift Supervisors (normally Capt., Lt., Sgt.).

b. Those conducting investigations.

c. Uniformed personnel performing duties with responsibility for responding to and managing incidents with the potential for involving a lawful arrest (i.e., traffic enforcement, property crimes, crimes against persons, disturbances).

(Note: Duties with the potential for the lawful detention of a person pending release to proper law enforcement authorities does not meet criteria for attendance at FAA training.)

D.1.2.3.4 Contractor personnel performing duties solely as security specialists within the personnel, information, SAP/SCI, IT, and physical security areas, and whose responsibilities center around managing and performing traditional security program duties such as classified material management, facility security inspections, or conducting interviews and research for the purpose of adjudicating access or suitability, shall not be armed. CS performing these functions will be armed only after AA/ OPS approval.

D.1.2.3.5 Contractor personnel standing static security posts are not required to attend FAA training. These personnel must complete the SOFC course.

D.1.2.4 To ensure consistency Agency-wide, the SOFC course shall be developed by the Federal Law Enforcement Agency, and taught by FAA certified trainers. The SOFC will include adequate training on:

a. Use of Force and Intermediate Use of Force.

b. Lawful Detaining of Persons.

c. Unarmed Defensive Tactics.

D.1.2.5 Mandatory Pass/Fail Testing Program.

D.1.2.5.1 To ensure only qualified individuals are authorized to carry firearms, the following standards shall apply for the SOFCC:

a. Must pass all portions of the designated program with minimum 80 percent passing grade.

b. In case of a failure, candidates shall be provided the opportunity to retake the section failed only one time after initial testing. A repeat failure after retaking the course of instruction will result in the nominee being dropped from SOFCC. CCPSs are NOT authorized to reduce any training standards established under this NPR.

c. An individual failing to demonstrate proficiency during a practical evaluation will be dropped from the SOFCC.

D.1.2.5.2 To ensure only qualified individuals are afforded the privilege of assuming FAA status, the following standards shall apply:

a. Must pass all portions of the designated program with minimum 80 percent passing grade.

b. In case of a failure, candidates shall be provided the opportunity to retake the section failed only one time after initial testing. A repeat failure after retaking the course of instruction will result in the nominee being dropped from the FAA program. CCPSs are NOT authorized to reduce any training standards.

c. An individual failing to demonstrate proficiency during a practical evaluation will be dropped from the FAA course.

D.1.2.6 Individuals authorized FAA shall carry the appropriate Miranda Advisement of Rights cards.

D.1.3 Use of Force

D.1.3.1 Under NASA FAA rules and procedures, Security Force personnel performing security duties may find themselves in a situation where they are required to take a person into custody or defend themselves or someone else.

D.1.3.2 CCPS shall ensure, at least semiannually, that NASA Use of Force training is conducted concurrent with required weapons qualification. Established training must include complete and current Use of Force theory and currently recognized practices to ensure an appropriate level of understanding and practical application is present among security force personnel.

D.1.3.2.1 The application of force during an officer/subject encounter should be based primarily on the perceived action(s) of the suspect within the totality of the circumstances. An officer’s response to a subject’s perceived actions must be guided by objective reasonableness when effecting lawful control.

D.1.3.2.2 If at any time a subject becomes injured, request medical personnel to respond to the scene.

D.1.3.3 If it becomes necessary to use a firearm as authorized in 14 CFR § 1203b.107, NASA CCPS shall comply with the following procedures:

a. The incident shall be reported to the CCPS, who in turn, will report it to the appropriate supporting law enforcement agency and then to the AA/ OPS as expeditiously as possible with as many details supplied as are available.

b. The officer shall be promptly suspended from duty with pay or reassigned to other duties not involving the use of a firearm, as the JPL Director or as the AA/ OPS deems appropriate, pending investigation of the incident.

c. The respective Center Director or AA/OPS shall appoint an investigating officer to conduct a thorough investigation of the incident. Additional personnel will also be appointed as needed to assist the investigating officer. Upon conclusion of the investigation, the investigating officer will submit a written report of findings and recommendations to the appropriate Center Director or AA/ OPS.

d. Upon conclusion of the investigation, the JPL Director and/or the AA/OPS, with the advice of the OGC or Office of Chief Counsel, shall determine the appropriate disposition of the case. If the investigation determines that the officer committed a crime, the information will be promptly reported to the supporting law enforcement agency.

D.1.3.4 Prohibitions.

D.1.3.4.1 Unreasonable use of force is considered misconduct. Such misconduct may result in administrative, civil, and/or criminal action.

D.1.3.4.2 Verbal abuse, verbal threats of violence, nonphysical threats, cannot alone be the justifiable basis for the use of force.

D.1.3.5 Security Equipment

D.1.3.5.1 Security and law enforcement equipment with use of force applications must be authorized by the JPL Director with the concurrence of the OGC and AA, OPS.

D.1.4 Training Curriculum

D.1.4.1 The NASA Office of Protective Services Training Program curriculum is developed and managed by the OPS NASA NOPST Advisory Committee. The curriculum is approved by the AA, OPS. Training shall consist of the following topics:

a. Legal Studies

b. General Law Enforcement Studies and Exercises

c. Weapons Familiarization and Defensive Tactics

D.1.4.2 All applicants must be qualified, as a minimum, with the designated handgun prior to attendance of any NOPST program (FAA and SOFCC).

D.1.4.3 Additional standards are required to qualify for ERT and K9.

Selection criteria:

1. Physical Fitness Test
2. Task Specific Physical Fitness Test
3. Weapons Qualification
4. Written Test
5. Oral Interview

All Task Specific Physical Fitness Test (Pass or Fail) must be approved by the NOPST Advisory Board. Each demonstration must be completed consecutively with a designated time to be determined based on the course developed and meet the objectives as designated;

1. Demonstrate overall physical fitness (run, push-ups, pull-ups, sit-ups)
2. Demonstrate defensive tactics
3. Demonstrate the ability to maneuver on the ground.
4. Demonstrate the ability to run stairs.
5. Demonstrate the ability to maneuver with designated equipment (vest, gas mask, helmet)
6. Demonstrate the ability to operate in confine space
7. Demonstrate the ability to reason under physical stress
8. Demonstrate the ability to manipulate handgun with gas mask still on and under physical stress. Conduct function check with handgun in a safe direction down range (ERT only).
9. Complete an Obstacle / Agility Course including a K-9 Handler task specific test (K9 only)

Upon selection, all ERT candidates must attend and pass a NOPST Advisory Board approved tactical officer certification course for ERT.

Upon Selection, all K-9 candidates must pass a NOPST Advisory Board approved canine training program.

Re-occurring training and certification requirements will be established by the NOPST Advisory Board.

D.1.4.4 Additional standards are required to qualify for K9

D.1.5 FAA and Use of Force Refresher/Certification Training

D.1.5.1 Personnel trained and certified under the NASA FAA and Use of Force Training Program will attend and complete 40-hour refresher training every training cycle.

D.1.5.2 Training cycles start every odd calendar year, January 1st and ends on the even numbered years, December 31st.

D.1.5.3 All applicants requesting certification or recertification must meet the standards outlined by NASA FLETA.

D.1.6 SOFC and Use of Force Refresher/Certification Training

D.1.6.1 Personnel trained and certified under the NASA SOFC and Use of Force Training Program will attend and complete 24-hour refresher training every training cycle.

D.1.6.2 Training cycles start every odd calendar year, January 1st and ends on the even numbered years, December 31st.

D.1.6.3 All applicants requesting certification or recertification must meet the standards outlined by NASA OPSTA.

APPENDIX E: NASA Firearms Qualification Courses

NASA Handgun Qualification and Course Of Fire Standards

Stage	Distance	Start	Shooter Response	Time Limit	X	Rounds Fired	Course Total
1	1-3 yards	Holster	From the hip, Fire 2 rounds	4 sec	2	4	4
2	3 yards	LR	Fire 2 rounds	1 sec	3	6	10
3	7 yards	Holster	Fire 2 rounds	4 sec	3	6	16
		LR	Fire 2 rounds	4 sec	3	6	22
4	7 yards	Holster	Fire 3 rounds	5 sec	2	6	28
5	7 yards	Holster	Fire 12 rounds with a mandatory reload	45 sec	1	12	40
6	15 yards	Holster	Fire 10 rounds	30 sec	1	10	50

This sequence should be fired twice, once for practice and then for record.

If their Range is sufficiently equipped Centers may use this alternate course of fire which requires the shooter to move between shots. Passing grade is 80% for uniformed personnel and NASA Agents and 90% for specialized teams.

Stage	Distance	Start	Shooter Response	Time Limit	X	Rounds Fired	Course Total
1	2 yards	Holster	Speed Rock', fire 2 rounds, move diagonally back 1 step	2 sec	3	6	6
2	3 yards	Holster	"Scoot and Shoot" Options, Fire 2 rounds, move 1 step	3 sec	4	8	14
3	5 yards	LR	Shooting hand only, fire 2 rounds, move 1 step	3 sec	2	4	18
			Support hand only, fire 2 rounds, move 1 step		2	4	22
4	5 yards	Holster	"Failure Drill", fire 2 rounds CM, 1 round Head, move 1 step	3 sec	2	6	28
5	7 yards	Holster	Fire 2 rounds- reload- fire 2 rounds, move 1 step	10 sec	1	4	32
6	10 yards	Holster	Fire 2 rounds- tactical reload- fire 2 rounds, move 1 step	15 sec	3	12	44
7	15 yards	Holster	Fire 1 round- reload- fire 2 rounds, move 1 step	12 sec	2	6	50

NASA Shotgun Qualification and Course of Fire Standards

Order and Position	Rounds	Time	Distance	Target
Phase I: Practice (See notes)				
1.Standing, strong hand	2	see note 1	15 yds.	IPSIC
2. Standing, weak hand	2	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	2	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	2	see note 1	7 yds.	IPSIC
8 Total Rounds				
Phase II: Evaluation (See notes)				
1. Standing, strong hand	3	see note 1	15 yds.	IPSIC
2. Standing, weak hand	3	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	3	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	3	see note 1	7 yds.	IPSIC
12 Total Rounds 20 Total Rounds (for course)				
Phase III: Qualification				
1. Each pellet striking the target counts as 1 hit. 2. Minimum passing score is 86 hits (80 percent), 97 hits (90 percent) for Emergency Response Team (ERT) personnel.				

Note 1: Time limit for practice is 45 seconds and evaluation is 60 seconds.

Note 2: Shooter will start in with six rounds in the weapon. On the fire command, they start the course firing three rounds from the strong side standing, and three rounds form the weak side standing. Keeping the weapon pointed down range, reload as you move to the ten-yard line and fire three shots strong hand kneeling. Move to the seven-yard line, reload the remaining three rounds from behind cover, and fire from the kneeling position, weak side barricade.

Note 3: Practice course is fired with two rounds from each position.

Order and Position	Rounds	Time	Distance	Target
Phase I: Practice (See notes)				
1.Standing, strong hand	2	see note 1	15 yds.	IPSIC
2. Standing, weak hand	2	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	2	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	2	see note 1	7 yds.	IPSIC
8 Total Rounds				
Phase II: Evaluation (See notes)				
1. Standing, strong hand	3	see note 1	15 yds.	IPSIC
2. Standing, weak hand	3	see note 1	15 yds.	IPSIC
3. Kneeling, strong hand	3	see note 1	10 yds.	IPSIC
4. Kneeling, weak hand barricade	3	see note 1	7 yds.	IPSIC
12 Total Rounds 20 Total Rounds (for course)				
Phase III: Qualification				
1. Each pellet striking the target counts as 1 hit. 2. Minimum passing score is 86 hits (80 percent), 97 hits (90 percent) for Emergency Response Team (ERT) personnel.				

NASA Rifle Qualification and Course of Fire Standards

Order	Position	Rounds	Time	Distance	Target
Phase I: Zero					
1.	Shooter's choice	3	N/A	100 yds.	IPSIC
2.	Shooter's choice	3	N/A	100 yds.	IPSIC
3.	Shooter's choice	4	N/A	100 yds.	IPSIC
10 Total Rounds					
Phase II: Practice					
1.	Prone Supported	10	30 sec.	100 yds.	IPSIC
2.	Prone Unsupported	10	30 sec.	100 yds.	IPSIC
3.	Kneeling /Sitting	10	30 sec.	100 yds.	IPSIC
4.	Kneeling/Sitting	10	30 sec.	50 yds.	IPSIC
5.	Standing	10	30 sec.	25 yds.	IPSIC
50 Total Rounds					

Phase III: Evaluation					
1.	Prone Supported	10	30 sec.	100 yds.	IPSIC
2.	Prone Unsupported	10	30 sec.	100 yds.	IPSIC
3.	Kneeling /Sitting	10	30 sec.	100 yds.	IPSIC
4.	Kneeling/Sitting	10	30 sec.	50 yds.	IPSIC
5.	Standing	10	30 sec.	25 yds.	IPSIC
50 Total Rounds 110 Total Rounds for course					
Phase IV: Qualification					
All hits on the IPSC target count. The Shooter must have 40 hits out of 50 for successful qualification. Emergency Response Team (ERT) officers must have 45 hits out of 50.					

NASA Submachine Gun Qualification and Course of Fire Standards

Order	Position	Rounds	Time	Distance	Target
Phase I: Practice					
1. (See note 1)	High Barricade	10 (5, 2 shot strings)	4 sec.	25 yds.	IPSIC
2. (See note 2)	Standing	16 (15, reload fire 1)	25 sec.	15 yds.	IPSIC
3. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	7 yds.	IPSIC
4. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	3 yds.	IPSIC
50 Total Rounds					
Phase II: Evaluation					
1. (See note 1)	High Barricade	10 (5, 2 shot strings)	4 sec.	25 yds.	IPSIC
2. (See note 2)	Standing	16 (15, reload fire 1)	25 sec.	15 yds.	IPSIC
3. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	7 yds.	IPSIC
4. (See note 3)	Standing	12 (6, 2 shot bursts)	3 sec.	3 yds.	IPSIC
50 Total Rounds 100 Total Rounds for course					
Phase III: Qualification 1. Each round striking the target counts as 1 hit. 2. Minimum passing score is 40 hits (80 percent), 45 hits (90 percent) for Emergency Response Team (ERT) personnel.					

Notes

Note 1: Semiautomatic, shooter will start in the strong barricade position, (may use barricade for support) and ensure finger is off the trigger.
Note 2: Semiautomatic, shooter will start in position, finger off the trigger.
Note 3: Automatic, shooter will start in position, finger off the trigger.

APPENDIX F: NASA Serious Incident Report Format

{Date}

TO: Assistant Administrator Office of Protective Services

FROM: Center Chief of Protective Services

SUBJECT: NASA Serious Incident Report

1. DATE/TIME OF INCIDENT:

2. CENTER:

a. Summary of Incident:
b. Responses to Incident:

(1) Actions Completed:
(2) Actions in Progress:
(3) Actions Pending:

3. EMPLOYMENT OF RESOURCES:

a. Center Protective Services Office:
b. Center Safety Office:
c. Local, State, and Federal Law Enforcement:

4. ACTIONS FOR ASSISTANT ADMINISTRATOR FOR PROTECTIVE SERVICES:

5. COMMENTS/RECOMMENDATIONS:

.

APPENDIX G: Security Signs Area

CONTROLLED A R E A

BY THE ORDER OF
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Unauthorized persons who enter shall be subject to prosecution under 18 U.S.C. 799.

G.1 Procedures for Ordering Signs:

a. Outdoor signs are metal, measuring approximately 40.64 cm/16 inches high and 50.8 cm/20 inches wide.

b. Indoor signs are of cardboard or foamboard, measuring approximately 22.86 cm/9 inches high and 12 inches wide.

G.2 Centers must order signs as needed through their normal supply source for NASA Forms:

a. Controlled Area Sign (Outdoors), NASA Form 1506

b. Controlled Area Sign (Indoors), NASA Form 1506A

c. Limited Area Sign (Outdoors), NASA Form 1507

d. Limited Area Sign (Indoors), NASA Form 1507A

e. Exclusion Area Sign (Outdoors), NASA Form 1508

f. Exclusion Area Sign (Indoors), NASA Form 1508A

APPENDIX H. Identifying and Nominating NASA Assets NCIPP

H.1 Introduction. HSPD 7, “Critical Infrastructure Identification, Prioritization, and Protection,” directs that every Government agency establish a program to identify their critical infrastructure or key resources, prioritize and evaluate their critical infrastructure or key resources for vulnerabilities, and fund appropriate security enhancements necessary to mitigate identified vulnerabilities.

H.2 Purpose. To establish the roles and responsibilities of key Agency and Center personnel in the implementation and support of HSPD 7 and the Agency CIPP.

H.3 CIPP. The Agency CIPP implements the Agency critical infrastructure and key resources protection strategy. The CIPP shall be consulted whenever action impacting an NCI asset is being considered.

H.3.1 Criteria for Determining NCI. Agency NCI is defined as those essential facilities, missions, services, equipment, and interdependencies that enable the Agency to fulfill its national goals and Agency essential missions. For the purposes of the NCI Protection Program, asset owners will use the following definitions when considering assets for inclusion:

a. A NASA infrastructure is to be considered critical, or a resource considered key, if its destruction or damage cause significant impact on the security of the nation - national economic security, national public health, safety, psychology, or any combination.

b. A NASA infrastructure or resource is to be considered mission critical if its damage or destruction would have a debilitating impact on the ability of NASA to perform its essential functions and activities.

c. Using paragraphs a & b above as guidance, NASA will use the following criteria to determine Agency critical infrastructure or key resource:

(1) Impact to National Security. Does the loss or compromise of the asset enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy critical missions in support of the National defense? Examples:

(a) Intelligence Functions

(b) Emergency Management Network

(c) Protection and Storage

(d) Nuclear Reactors Programs

(e) Defense and Transportation Programs

(2) Impact on Public Safety, Health, or Continuity of Government Services.

(a) Does the loss or compromise or the asset endanger or otherwise threaten the safety and health of the general public? Refers to:

1. NASA facilities and systems that protect the general public from hazardous materials.

2. Situations that could be generated using materials owned by NASA to create safety and health hazards.

3. Utilities, communications, or other similar systems on which other Agencies depend to accomplish their essential missions serving the general public.

4. Weather prediction or other systems on which other Agencies depend to accomplish their essential missions serving the general public.

(2) Impact on Economic Security. Does the loss or compromise of the asset enable the hostile entity to disrupt or otherwise threaten NASA's ability to satisfy its critical mission in support of the economic well being of the Nation? Refers to:

a. Assets operated or controlled by NASA, its contractors, or its agents that, if compromised or destroyed, would cause irreparable harm to the economic stability of the Nation.

(3) Impact on Essential NASA Missions that:

(a) Have very high public visibility in terms of the general public's perception of NASA as a symbol of national pride.

(b) Are integral to the performance of NASA's mission, have a very large dollar value, or are difficult or impossible to replace in a reasonable period of time.

(c) The loss or compromise of the asset would enable a hostile entity to disrupt or otherwise threaten the ability of NASA to satisfy its Essential Missions. Refers to:

1. Critical elements of the NASA Strategic Enterprises that are absolutely required for NASA's Mission capability.

2. Critical Infrastructure Interdependencies (IT resources, data, electric power, water, oil and gas, environmental control networks) that are dependent on or support NCI and whose loss could directly impact NASA's essential mission capability. These assets need not be identified as separate NCI but shall be integrated into JPL NCI asset protection scheme, evaluated for security risk assessments and protected accordingly.

(4) Impact on Human Life. Does the loss or compromise of the asset (telecommunications, telephone system, local area networks, wide-area components, transportation, security and safety, buildings or facilities) endanger or otherwise threaten the life, health, or safety of personnel engaged in the performance of NASA's missions?

H.4 Appointment of Agency and Center CIAO. Per the CIPP, the NASA Administrator and Center Directors shall appoint, in writing, a senior member of their staff to perform the duties as the CIAO.

H.4.1 The AA/OPS has been designated by the NASA Administrator as the NASA CIAO. The NASA CIAO, in coordination with Center CIAO's, shall coordinate and oversee all aspects of the Agency NCIPP.

H.4.2 The Agency CIO and Center CIO's, respectively, are responsible for coordinating and overseeing all aspects of the protection of Agency and individual Center cyber-infrastructure assets and interdependencies and will coordinate all critical and/or key cyber-infrastructure identification, prioritization, and protection requirements with the NASA CIAO. Together, the NASA CIAO and CIO set the tone for the success of the Agency NCIPP.

H.5 Procedures for Nominating NASA Assets for Consideration for Inclusion Under the NCIPP.

H.6 Procedures for identifying, nominating, and assessing initial Agency and Center NCI were established and implemented in 1999 to enable the Agency to meet National level mandates. Those procedures were implemented, and the Agency successfully identified and assessed all existing NCI and met all initial milestones.

H.7 Procedures for Adding/Deleting NASA Assets to the NCI Inventory. At a minimum, all proposed changes to the NCI list shall be coordinated by JPL with the responsible Headquarters Mission Directorate Associate Administrator, JPL 's CIO, CCPS, and CIAO.

H.8 Using the criteria outlined in paragraph 4 above, personnel responsible for JPL and/or Agency asset deemed a candidate for inclusion or deletion under the NCIPP shall follow the below procedure to determine the appropriateness of the NCI designation or deletion.

H.8.1 For IT Assets:

a. System owner, in coordination with JPL CIO, Chief of Security, IT System Security Manager, and JPL CIAO, shall propose IT System inclusion/deletion on the Agency NCI inventory to the JPL Director.

b. Upon final determination that the asset must be designated or deleted as a NCI, a written proposal shall be prepared for the JPL Director's approval.

c. Upon JPL Director's approval, JPL CIO shall forward the fully justified proposal to the NASA Deputy CIO for ITS.

d. The NASA Deputy CIO for ITS, in consultation with JPL ITS Manager, shall recommend acceptance or rejection of the proposal to the NASA CIO.

e. Based on the recommendation of the NASA Deputy CIO for ITS, the NASA CIO shall coordinate with the NASA CIAO and either approve or reject the proposed change.

f. Upon approval, JPL IT Security Manager and System Owner shall conduct an appropriate IT NCI system assessment using requirements established in NPR 2810.1.

g. Appropriate mitigation plans shall be prepared and implemented to address all vulnerabilities, or if the proposal is disapproved, the NASA CIO will coordinate with the

affected Center CIO and Mission Directorate Associate Administrator to establish the appropriate appeals process, if warranted.

h. Upon approval to delete an IT asset from the NCI list, the NASA CIO shall notify the requesting JPL Director, Center CIO, and Center CIAO of the decision and submit appropriate information to the NASA CIAO so they will update/distribute the NCI list, accordingly.

H.8.2 For physical assets:

a. Facility owner, in coordination with the CCPS and JPL CIAO, shall propose facility inclusion or deletion on the Agency NCI inventory to the JPL Director.

b. Upon final determination that the asset must be designated or deleted as a NCI, a written proposal shall be prepared for the JPL Director's approval.

c. Upon Center Director's approval, the CCPS shall forward the fully justified proposal to the NASA CIAO, with copies to the manager of the Mission Directorate Associate Administrator.

d. The NASA CIAO, in consultation with the CCPS and Mission Directorate Associate Administrator, shall recommend acceptance or rejection of the proposal to the NASA CIAO.

e. The NASA CIAO shall either approve or reject the proposed change.

f. If the proposal is approved, the NASA CIAO shall modify and distribute the updated NCI list, and notify the requesting Center Director, CCPS, AA, OPS and Center CIAO of the decision.

g. Upon approval of request for designation as an NCI, the CCPS and Center CIAO, shall ensure the following is accomplished.

(1) Conduct of an appropriate physical security assessment.

(2) Prepare and implement appropriate mitigation plans to address all vulnerabilities.

h. If the proposal is disapproved, the CIAO shall coordinate with the affected Center CIAO and Mission Directorate Associate Administrator to establish the appropriate appeals process, if warranted.

H.9 Upon approval to delete a physical asset from the NCI list, the NASA CIAO shall notify the requesting Center Director, CCPS, Agency CIO, AA, OPS and Center CIAO of the decision and update and distribute the NCI list, accordingly.

APPENDIX I: NASA Security Statistics Format

Center Law Enforcement and Security Statistics - Qtr #/CY##

1. Crimes Against Persons (Civil Servants, Contractors, Other -- *include date, time, description, and applicable report numbers (internal – NASA/external – law enforcement,*))

a. Murder
b. Rape
c. Attempted Murder
d. Assault
e. Armed Robbery

2. Recovered Stolen Property (Government, Contractor-owned, Personal – *include date, time, description, dollar-value of loss, and applicable report numbers (internal – NASA/external – law enforcement*)

a. Theft
b. Burglary
c. Vandalism

3. Property Damage (Government, Contractor-owned, Personal – *include date, time, description, dollar-value of loss, and applicable report numbers (internal – NASA/external – law enforcement))*

a. Damage Caused by Fire
b. Damage Caused by Weather

4. Traffic Management Program

a. Driving Under the Influence/Driving While Intoxicated
b. Moving Violation Tickets Issued
c. Parking Tickets Issued
d. Motor Vehicle Accidents/Mishaps
e. Pedestrian/Vehicle Accidents

5. Security Incidents:

a. Visitor Escort Policy and Procedure Violations
b. Compromise of CNSI
c. Unauthorized Access to Security Area
d. Suspension of Security Clearance
e. Denial/Revocation of Security Clearance
f. Debarment Actions
g. Denial/Revocation of Suitability (HSPD-12)
h. Unauthorized Entry/Entry Attempts
i. Weapons Violations
j. Bomb Threats
k. Illegal Drugs – Found, Public Intoxication

SECURITY PROGRAM

1. Visitor Escort Policy and Procedure Violations:

2. Number of Classified Contracts (Form DD Form 254):

3. Security Incidents:

a. Compromise of CNSI:
b. Unauthorized Access to Security Area:
c. Suspension of Security Clearance:
d. Denial/Revocation of Security Clearance:
e. Debarment Actions:
f. Other (suspicious activity)

ATTACHMENT I

JPL NM 1600-96, Personnel Security

CHAPTER 1. Introduction

1.1 Overview

a. Evaluate character and conduct of government workers with suitability determinations for positions covered by 5 C.F.R. pt.731 and continuous evaluation through reinvestigations of individuals in position of public trust as required by Exec. Order No. 13488.

b. Evaluate character and conduct of workers by making fitness determinations for contractor employment per contractual requirements.

c. Reserved

d. Reserved

e. Determine eligibility under Homeland Security Presidential Directive 12 (HSPD-12) for Personal Identity Verification (PIV) as mandated in Federal Information Processing Standards (FIPS) Publication 201-1 for access to Federal facilities and federally controlled information systems. Specifics for PIV processing are outlined in FIPS SP 800-79-1 and referenced in NPR 2841.1, Identity, Credential, and Access Management.

Additional comment: Specifics for PIV processing is outlined in NASA Interim Directive NID 1600.95 of June 3, 2011

1.2 Recordkeeping

1.2.1 Records and information related to this policy shall be managed in accordance with NPD 1440.6H, NASA Records Management, and NPR 1441.1D, NASA Records Retention Schedules. Personnel security files are temporary records and are destroyed in accordance with the disposition instructions NPR 1441.1D.

1.2.2. Information from personnel security files may be disclosed to a Federal agency, in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, conducting a security or suitability investigation, classifying a job, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

1.2.3. Subjects of personnel security investigations and screenings may request copies of excerpts, summaries, or any analytical extract of information from the NASA case file under the Freedom of Information and Privacy Act procedures. The subject may not be provided a copy of

any third party investigations (i.e., OPM, FBI). The subject must obtain copies of the third party investigation directly from the appropriate agency.

1.2.4 Reserved

1.2.5 OPM's Federal Investigative Services Division maintains the Personnel Investigations Processing System (PIPS), a computer system which maintains the Security/Suitability Investigations Index (SII), a repository of millions of background investigation records of Federal and contract employees, and military personnel. These records are maintained for a minimum of 16 years. NASA security specialists who are authorized by the Security Management Division Director may access these files and perform searches of the database to determine if an individual already has a background investigation that may serve for hiring, credentialing or security clearance determining. Authorized individuals can perform SII searches, request files, and transmit messages to the investigation provider. Other features include access to security clearance information through the Clearance Verification System (CVS).

Additional Comment – Some JPL contractors who support the personnel security function may be required to perform searches within CVS.

1.3. Responsibilities

1.3.1 Reserved

1.3.2 Reserved

1.3.3 The CCS/Chief of Protective Services (CPS) shall:

a. Reserved

b. Process and submit background investigation requests to OPM electronically. Electronic Questionnaires for Investigations Processing (e-QIP) are mandated for use to submit background investigations for civil servant and contractor employees to OPM. CCS/CPS will ensure that a check of OPM databases such as PIPS/CVS is performed to identify any previous investigation that will serve reciprocally before initiating a background investigation. The acceptance of prior determinations must be based on an equivalent investigation and evidence of a favorably adjudicated investigation on the individual.

c. Notify NASA Central Adjudicating Facility (CAF) personnel of any adverse information regarding anyone at the Center who holds a security clearance.

d. Reserved

e. Maintain close coordination with OPM Investigations Service (OPM-IS) and Federal Investigations Processing Service (OPM-FIPS) and process the appropriate requests for background investigations conducted.

f. Reserved

g. Reserved

h. Reserved

i. Reserved

j. Reserved

k. Reserved

l. Reserved

m. Reserved

n. Maintain, in accordance with the Privacy Act and existing NASA system of records, individual personnel security files on all investigated personnel; review applicable reports with officials in the review process who shall make the determination relative to continued access or revocation of access privileges. Files must contain, at a minimum:

(1) Copies of the OPM Case Closing Transmittal, Certification of Investigation, signed e-QIP release sheets and a signed and dated copy of the OPM Form OF79A.

(2). Any adverse information reports on affected contractor or civil servant employees.

Additional Comment – Some JPL contractors supporting personnel security function will be submitting background investigation requests to OPM and creating personnel security files. They must comply with above.

1.3.4 The CCS/CPS shall establish written procedures for the following:

a. Maintaining electronic files and distributing instructions for the completion of all electronic forms for the investigation process.

b. Assuring the appropriate investigation has been conducted for each NASA federal or contractor employee.

c. Referring medical related data in investigative files to the appropriate medical authority for review and evaluation if needed to make a credentialing decision.

d. Conducting local records checks or automated record checks when necessary to clarify, expand, or mitigate information that has been forwarded to the CCS/CPS.

1.3.5 The Director of Office of Human Capital Management (OHCM) at each Center shall:

a Reserved

b. Reserved

c. Reserved

d. Grant reciprocal recognition to prior suitability determinations in accordance with Exec. Order No. 13488 when:

(1). The gaining agency uses criteria from making fitness determinations equivalent to suitability standards established by OPM;

(2). The prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by OPM; and

(3). The individual has had no break in employment since the favorable determination was made.

e. Deny reciprocal recognition of a prior favorable fitness or suitability determination when:

(1). The new position requires a higher level of investigation than previously conducted for that individual;

(2). An agency obtains new information that calls into question the individual's fitness based on character or conduct; or

(3). The individual's investigative record shows conduct that is incompatible with the core duties of the new position

1.3.6. Reserved

1.3.7 Program, Line Mangers, and Supervisors shall:

a. Reserved

b. Coordinate with the CCS/CPS for the designation of risk for contractor employees and the timely on boarding of contractor employees.

1.4 Reserved

1.5 Violations of Security Requirements.

1.5.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA personnel security program is subject to disciplinary action up to

and including termination of employment and/or possible prosecution under 18 U.S.C.§ 799, that provides fines or imprisonment for not more than 1 year, or both.

CHAPTER 2. Access to National Security Information

2.1 Reserved

2.2 Reserved

2.3 Reserved

2.4 Reserved

2.5 Processing Personnel Security Requests in e-QIP

2.5.1 Electronic Questionnaires for Investigation Processing (e-QIP) is a secure website that is designed to transmit all personnel background investigation requests. These questionnaires are processed through e-QIP. The Standard Form (SF 86) is the questionnaire for National Security Positions. The SF 85P is the questionnaire used for Public Trust Positions and the SF 85 is the questionnaire for Non-Sensitive Positions.

2.5.2 Every e-QIP user – both agency staff and applicant – has specific responsibilities that correspond to e-QIP roles as follows:

a. Agency Advocate is the highest-level official within each activity and this role is shared between the AA Office of Protective Services and AA for Human Capital

b. Functional Administrator is the highest -level official within each functional area of NASA.

c. Technical Administrators are the experts in technology available at each agency and the

Agency Chief Information Officer (CIO).

d. Program Specialists serve as team leaders and manage day-to-day operations at each Center.

2.5.3 The Office of Personnel Management (OPM) has mandated that individuals who are given roles in Electronic Questionnaire for Investigations Processing (e-QIP) are vetted as follows:

a. NACLC (National Security) or MBI (Public Trust): Agency Administrator, Program Manager, Approver and Reviewer Role

b. User Administrator = SSBI (National Security) or BI (Public Trust): User Administrator

c. NACI : Business Manager Role, Initiator, and Agency Help Desk Role

2.5.4 e-QIP users must access the OPM portal as a gateway to the e-QIP database. The portal is a secure, encrypted environment known as the OPMIS secure portal. The OPMIS secure portal can be used for the exchange of Sensitive but Unclassified Information (SBU), such as Privacy Act Information and Personally Identifiable Information (PII). e-QIP users and other community members with portal access can send and receive email, review and download documents, and access information on OPM products and services. In addition to e-QIP, the portal acts as the gateway to OPM-FISD's computer systems (Personnel Investigations Processing System (PIPS) and Clearance Verification System (CVS)).

Additional Comment - JPL contactors supporting personnel security function must have the appropriate background investigation in order to be assigned a role in e-QIP

2.6 Sensitive Compartmented Information (SCI)

2.6.1 Candidates for SCI access must have a favorably adjudicated Top Secret investigation

2.6.2 Requests for access to Sensitive Compartmented Information (SCI) require the submittal of Form 2018A, (Special Access Request).

2.6.3 The Form 2018A must be prepared and justified by the employee's immediate supervisor, The line supervisor through the Division Director, or higher depending on the applicant's Organizational position shall also review and approve the submittal. The request is then forwarded along with copies of the employee's personnel security file (PSF) and an additional copy of an updated SF 86, to the HQ Special Security Office (SSO) for appropriate action.

2.6.4 The Form 2018A and the original signed SCI Non-disclosure Form shall be retained by the SSO representative at the Center.

2.6.5 *Investigative Standards for Background Investigations for Access to Classified Information*, established as a result of Exec. Order No. 12968, individuals with "Q", Top Secret (TS), or Sensitive Compartmented Information (SCI) access, are subject to periodic reinvestigations at any time following the completion of, but no later than five years from the date of the previous investigation

Additional Comment – JPL contractors who are submitted for SCI access must adhere to the above process.

2.7 Reserved

2.8 Reserved

2.9 Reserved

2.10 Reserved

2.11 Reserved

2.12 Reserved

2.13 Reserved

2.14 Bond Amendment

2.14.1 The Bond Amendment repealed 10 U.S.C. Section 996 formerly known as the Smith Amendment, and places restrictions that are similar to the Smith Amendment, but which apply to all Federal Government Agencies. The Bond Amendment bars persons from holding a security clearance for access to Special Access Programs, Restricted Data and SCI if they have been:

a. Convicted of a crime and served more than one year of incarceration

b. Discharged from the Armed Forces under dishonorable conditions

c. Determined to be mentally incompetent by a court or administrative agency

Additional Comment: JPL contractors who have Bond Amendment violations will not be eligible to have access to Special Access Programs, Restricted Data and SCI .

2.15 Reserved

2.16 Reserved

2.17 Reserved

2.18 Reserved

2.19 Classified Visits and Meetings

a. Reserved

b. Reserved

c. Reserved

d. Special Access Program Visits. All visit requests involving a special access program shall be processed by the appropriate Special Security Office.

CHAPTER 3. NASA Personnel Security Program

3.1 General

3.1.1 Reserved

3.1.2 Contractor employee means an individual who performs work for or on behalf of NASA under a contract and who, in order to perform the work specified under the contract, requires access to space, information, information technology systems, staff, or other assets of NASA. Such contracts include, but are not limited to:

3.1.3. NASA determines the fitness of contractor employees to perform work as contractor employees, prior favorable fitness or suitability determinations should be granted reciprocal recognition, to the extent practicable. Per Exec. Order No. 13488, there is no requirement that the prior favorable fitness or suitability determination must have been made within a specific time period. However, there must be no break in employment since a favorable determination was made. Exec. Order No. 13488 gives NASA the authority to grant reciprocal recognition to prior favorable fitness or suitability determinations made by other agencies.

3.1.4. Individuals covered by Exec. Order No. 13467 who perform work for or on behalf of the agency are subject to a background investigation to determine whether they are:

a. suitable for Government employment;

b. eligible for logical and physical access;

c. Reserved

d. Reserved

e. fit to perform work for or on behalf of the Government as a contractor employee.

3.1.5 Reserved

3.1.6 Reserved

3.1.7. Investigations that meet the requirements for a specified position shall be reciprocally accepted for that and lower investigations with no additional investigation provided there is no break in employment, derogatory or questionable information, or need based on change of position with a higher investigation requirement.

Additional Comment – JPL contractors will be vetted in accordance with EO 13488 and EO 13467

3.2 Reserved

3.3 Reserved

3.4 Designation of Risk Levels

3.4.1 Risk level designations for contracts, grants, cooperative agreements, and MOA or MOU shall be made by the NASA Center program office representative (typically the designated Civil Service project manager (sponsor), COTR, in coordination with the CCS/CPS, and IT Security Manager(s).

3.4.2 Reserved

3.4.3 Reserved

3.4.4. The risk level should be determined in the statement of work of the contract and it determines the investigative requirements for the contractor employee who shall perform the work.

3.4.5. Fitness determinations will be conducted for contractor employees per contractual requirements.

3.4.6. If an employee's duties require any overlap into a higher or lower risk level, the position risk must then be set at the highest risk level anticipated.

Additional Comment – JPL employees will have a position description describing the nature of the work that will be performed. The categories of the position description will consist of narrative for describing the position, knowledge required by the position, supervisory controls, guidelines, complexity, scope and effect, personal contacts, purpose of contacts, physical demands, and work environment for each contractor employee assigned to the contract. The duties will describe the nature of the duties and include a risk level determination to those duties of low, medium or high. OPM example for this process can be found at Federal classification and job grading systems guidance as provided at http://www.opm.gov/fedclass/html/gsclass.asp

3.5 HIGH RISK: Is a Public Trust Position.

High Risk positions are those that have the potential for exceptionally serious impact involving duties especially critical to the Agency or a program mission of the Agency with broad scope of policy or program authority.

3.6. MODERATE RISK: Is a Public Trust Position.

Moderate Risk positions are those that have the potential for moderate-to-serious impact involving duties of considerable importance to the Agency or a program mission of the Agency with significant program responsibilities and delivery of customer services to the public.

3.7 Low Risk:

Low Risk positions are those that have the potential for impact involving duties of limited relation to the Agency mission with program responsibilities with affect the efficiency of the service. It also refers to those positions that do not fall within the definition of a High or Moderate Risk position. Positions designated at the Low Risk level are not considered Public Trust positions.

3.7.1 Reserved

3.7.2. In instances where there is a wide variance in the security risk level of the work to be performed, individual contractor employees must be processed at the risk designation commensurate with the highest risk level of their duties. In meeting this contingency, the contract, grant, MOA, or MOU must specifically apply controls to ensure that work of the lower risk positions does not overlap with that for the higher risk position

3.7.3 Reserved

3.7.4. The entire contract, grant, MOA, or MOU may be designated High or Moderate Risk due to the former case, but those NASA contractor employees whose work would be Moderate or Low Risk must be investigated accordingly.

3.7.5. The contractor and COTR must specify control measures to be used to ensure that there is no overlap of work duties between the lower designated positions.

3.8 Lautenberg Amendment

3.8.1. Federal and Contractor employees in positions that require the carrying of a firearm are affected by the Lautenberg Amendment to the Gun Control Act of 1968, effective 30 September 1996. The amendment makes it a felony for those convicted of misdemeanor crimes of domestic violence to shop, transport, possess, or receive firearms or ammunition. The amendment also makes it a felony to transfer a firearm or ammunition to an individual known or reasonably believed to have a conviction.

Additional Comment – JPL contractors who have felony or misdemeanor crimes of domestic violence will not be eligible for work that requires the carrying of a firearm

3.9 Personnel Security Background Investigations Requested by NASA

3.9.1 NASA will comply with OPM standards for requesting background investigations. Use the chart to select the appropriate investigation.

For this Position Designation:	You will use this request format:	To request this investigation:
Risk/Sensitivity Level	**Standard Forms**	**You will use the following OPM Investigative Products**
Non-Sensitive Position Low Risk/HSPD-12 Credential	SF 85 (Questionnaire for Non Sensitive Positions) OF 306	National Agency Check and Inquiries (NACI)
Moderate Risk Public Trust Position (No national security sensitivity)	SF 85P (Questionnaire for Public Trust Positions) OF 306	Moderate Risk Background Investigation (MBI) (Limited Background Investigations (LBI) will be eliminated. After October 1, 2010 requests for LBI will be converted to MBI.)
Risk Public Trust Position (No national security sensitivity)	SF 85P (Questionnaire for Public Trust Positions) OF 306	Background Investigation (BI) (Public Trust Special Background Investigations (PTSBI) will be eliminated. After October 1, 2010 requests for PTSBI will be converted to BI.)
Secret/Confidential (Undesignated – e.g., Military/Contractor)	SF86 (Questionnaire for National Security Positions)	National Agency Check with Law and Credit (NACLC)
Noncritical-Sensitive Position and/or Secret/Confidential Security Clearance (Low Risk)	SF 86 (Questionnaire for National Security Positions)	Access National Agency Check and Inquiries (ANACI)
Noncritical-Sensitive Position and/or Secret/Confidential Security Clearance (Moderate Risk)	SF 86 (Questionnaire for National Security Positions)	Moderate Risk Background Investigation (MBI)
Critical-Sensitive Position and/or Top Secret (TS) Security Clearance (Any level of risk)	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)
Special-Sensitive Position and/or TS Security Clearance with Sensitive Compartmented Information (SCI) (Any level of risk)	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)
Position Sensitivity (any level) with High Risk Public Trust	SF 86 (Questionnaire for National Security Positions)	Single Scope Background Investigation (SSBI)

3.9.2 Reserved

3.9.3. The NASA employee shall submit a fingerprint and complete and submit the electronic forms in e-QIP, and sign the appropriate release pages.

3.9.4. The timing of security form submittal and the established risk level may dictate whether a proposed NASA employee can begin work prior to a final access determination. Based on the specifics of the situation and a preliminary review of the fingerprint results and submitted forms, the CCS/CPS shall advise the sponsor whether the individual can commence working prior to the receipt of the completed investigation and final access determination.

3.9.5. Pre-assignment Checks for **High Risk** Positions.

3.9.5.1. Upon selection, but prior to assignment, a check will be performed to determine if an appropriate investigation has already been completed and favorably adjudicated that will serve; or a background investigation is initiated for the employee in e-QIP.

3.9.5.2. Upon review of information in the completed e-QIP, the reviewer may:

a. Request additional information from the subject and conduct screening to resolve any issues that are found during the review process; or,

b. Release the electronic form to the e-QIP Approver to transmit the investigation to the investigation provider and await final results; or,

c. Grant interim authority to access a NASA Center pending receipt of completed investigation and final access approval determination; or,

d. Deny access and take the necessary actions.

3.10 Investigation and reinvestigation Requirements for NASA Contractor employees without access to CNSI

3.10.1. Contractor employees performing low risk work will submit a National Agency Check with Inquiries (NACI) in e-QIP on a SF 85 with a finger print card (FD 258). Contractor employees are not required to submit an application or resume. However, investigations requested on the SF 85 require the applicant to answer specific questions found on the OF 306 (2001 version): 1, 8, 9, 10, 11, 12, 13, 16, and 17a. To provide that additional information, the OF 306 may be used, or the specific questions and answers may be provided on an attachment to e-QIP. Reinvestigations for low risk contractor employees will be a NACI with a FD 258 fingerprint card every ten years or sooner if determined by the governance agency.

3.10.2. Contractor employees performing moderate risk work will submit a Minimum Background Investigation (MBI) in e-QIP on a SF 85P and a fingerprint card (FD 258). Reinvestigations with be performed every five years on a National Agency Check with Law and Credit with a fingerprint card (FD 258).

3.10.3. Contractor employees performing high risk work with no access to CNSI will submit a Background Investigation (BI) in e-QIP on a SF85P with a fingerprint card (FD 258). Reinvestigations will be performed every five years with a Periodic Reinvestigation (PRI) with a fingerprint card (FD 258).

3.10.4. When a contractor employee experiences a change in work due to promotion or reassignment and the risk level is higher; a new investigation commensurate to the risk should be initiated within 14 calendar days after the promotion or reassignment is final.

3.11 Individuals with Prior Criminal Record

3.11.1 Individuals with a criminal record (except minor traffic) will be adjudicated in accordance with “Memorandum to Heads of Departments and Agencies, Chief Human and Security Clearance Decision Making Guide”.

a. If an individual is still under probation/parole or incarcerated for a felony conviction, this alone serves as an immediate disqualifying factor for physical/logical access based on the unacceptable risk the criminal activity poses to a NASA. A felony is defined as a serious crime which in the US is usually punishable upon conviction either by a large fine, or by a term of imprisonment longer than one year, or by both a large fine and imprisonment, or which is punishable by death. The PIV Authorizer will notify the PIV Sponsor that processing has been suspended.

b. At such a time as the hearing, trial, criminal prosecution, sentencing, suspended sentencing, deferred sentencing, incarceration, probation, or parole has been completed; the individual may be resubmitted to the identity verification process to determine eligibility for a credential.

3.11.2 If the CCS/CPS determines that access is justified based on compelling mitigating factors, then the investigative records and a signed memorandum containing a full justification for favorable consideration will forwarded to the AA for Protective Services.

a. The AA for Protective Services via the NASA CAF, in consultation with the Headquarters (HQ) Office of General Counsel (OGC), makes the final determination and forwards the results to the Center Chief of Security.

b. Physical or logical access PIV credentials may not be granted until approval is acted upon by the AA for Protective Services.

3.12 Adverse Information

3.12.1. When adverse information is self reported, developed or received in the course of any personnel security investigation, or subsequent to such investigation and initial favorable determination, the scope of inquiry shall be expanded to the extent necessary to obtain sufficient information to make a reasonable and sound determination. A determination must be made that the employee is fit to perform work for or on behalf of the Government and/or eligible for logical and physical access in accordance with Exec. Order No. 13467.

3.12.2. Counterintelligence-related adverse information is to be relayed as soon as possible, but no later than the next business day after the information has been obtained, to the Center Counterintelligence Office or the NASA Office of Protective Services.

3.12.3. A personal interview or expanded inquiry shall be held with employee on whom significant unfavorable or derogatory information has been developed or received during the screening process. The employee shall be offered an opportunity to refute, explain, clarify, or mitigate the information in question.

3.12.3.1. The personal interview or expanded inquiries may be conducted by a qualified NASA security official, by the original investigating agency, or another agency of the Federal Government at NASA's request.

3.12.3.2 Agency officials may conduct a new fitness or suitability determination at any time adverse information is obtained that calls into question an individual's fitness based on character or conduct. This may include a new background investigation or database query and adjudication

3.13 Reciprocity of other agency Adjudications and Adjudication Process for Contractor Employees

3.13.1. A check will be made of OPM's Central Verification System (CVS) by a NASA trusted information provider who has undergone a favorably adjudicated background investigation to determine if a prior investigation will serve reciprocally for a NASA determination for contractor fitness or access to physical and logical resources. If there is no favorably adjudicated background investigation that will serve reciprocally, a background investigation will be initiated in e-QIP for the contractor employee commensurate to the risk level associated with the work of the contract.

3.13.2. Reciprocal recognition of fitness will be granted to a prior favorable fitness or suitability determination when:

a. equivalent adjudicative criteria was used (5 C.F.R. pt. 731 for federal employees) and (OPM's Final Credentialing Standards for issuing Personal identity Verification Cards under HSPD-12 of July 31, 2008 was used for contractor employees) and;

b. the individual has had no break in employment since the favorable determination was made. With regard to contractor employees, a break in employment also refers to a break in employment on a Federal contract, and not just a break in employment with a particular contractor. If the individual has stopped working on a Federal contract, but continues to work for the contractor on a non-Federal contract, this is deemed to be a break in employment.

3.13.3. NASA personnel are not required to grant reciprocal recognition to a prior favorable fitness or suitability determination when:

a. the new position requires a higher level of investigation than previously conducted for that individual;

b. an agency obtains new information that calls into question the individuals fitness based on character or conduct; or

c. the individuals investigative record shows conduct that is incompatible with the core duties of the new position

3.13.3.1. To ensure alignment for purposes of fitness and suitability, a core duty is a continuing responsibility that is of a particular importance to the achievement of NASA's mission.

3.13.4. OPM's Final Credentialing Standards will be used by trained adjudicators when determining eligibility for physical and logical access only. PIV Authorizers must be trained in adjudication by certified adjudication training providers if they perform adjudication duties. A PIV card will not be issued to a person if:

a. The individual is known to be or reasonably suspected of being a terrorist;

b. The employer is unable to verify the individual's claimed identity;

c. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;

d. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;

e. There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or

f. There is a reasonable basis to believe the individual will use Federally-controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

g. There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;

h. There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;

i. There is a reasonable basis to believe; based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV card poses an unacceptable risk;

j. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

k. There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

l. A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or

m. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

3.13.6. For the purpose of this adjudicative policy, the "whole person concept" is defined by those eligible for physical and logical access shall be granted for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicate there is no unacceptable risk to the life, safety or health of employees, contractors, vendors, or visitors; to the government physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial or medical records; or to the privacy of data. An individual's trustworthiness, honesty, reliability, discretion, and sound judgment are fundamental to the adjudicative process. This "whole person concept" will provide a balanced assessment of positive as well as negative aspects of an individual's past and present activities.

3.13.7. Adjudicators will use the OPM's Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide, January 14, 2008 as a resource for deriving a reasonable conclusion or decision based on the standards outlined in OPMs' Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD -12. Adjudicators will not add or delete or modify the adjudicative standards. Final adjudications will be performed within twenty days from receipt of a Report of Investigation (ROI) from OPM. The investigation closing date and adjudicative action will be recorded in IdMAX, OPM form INV 79A or electronically annotated in OPM PIPS under Agency Menu as soon as possible after adjudication. Batch files from IdMAX may also be uploaded into OPM's PIPS system.

3.14 Reconsideration Procedures for Contractor Employees and other Agency Affiliates

3.14.1 Notice of Proposed Action - When an adjudicator determines that a PIV applicant has not provided his or her true identity or is otherwise not suitable to be employed in the current or applied for position based on an unfavorable adjudication, the adjudicator shall provide the individual reasonable notice of the determination including the reasons(s) the individual has been determined to not have provided his or her true identity or is otherwise unsuitable. The notice shall state the specific reasons for the determination, and that the individual has the right to answer the notice in writing within 10 working days. The notice shall inform the individual of the time limits (usually 10 days for response), as well as the address to which such response should be made.

3.14.2 The individual may respond to the determination in writing and furnish documentation that addresses the validity, truthfulness, and/or completeness of the specific reasons for the determination in support of the response.

3.14.3 Decision – After consideration of the determination and any documentation submitted by the PIV applicant for reconsideration of the initial determination, the Center Chief of Security or his/her designee will issue a written decision (usually within 10 days), which informs the PIV applicant of the reasons for the decision.

3.14.4 Reconsideration – If a denial letter is provided and the subject subsequently requests an appeal, the Center Chief of Security /Chief of Protective Services shall appoint a panel to review the Credentialing Adjudication Review Panel (CARP) surrounding the denial or revocation. The panel shall be composed of three NASA employees who have demonstrated reliability and objectivity in their official duties. Panel members must have been the subjects of a favorable background investigation, and only one of the panel members shall be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the CARP or they may request to appeal in person to the CARP. Any approved personal appearance before the CARP shall be documented by means of a written summary or recording which shall not be made a part of the subject's security record.

3.14.5 Prior to finalizing the CARP determination, a CARP panel member or the center Chief of Security may refer the CARP proposed decision to the Center Director for an additional level of review. If no referral is made to the Center Director, the CARP decision is final. If there is a referral to the Center Director, the Director's decision is final.

3.14.6 Upon determination that a clearance revocation or denial has been upheld, there is no further reconsideration process. The individual may be debarred from access to the NASA center based on the denial for a period of one to three years. The IdMAX will reflect any debarments to the center based on denial or revocation of PIV.

NASA Procedural Requirements

JPL NPR 1620.2

COMPLIANCE IS MANDATORY

Subject: Facility Security Assessments

Responsible Office: Office of Protective Services

CHAPTER 1: Determining the Center/Facility Security Level

1.1 General

1.1.1. The initial FSL determination for new leased or owned space shall be made as soon as practical after the identification of a space requirement (including succeeding leases). The determination should be made early enough in the space acquisition process to allow for the implementation of required countermeasures (or reconsideration of the acquisition caused by an inability to meet minimum physical security requirements).

1.1.2 Risk assessments shall be conducted at least every 3 years for all facilities. There will be an FSL designated for the Center overall, and each facility within the Center will have its own FSL designation. Implementation of countermeasures inclusive of policies and procedures will be based on risk with the appropriate FSL level. The FSL will be reviewed and adjusted, if necessary, as part of each initial and recurring risk assessment. The responsibility for making the final FSL determination rests with the Center Director as the Designated Official, who must either accept the risk or fund security measures to reduce the risk:

a. For single-tenant Government-owned or -leased facilities, a representative of the Office of Protective Services shall make the FSL determination, in consultation with the Center Director responsible for the facility.

b. In multi-tenant Government-owned or -leased facilities, the Designated Official in coordination with a representative of each Federal tenant i.e., the Building Security Committee shall make the FSL determination in consultation with the owning/leasing department, or agency and the security organization(s) responsible for the facility.

c. A campus or NASA Center consists of two or more Federal facilities located contiguous to one another and sharing some aspects of the environment (e.g., parking, courtyards, vehicle access roads, or gates) or security features (e.g., a perimeter fence, guard force, or onsite central alarm/closed circuit television monitoring station). In multitenant centers, all individual facilities in the campus shall be assigned an FSL in accordance with this NPR.

d. While the incorporation of additional factors and criteria makes this NPR more useful to determine the FSL for special-use and other unique facilities, such as high-security laboratories, hospitals, or unique storage facilities for chemicals or munitions, some facilities may still not fit neatly into the criteria defined here. The criticality of the mission or the symbolic nature of the facility could be such that it merits a degree of protection above that specified for a FSL Level IV facility, even though the other contributing factors, such as population or square footage, might be scored lower. For example, a research laboratory might receive lower score values for symbolism, square footage, and population size. However, the laboratory may be responsible for critical research and diagnostic activities that are vital to protecting NASA research and intellectual property that if compromised could pose a threat to the United States National Security. This mission, combined with the fact that it may be the only such laboratory in the country, would suggest that the criticality factor would far outweigh lower score values in symbolism, population, and/or facility size, and thus the facility should be considered for a Level V designation. As a result, the criteria and decision-making authority for identifying Level V facilities are within the purview of the individual Center. As general guidance, Centers shall consider a facility as potentially suitable for a Level V designation if it receives a "very high" score value for criticality or symbolism and is a one-of-a-kind facility (or nearly so).

1.2 Purpose of a Center/Facility Security Level Determination

1.2.1. Not all NASA assets at all Centers and locations require the same degree of protection.

1.2.2. Protection of assets shall be based on a realistic assessment of the risk associated with the types of threats likely to be directed at the assets in their actual locations, the vulnerability of the asset, the asset value, and response capabilities of law enforcement and/or security forces.

1.2.3. Performing the Center/Facility Security Level assessment allows NASA managers to establish asset protection programs appropriate for their value and the likelihood of an attempt to compromise them.

1.2.4. The Center/Facility Security Level Determination allows Center management to prioritize assets so that physical security resources can be applied in the most efficient and cost-effective manner possible.

1.3 Risk

For the purposes of this NPR, Risk is identifying creditable threats, vulnerabilities, and measuring the probability of the consequences using countermeasures to mitigate the threats and vulnerabilities, and/or accepting the risk as they are associated with NASA assets.

1.4. Undesirable Events

The undesirable events to NASA facilities from criminal elements shall also be evaluated in determining the FSL. Consideration must be given to the risk from more common criminal acts, such as theft, assault, unlawful demonstrations, workplace violence, and vandalism—acts which historically occur more frequently at Federal facilities than acts of terrorism. Although terrorism

is of concern based on past events, it should not be the default threat unless there is creditable threat intelligence directly related to NASA assets.

1.5 Vulnerabilities

Vulnerabilities for purposes of this NPR are identified as the unmitigated threats and/or mitigated threats of a NASA asset that still could be compromised. Although the vulnerability may be already mitigated, outdated technologies or more sophisticated threats may create the vulnerability.

1.6 Consequences

After identifying the threats and vulnerabilities of NASA assets, a consequence shall be identified as a result of the attack. Based on the severity of the attack and the criticality of the asset, the consequence will need to be mitigated. Although the consequence could be severe, the likelihood of threat event taking place could be low. This should not be reason to eliminate or not address the consequences of the threat and vulnerabilities. It should be a consideration of the mitigation strategy implemented.

1.7 Assets

NASA assets are people, property, and information. Much of the direction of the NASA Critical Infrastructure Protection Program (NCIPP) is directed at protecting NASA critical infrastructure assets. Typically, it is the potential publicity that would come with bombing a NASA facility or destroying and compromising a critical or symbolic NASA resource that an aggressor would find desirable. The NASA Security Program is based upon protecting the greater installation, its critical facilities, and other critical assets, which will, in turn provide greater protection for NASA assets.

CHAPTER 2: Scoring Factors of the Determination Matrix

2.1 FSL Matrix (NASA FORM 1805)

2.1.1 The FSL matrix uses five equally weighted security factors to be evaluated, with corresponding points of 1, 2, 3, or 4 allocated for each factor. The sections that follow provide the criteria to be used in evaluating each factor and assigning points. However, the criteria cannot capture all of the circumstances that could be encountered. Thus, the NPR includes a sixth factor— intangibles—to allow the assessor to consider other factors unique to the department/agency needs or to the facility.

2.1.2 Additionally, although the requirement for assessment-specific judgment has been reduced to the extent possible, it may still be necessary. To that end, this NPR includes an explanation of why each factor was included, a description of its intended impact on the score, and examples to allow security professionals encountering conditions that do not clearly match those anticipated here to make an informed decision based on the same rationale used in the development of this process.

2.1.3 To use the FSL matrix, each of the factors will be examined and a point value assigned based on the scoring criteria provided. The points for all factors will then be added together and a preliminary FSL identified, based on the sum. The assessor may then consider any intangibles that may be associated with the facility. An adjustment to the FSL shall be made (and documented) accordingly, and a final FSL determined.

Table 1 FSL Matrix

Factor	Points 1	2	3	4	Score
Mission Criticality	LOW	MEDIUM	HIGH	VERY HIGH	
Symbolism	LOW	MEDIUM	HIGH	VERY HIGH	
Facility Population	< 100	101–250	251–750	> 750	
Facility Size	< 10,000 sq. ft.	10,001–100,000 sq. ft.	100,001–250,000 sq. ft.	> 250,000 sq. ft.	
Threat to Tenant Agencies	LOW	MEDIUM	HIGH	VERY HIGH	
					Sum of above
Facility Security Level	**I** 5–7 Points	**II** 8–12 Points	**III** 13–17 Points	**IV** 18–20 Points	Preliminary FSL
Intangible Adjustment	Justification				+ / - 1 FSL
					Final FSL

2.2 Mission Criticality

2.2.1 The value of a facility to NASA is based largely on the mission of the facility, particularly as it may relate to NCIPP and other important business of the Government.

2.2.2 At NASA, facilities considered to be Mission Essential shall be included. As vital as it is for the NASA to perform these activities, it is equally attractive to adversaries to disrupt important NASA missions. The mission criticality score is based on the criticality of the missions carried out by tenants in the Center/facility. In a multi-tenant or mixed-multi-tenant facility, the highest rating for any tenant in the facility should be used for this factor. COG and COOP documents are good sources of information regarding the performance of essential functions.

Table 2 Criticality Scoring

Value	Points	Criteria	Examples
Very High	4	Communications centers that support national essential NASA functions NASA essential communications equipment necessary for defense or intelligence activities. NASA individuals necessary to advance American interests with foreign governments. NASA government officials of foreign nations NASA individuals or specialized equipment necessary to identify and analyze threats to homeland security	Intelligence community facilities, including communications and weapons/munitions storage Emergency operations centers, national response assets (e.g., Nuclear Emergency Support Teams) CNSI TS/SCI Program, SCIF Operations, National Security Programs
High	3	Original, irreplaceable material or information central to the daily conduct of NASA. Designated as a shelter in the event of an emergency incident. Center or headquarters policy and management oversight. Biological/chemical/radiological/medical research or storage of research and development (de minimis) quantities of chemicals, biohazards, explosives, and similar items. COOP facilities for department and agency headquarters. General criminal investigative work.	Special Program Area Storing CNSI, MEI Facility, Other Very Sensitive Documents or Equipment, SEB, Mishap Investigation Facility
Medium	2	State-wide service or regulatory operations. COOP facilities for other than national headquarters.	Building, Program or Code Has Requested Accountability Controls, Access to Program Area Not Storing CNSI, No MEI Facility
Low	1	Administrative, direct service, or regulatory activities	Visitors Center, Roadways, Cafeterias, Gift Shop, Recreation Facilities,

2.3 Symbolism

2.3.1 The symbolism of the facility is based on both its attractiveness as a target and the consequences of an event. The symbolic value is first based on external appearances or well-known/publicized operations within the facility that indicate it is a NASA facility. Domestic criminals may seek to make a statement against NASA for many reasons that range from espionage, vandalism, sabotage, assault, or a number of other criminal acts. It should be recognized that the partnerships that NASA has with foreign governments and various contractors sometimes presents opportunities for these types of crimes to occur and should be considered when evaluating threats.

2.3.2 Symbolism is also important because of the potential negative psychological impact of an undesirable event occurring at a prominent Federal facility. Attacks at certain NASA facilities, particularly those that are perceived to be well-protected and central to the safety and well-being of NASA, could result in a loss of confidence of NASA and the U.S. Government domestically or internationally.

2.3.3 It is also necessary to recognize that even if there are no external appearances or well-known operations of NASA, a mixed-tenant or mixed-multi-tenant facility may be symbolic to terrorists with other motivations. For example, facilities such as financial institutions, communications centers, transportation hubs, and controversial testing laboratories may be symbolic in the eyes of single-interest radicals and international terrorist organizations, whose leaders have stated that strikes against the American economy are a high priority. The symbolism of non-U.S. Department of Defense (DOD) Federal facilities on a DOD campus shall be assessed similarly.

Table 3 - Symbolism

Value	Points	Criteria	Examples
Very High	4	Popular destination for tourists. A nationally significant historical event has occurred at the facility. Contains significant original historical records or unique artifacts that could not be replaced in the event of their damage or destruction. Executive department headquarters building. Other prominent symbols of U.S. power or authority.	Centers or NASA facilities that meet these criterion
High	3	Well-known, regional U.S. Government facility. Agency/bureau headquarters. Located in a symbolic commercial financial building. Co-located with other nongovernmental but highly symbolic facilities.	Centers or NASA facilities that meet these criterion
Medium	2	Readily identified as a U.S. Government facility based on external features. Readily identified as a U.S. Government facility based on the nature of public contact or other operations (even without external features). Dominant, single Federal facility in a community or rural area. Nongovernmental commercial laboratory or research facility that may be symbolic to single-interest radicals.	Centers or NASA facilities that meet these criterion
Low	1	No external features or public contact readily identifying it as a U.S. Government facility.	Centers or NASA facilities that meet these criterion

2.4 Facility Population

2.4.1The infliction of mass casualties is an acknowledged goal of many terrorist organizations. Recovered terrorist preoperational surveillance reports include considerable details on the times of day that the target population is at its highest and do not distinguish between tenants and visitors. From a consequence perspective, the potential for mass casualties shall be a major consideration.

2.4.2 Thus, the facility population factor is based on the peak total number of personnel in Government space, including employees, onsite contract employees, and visitors. This number shall not include such transient influxes in population as an occasional conference (or similar event), unless the facility is intended for use in such a manner (such as a conference center) and the population is part of normal business. Transient shifts in population such as the occasional conference should be addressed by contingency security measures.

2.4.3 The number of daily visitors shall be determined using the best metrics available to ensure the most accurate population. Ideally, this would be achieved through a review of visitor logs or access control lists; however, it may necessitate an estimate or a short-term sampling of visitor throughput.

2.4.4 Facilities such as stand-alone parking garages shall be considered to have a "population" of less than 100.

2.4.5 The sensitive nature of childcare centers located in Federal facilities requires every Federal childcare center or facility with a childcare center to receive a facility population score of "very high" and a point value of 4.

2.4.6 If the non-Federal population of a mixed-tenant or mixed-multi-tenant facility contributes to the target attractiveness (e.g., creates a substantial population over and above the Federal population), document the rationale and add 1 point, not to exceed the maximum of 4 points.

Table 4 - Facility Population

Value	Points	Criteria
Very High	4	Greater than 750 or facilities with childcare centers
High	3	251 to 750
Medium	2	101 to 250
Low	1	Less than 100

2.5 Facility Size

2.5.1 The facility size factor is based on the square footage of all Federally-occupied space in the facility, including cases where an agency with real property authority controls some other amount of space in the facility. If the entire facility or entire floors are occupied, gross square footage should be used (length x width); if only portions of floors are occupied in a multi-tenant facility, assignable or rentable square footage should be used.

2.5.2 Size may be directly or indirectly proportional to the facility population. An office facility with a large population will generally have a correspondingly large amount of floor space; however, a large warehouse may have a very small population.

2.5.3 For a terrorist, an attack on a large, recognizable facility results in more extensive press (video) coverage. However, it should also be understood that large facilities require a more substantial attack to create catastrophic damage, entailing more planning and preparation by adversaries, which could be a deterrent.

2.5.4 From a consequence perspective, the cost to replace or repair a large facility is a major consideration. The National Infrastructure Protection Plan considers the cost to rebuild a facility in determining the potential economic impact of a successful attack.

2.5.5 If the total size of a mixed-tenant or mixed-multi-tenant facility beyond that occupied by the Federal population contributes to the target attractiveness (e.g., creates a highly recognizable structure based on size alone), document the rationale and add 1 point, not to exceed the maximum of 4 points.

Table 5 - Facility Size

Value	Points	Criteria
Very High	4	Greater than 250,000 square feet
High	3	100,000 to 250,000 square feet
Medium	2	10,000 to 100,000 square feet
Low	1	Up to 10,000 square feet

2.6 Campuses, Complexes, and Federal Centers

2.6.1 A campus consists of two or more Federal facilities located contiguous to one another and sharing some aspects of the environment (e.g., parking, courtyards, vehicle access roads, or gates) or security features (e.g., a perimeter fence, guard force, or onsite central alarm/closed circuit television monitoring station). It may also be referred to as a "complex" or "Federal center."

2.6.2 In the case of a campus that houses a single tenant, such as some of NASA Center's, an overall FSL shall be established for the Center and for each facility within the Center. Single tenant in this scenario will consist of all NASA and NASA contractor's physical space. If this Center is shared with a DOD entity, the perimeter of the facility where the demarcation point(s) are located will be considered the NASA Center. If the NASA facility sits within another property footprint, this NASA facility will be considered a single tenant facility and will require its own assessment unless the organization that has real property authority is consistent with ISC Criteria and meets this NPR. In multi-tenant campuses, all individual facilities in the campus will either be assigned an FSL in accordance with this NPR, or all tenants may agree to determine an overall FSL for the entire campus with the approval of the OPS HQ Associate Administrator, treating the entire campus as though it were a multi-tenant facility (using the

highest rating of any tenant in the facility for each factor). All NASA facilities that are being leased through NASA or the General Service Administration will follow this NPR.

2.7 Undesirable Events to NASA Centers/Facilities

2.7.1 Unlike the criticality of mission criterion, which is considered in terms of consequences, the threat to tenant agencies criterion is considered from a perspective of target attractiveness. The facility will be viewed in terms of whether the nature of public contact required in or resulting from the conduct of business is adversarial, whether there is a history of adversarial acts committed at the facility, against facility tenants, or against the tenant agencies elsewhere. To determine undesirable events, inquires to the OPS Counter-Intelligence Division shall be made as well as reading the ISC's Design Basis Threat Update document.

2.7.2 The highest score applicable to any tenant in a multi-tenant facility will be considered when determining the FSL, even though it may be possible to limit the implementation of countermeasures for that threat to a specific tenant's space or part of the facility.

2.7.3 As with the impact of commercial tenants on the facility's symbolism score, the potential threat to non-Federal tenants in a mixed-tenant or mixed-multi-tenant facility may result in a collateral risk to Federal tenants. Thus, in considering the criteria, the threat to all tenants in a facility— including non-Federal tenants—should be considered and the highest score used for the rating.

Table 6 – Undesirable Events

Value	Points	Criteria	Examples
Very High	4	Tenant mission and interaction with certain segments of the public is adversarial in nature. Tenant mission is controversial in nature and routinely draws the attention of organized protest groups. Located in a high-crime area. Significant history of violence directed at or occurring in the facility. More than 10 incidents per year requiring law enforcement/security response for unruly or threatening persons on site.	Centers or Facilities that meet this criterion.
High	3	Public contact is occasionally adversarial based on the nature of business conducted at the facility. History of demonstrations at the facility. Located in a moderate-crime area. History of violence directed at the facility or the occupants; 5–10 incidents per year requiring law enforcement/security response for unruly or threatening persons on site.	Centers or Facilities that meet this criterion.
Medium	2	Generally non-adversarial public contact based on the nature of business conducted at the facility. History of demonstrations against the tenant agency (not at the facility). Located in a low-crime area. History of violence directed at tenant agencies/companies (not at the facility).	Centers or Facilities that meet this criterion.
Low	1	Generally little-to-no public contact. No history of demonstrations at the facility. No history of violence directed at the facility or the occupants.	Centers or Facilities that meet this criterion.

2.8 Intangible Factors

2.8.1 It is not possible for this criterion to take into account all the conditions that may affect the FSL decision for all the different NASA Centers/Facilities. Certain factors, such as a short duration of occupancy, may reduce the value of the facility in terms of investment or mission, which could justify a reduction of the FSL. Such factors shall be indicative of a reduced value of the facility itself and a corresponding reduction in the consequences of its loss.

2.8.2 Other factors may suggest an increase in the FSL, such as the potential for cascading effects or downstream impacts on interdependent infrastructure, or costs associated with the reconstitution of the facility.

2.8.3 Accordingly, the FSL may be raised or lowered one level at the discretion of the Associate Administrator by a written request of the Center Security Chief and the concurrence of the Center Director based on intangible factors. However, the intangible factor shall not be used to raise or lower the FSL in response to a particular threat act. The FSL characterizes the entire facility; concerns about specific threats should be addressed with specific

countermeasures, even if they are over and above those required as the baseline for a particular security level.

2.8.4 Short-term events could also temporarily affect the factors evaluated here. Unless these events happen on a recurring basis, they should not affect the FSL determination. Instead, contingency plans shall be developed to implement temporary measures until the event has passed. For example, a weeklong conference may increase the population of a facility substantially during the conference, but it should not be considered in the FSL determination. On the other hand, if the facility is a conference center that normally holds such gatherings, the population during those conferences should be factored into the FSL.

2.8.5 Like all risk-management decisions, it is important to document these intangible factors and the resulting adjustments made to the FSL score. The decision-making authority should document any intangible factors and the associated adjustment and retain this information as part of the official facility security records.

CHAPTER 3: Level V Facilities

3.1.1 While the incorporation of additional factors and criteria makes this NPR more useful to determine the FSL for special-use and other unique facilities, such as high-security laboratories, hospitals, or unique storage facilities for chemicals or munitions, some facilities may still not fit neatly into the criteria defined here. The criticality of the mission or the symbolic nature of the facility could be such that it merits a degree of protection above that specified for a FSL Level IV facility, even though the other contributing factors, such as population or square footage, might be scored lower.

3.1.2 For example, a research laboratory might receive lower score values for symbolism, square footage, and population size. However, the laboratory may be responsible for critical research and diagnostic activities that are vital to protecting the Nation’s citizenry or animal and food products from disease agents accidentally or deliberately introduced into the United States. This mission, combined with the fact that it may be the only such laboratory in the country, would suggest that the criticality factor would far outweigh lower score values in symbolism, population, and/or facility size, and thus the facility should be considered for a Level V designation. As a result, the criteria and decision-making authority for identifying Level V facilities are within the purview of the individual agency. As general guidance, agencies shall consider a facility as potentially suitable for a Level V designation if it receives a “very high” score value for criticality or symbolism and is a one-of-a-kind facility (or nearly so).

CHAPTER 4: Transition to NPR 1620.3

4.1.1Once the FSL determination has been established, the security specialist shall move to NPR 1620.3 to implement the countermeasures that are associated with the FSL level. The corresponding FSL numeric number is found at the top of the columns of Chapter 7 of NPR 1620.3. Based on risk to the asset, an appropriate level of protection will be implemented. The DHS document, The Design Basis Threat, 2011 should also be consulted to determine if credible threats pertain to the NASA facility being assessed.

Appendix A: Definitions

Campus: Two or more Federal facilities located contiguous to one another and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected facilities. A campus may also be referred to as a "Federal center" or "complex."

Designated Official: The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials. For facilities owned and leased by the U.S. General Services Administration (GSA), the definition appears in Title 41, Section 102-71.20, of the *Code of Federal Regulations* (41 C.F.R. 102-71.20). For the purposes of NASA, the Center Director shall be the Designated Official.

Essential Functions: Government functions that enable Federal Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the industrial/economic base in an emergency.

Facility Security Level: A categorization based on the analysis of several security-related facility factors, which then serves as the basis for the implementation of certain protective security measures specified in other ISC standards.

Federal Departments and Agencies: Those executive departments enumerated in 5 U.S.C. §101, and the U.S. Department of Homeland Security (DHS); independent establishments as defined by 5 U.S.C. §104(1); Government corporations as defined by 5 U.S.C. §103(1); and the United States Postal Service.

Federal Facilities: Leased and owned buildings and facilities in the United States (inclusive of its territories) occupied by Federal Executive Branch employees for nonmilitary activities.

Mixed-Tenant Facility: A facility that includes one Federal tenant as well as non-Federal tenants, including commercial and State/local government tenants.

Multi-Tenant Facility: A facility that includes tenants from multiple Federal departments and agencies but no non-Federal tenants.

National Essential Functions (NEFs): That subset of essential functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through the Continuity of Operations (COOP) and the Continuity of Government (COG) capabilities.

Primary Mission Essential Functions: Those essential functions that must be performed to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

Security Organization: The Government agency or an internal agency component responsible for physical security at the specific facility (e.g., the DHS Federal Protective Service, NASA Office of Protective Services).

Single-Tenant Facility: A facility that only includes one Federal tenant or multiple components of the same Federal department or agency that fall under one "umbrella" for security purposes.

Special-Use Facilities: An entire facility or space within a facility itself that contains environments, equipment, or data normally not housed in typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, hospitals, aircraft and spacecraft hangers, or unique storage facilities designed specifically for such things as chemicals and explosives.

Appendix B: Acronyms

CNSI	**Classified national security information**
CUI	**Controlled unclassified information**
DHS	**Department of Homeland Security**
DOD	**Department of Defense**
FSL	**Facility Security Level**
HSPD-7	**Homeland Security Presidential Directive**
ISC	**Interagency Security Committee**
NCIPP	**NASA Critical Infrastructure Protection Program**
NPR	**NASA Procedural Requirement**
OPS	**Office of Protective Services**
PDD-62	**Presidential Decision Directive**
SBU	**Sensitive But Unclassified**

National Aeronautics and Space Administration

SENSITIVE BUT UNCLASSIFIED (SBU)

S B U

THIS INFORMATION MAY BE EXEMPTED FROM DISCLOSURE BY STATUTE, INCLUDING INFORMATION EXEMPT FROM DISCLOSURE BY THE FREEDOM OF INFORMATION ACT EXEMPTION CRITERIA

DEGREE OF PROTECTION: When not under the continuing control and supervision of a person authorized access to such material, it must be, at a minimum, maintained under locked conditions. Handling, storage, and reproduction must be in accordance with applicable Executive Orders, statutes, and agency implementing regulations. Keep access and reproduction to the absolute minimum required for mission accomplishment.

VIOLATIONS AND SANCTIONS: Individuals may be subject to administrative sanctions if they disclose information designated SBU. Sanctions include, *but are not limited to,* a warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal or discharge.

DECONTROL IN ACCORDANCE WITH NPR 1600.1

Check appropriate boxes (refer to Section 5.24 of NPR 1600.1):

- ☐ Arms Export Control Act
- ☐ Business/Company Confidential
- ☐ Developing or Current Technology Information
- ☐ Emergency Contingency/Continuity of Operations Information
- ☐ Export Administration Act
- ☐ Financial Institution Information
- ☐ Geological/Geophysical Information
- ☒ Infrastructure or Security Vulnerabilities Information
- ☐ Inter or Intra-Agency Memoranda or Letters
- ☐ Internal Personnel Rules/Practices
- ☐ Investigative Records
- ☐ NASA Information Technology/ Internal Systems Data
- ☐ NASA Sensitive
- ☐ Patent Information
- ☐ Personnel, Medical and Similar Files
- ☐ Privileged/Proprietary Commercial or Financial Information
- ☐ Space Act (Sec. 303b)
- ☐ Subject to Trade Secrets Act
- ☐ Systems Security Data Information
- ☐ Other *(Specify)* _____

SBU Designation Applied By: Kathy Healy

Organization: HQS/OPS **Date:** 06/20/2011

Agencies external to NASA shall handle this document as

------ FOR OFFICIAL USE ONLY ------

NASA Procedural Requirement

JPL NPR 1620.3

Effective Date:

Expiration Date:

COMPLIANCE IS MANDATORY

Subject: Physical Security Requirements for NASA Facilities and Property

Responsible Office: Office of Protective Services

TABLE OF CONTENTS

PREFACE

P.1 Purpose

P.2 Applicability

P.3 Authority

P.4 Applicable Documents and Forms

P.5 Measurement/Verification

P.6 Cancellation

CHAPTER 1. Introduction

1.1 Responsibilities
1.2 Security Measures and Requirements
1.3 Physical Security Measures for Stand-Alone Facilities or Facilities Located in Foreign Countries
1.4 Risk Management and Risk Acceptance Process
1.5 Terms, Abbreviations and Acronyms

CHAPTER 2. Physical Security Vulnerability Risk Assessments

2.1 General
2.2 Use of Physical Security Vulnerability Risk Assessments
2.3 Implementation of Physical Security Vulnerability Risk Assessments

CHAPTER 3 – Physical Security Requirements for NASA Assets by Category
3.1 General
3.2 Categories of NASA Physical Assets
3.3 Aircraft and Components at NASA Aviation Facilities (Includes Remotely Piloted UAV and Balloons)
3.4 NASA Aircraft and Components Not at NASA Aviation Facilities
3.5 NASA Vehicles and/or Watercraft and Components
3.6 NASA Vehicles, Watercraft, or Aircraft with On-Board Classified or Sensitive Equipment
3.7 Petroleum, Oils, Lubricants (POL) at Bulk Storage Facilities
3.11 Facility Engineering Supply and Construction Material Storage Areas
3.12 Rocket Engine, Wind Tunnels, Simulators, and Other High-Speed Testing Facilities and Equipment
3.13 Research and Associated Facilities
3.15 Spacecraft (Shuttle, ISS, Etc.) and Associated Equipment
3.16 Industrial and Utility Facilities and Equipment
3.17 Arms, Ammunition, and Explosives (AA&E)
3.18 Mission-Critical and High-Risk Personnel
3.20 Administrative Support Facilities
3.21 Terrorism Counteraction Measures

CHAPTER 4 – Minimum Physical Security Requirements for Other Categories of NASA Property Not Necessarily Subject to Risk Assessment
4.1 Miscellaneous Pilferable Assets (Includes Hand-Held Precision Tools and Laptop Computers)
4.2 Administrative and Housekeeping Supplies and Equipment
4.3 Precious Metals/Materials
4.4 Mailrooms
4.5 Security of Medical Supplies and Equipment at Medical Facilities
4.6 NASA Visitor Centers and Outdoor Exhibit Displays
4.7 TV, VCR, DVD, Cameras, Bicycles and Other Sensitive Items

CHAPTER 5 – Keys, Locks Locking Devices (Including Hasps and Chains), and Protective Seals
5.1 Key Issuance
5.2 Master Keys
5.3 Key Depository
5.4 Locks
5.5 Key and Lock Accountability
5.6 Additional Key and Lock Controls for Key Containers
5.7 Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas
5.7 Additional Key and Lock Requirements
5.8 Chains
5.9 Use and Control of Protective Seals
5.10 Disposition of Used Seals
5.11 Changing Seals

CHAPTER 6 – Center Perimeter Physical Security and Barrier Requirements
6.1 Purpose
6.2 NASA Standard Perimeter Physical Security Requirements
6.3 Types of Barriers
6.4 General Considerations
6.5 Temporary Barriers
6.6 Security Fences
6.7 Security Fence Standards
6.8 Barriers
6.9 Doors, Windows and Skylights
6.10 Sewers, Culverts and Other Utility Openings
6.11 Utility Poles and Trees
6.12 Clear Zones
6.13 Inspection and Repair of Barriers
6.14 Signs and Posting of Boundaries

CHAPTER 7 – Security Criteria and Level of Protection (LOP)
7.1 Purpose
7.2 Details of Security Measures
7.3 Undesirable Events (UDEs)

APPENDIX A. Definitions

APPENDIX B. Acronyms

APPENDIX C. Verification Matrices

PREFACE

P.1 PURPOSE

a. This NPR establishes a baseline set of physical security measures to be applied for safeguarding and mitigating the risks to NASA assets to an acceptable level. The threats or undesirable events (UDEs) addressed by this NPR are primarily man made. A UDE is an incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency. UDEs are further explained in Chapter 7 of this NPR. Other threats to buildings, such as earthquakes, fire, or storms are beyond the scope of this document. Its objectives are to:

(1) Establish standardized NASA minimum perimeter physical security requirements for Centers.

(2) Establish NASA standardized Facility Security Levels (FSL) for specific categories of NASA assets. Each FSL corresponds to a level of risk, which then relates directly to a Level of Protection (LOP) and associated set of baseline security measures. Each FSL corresponds to a level of risk, which then relates directly to an LOP and associated set of baseline security measures. Specifically, the FSL directs the user to a set of baseline standards which may be customized to address site-specific conditions.

(3) Base physical security LOP on an established physical security vulnerability risk assessment process, outlined in NPR 1620.2, “NASA Physical Security Vulnerability Risk Assessments,” that allows Center management the flexibility to 1). Prioritize assets based on their FSL and criticality to the overall mission and, 2). Tailor FSLs II through IV LOP to meet local needs provided that FSL I or other more appropriate compensatory physical security enhancements have been implemented. As demonstrated in the chart below, the FSL directly relates to the Level of Risk and correlates to the Level of Protection.

Table A – Facility Security Levels

Facility Security Level	Level of Risk	Baseline Level of Protection
I	I	I
II	II	II
III	III	III
IV	IV	IV

(4) Ensure a comprehensive approach to meeting Federal facility security needs in today's threat environment, and that the scope (and cost) of security is commensurate with the risk posed to NASA assets and facilities.

P.2 APPLICABILITY

a. This NPR is applicable to NASA Headquarters and NASA Centers, including Component Facilities, to the Jet Propulsion Laboratory (JPL), and NASA contractors to the extent specified in their contracts. Address comments regarding this NPR to the Director, Security Management Division (DSMD), Office of Protective Services, NASA Headquarters-Washington, DC, 20546. Refer questions concerning the application of these requirements to specific NASA Centers to the appropriate NASA Center Protective Services Office.

P.3 AUTHORITY

(1) National Space Program, 42 U.S.C., § 2473(c) (1)

(2) NPD 1600.2C, NASA Security Policy

P.4 APPLICABLE DOCUMENTS AND FORMS

(1) Exec. Order No. 12977, Interagency Security Committee as amended by Exec. Order No. 13286

(2) PDD 62, Combating Terrorism

(3) PDD 67, Enduring Constitutional Government and Continuity of Government Operations

(4) National Aeronautics and Space Administration, 14 C.F.R. Pt. 1203

(5) NPR 1600.1, NASA Security Program Procedural Requirements, w/change 2

(6) NPR 1600.2, Physical Security Vulnerability Risk Assessments

(7) NPR 4200.1, NASA Equipment Manual

(8) NPR 4310.1, Identification and Disposition of NASA Artifacts

(9) NPR 8820.2, NASA Construction of Facilities Procedural Requirements.

(10) Government Accounting Office (GAO) - 02-95, Vulnerability Assessment of Federal Facilities, October 1995

(11) GAO - 03-08, Building Security - Security Responsibilities for Federally Owned and Leased Facilities, October 2002

(12) Homeland Security - Interagency Security Committee Standard (ISC), Physical Security Criteria for Federal Facilities, 2008

(13) Homeland Security - ISC, Facility Security Level Determinations for Federal Facilities, 2008

(14) Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection

(15) HSPD 20, National Continuity Policy

(16) National Institute of Standards and Technology Special Publication (NIST SP) 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

P.5 MEASUREMENT VERIFICATION

a. Center Directors and Center Chiefs of Protective Services (CCPS), or their designees determine and document compliance by applying a verification approach that is tailored to meet the needs of the Center. The Office of Protective Services (OPS) conducts functional reviews of the Centers and conducts spot-checks and inspections to review Center compliance and implementation.

b. To determine the OPS compliance with the requirements contained in this NPR, internal and external auditors responsible for verifying Headquarters requirements and processes shall evaluate performance against the requirements contained within this NPR

P.6 Cancellation

None

/S/
Dr. Woodrow Whitlow, Jr.
Associate Administrator
Mission Support Directorate

CHAPTER 1: General

1.1 Responsibilities

1.1.3 Center Chiefs of Protective Services Offices shall:

a. To the extent possible, ensure a physical security vulnerability risk assessment is conducted for all assets under their control in a timely manner. At a minimum, all NCI shall be subject to the appropriate security vulnerability risk assessment immediately upon designation as NCI and/or key resource and every three (3) years thereafter.

b. Ensure the physical security measures identified in this NPR are implemented as soon as practical, after funding is identified through the budgetary process.

b. Establish end-of-day security checks using Standard Form (SF) 701 (Activity Security Checklist) when storing Classified National Security Information (CNSI).

c. As required, notify the NASA Office of Inspector General of all crimes at NASA owned and/or leased facilities, to include theft or misuse of, or damage to, Government property.

1.1.4 Organizational Heads shall control and safeguard all property within their activity by:

a. Promptly report to the Center law enforcement/security organization, and assist in any investigative activity and resolve incidents involving loss, theft, misuse, or damage of NASA resources.

b. Implement security measures commensurate with the results of the physical security vulnerability risk assessment conducted by Center security personnel.

1.1.5 Organizations involved in logistic and supply operations shall protect supplies and equipment as indicated in this NPR.

1.1.6 Organizations assigned custody of controlled medical substances shall implement measures to safeguard them as required by this NPR. These responsibilities include:

a. Ensuring physical security responsibilities are fixed in the receipt, storage, issue, transportation, use, disposal, turn-in, and accounting for all controlled medical substances and sensitive items.

b. Providing specific security instructions to individuals who are in the possession and control of, or who are responsible for, controlled medical substances and sensitive items.

c. Ensuring the careful selection of personnel, including volunteer workers, who are assigned duties that require access to controlled medical substances and sensitive items storage areas or who have custodianship or possession of keys and combinations to locks securing these areas.

d. Taking action to deny access to controlled substances by individuals undergoing investigation, treatment, rehabilitation, or administrative action as a result of actual or suspected drug abuse or as a result of suspected illegal activity involving controlled drugs (for example, theft, wrongfully prescribing, and inventory manipulation.)

e. Establishing appropriate escort procedures and designating escort personnel, by name or duty position, to escort unauthorized people into storage areas.

f. Ensuring a Facility Security Coordinator (FSC) is appointed, in writing, by the medical facility manager to assure that appropriate protection is provided for all controlled medical substances and sensitive items.

1.2 Security Measures and Requirements

a. At a minimum, the baseline LOP identified in this NPR for each Facility Security Level (FSL) must be implemented unless a deviation (up or down) is justified by a risk assessment.

b. Physical security measures more stringent than those contained in this NPR may be implemented by a Center official based on the criticality or “value” of the asset under consideration, analysis of local threat, identified vulnerabilities, and available security resources. These measures shall be incorporated into the Center’s physical security plan as an annex or as a mission specific security plan

c. Provisions for security program funding shall be included in normal budget deliberations.

d. Tenant activities shall coordinate their security program status, and when appropriate, security requirements to the host installation, so support may be provided at reimbursable cost.

e. Provision of security measures beyond those required by this NPR and other NASA procedural requirements shall be determined on a case-by-case basis by the CCPS.

1.4 Risk Management and Risk Acceptance Process

1.4.1 The DO and security may disagree on the LOP required for a particular asset. When the DO disagrees on the LOP required, they may opt to acknowledge and accept the risk of implementing less stringent security measures than those required through the risk assessment process established in NPR 1620.2, NASA Physical Security Vulnerability Risk Assessment, provided the asset is not designated as NCI. In the case of a designated NCI asset, only the Assistant Administrator for Office of Protective Services may accept the risk.

1.4.2 Every effort will be made to resolve the differences at the Center level. Management will:

a. Document their position regarding the required security measures, and outline their recommended alternative approach.

b. Include any pertinent information, including an acknowledgement of risk.

c. Submit to the CCPS, who will review and concur/non-concur.

d. If concurrence is given, no further action is necessary. A copy of all documentation will be maintained at the Center Protective Services Office.

e. If the review results in a non-concurrence, the CCPS must provide appropriate rationale and justification for the non-concurrence.

f. If an agreement between the CCPS and management cannot be reached, the issue must be presented to the DO for resolution.

1.4.3 When the DO cannot resolve the impasse and is not willing to acknowledge and accept the risk, or when the issue involves designated NCI, a request for waiver or exception of requirements must be processed in accordance with NASA Security Program Procedural Requirements, NPR 1600.1 w/Change 2, Chapter 1, Section1.3. The AA OPS is the only official that can authorize deviation and acceptance in this situation.

1.5 Terms, Abbreviations, and Acronyms

a. Terms, abbreviations, and acronyms used in this NPR are explained in Appendixes A and B

DISTRIBUTION:
NODIS

CHAPTER 2: Physical Security Vulnerability Risk Assessments

2.1 General

2.1.1 To provide the most practical physical protection for NASA assets, NASA managers must identify their NCI and analyze the risks to those assets from UDEs.

2.1.2 Assessment of these UDEs shall assist in determining the type and minimum level of physical protection needed to safeguard the identified NCI resources adequately and economically. The objectives of a physical security vulnerability risk analyses are the following:

a. Provide NASA managers a tool with which to design a security program based on local needs.

b. Working from a baseline designation of LOP I, allows the flexibility to adapt FSLs II through IV physical security measures to meet local risk conditions, provided FSL I or comparable security measures are in place and effective. In asset categories where physical security requirements have only been set at the higher FSLs, Center Protective Services Offices shall develop minimum physical security requirements that provide for the appropriate level of security commensurate with the postulated threat.

c. Obtain the maximum return possible from invested resources.

d. Serve as a basis for an asset-specific threat analysis.

2.2 Use of Physical Security Vulnerability Risk Assessments

2.2.1 The background and explanation of step-by-step procedures for conducting a physical security vulnerability risk assessment for categories of NASA assets and determining minimum security requirements are contained in NPR 1620.2, Physical Security Vulnerability Risk Assessments.

2.2.2. A physical security vulnerability risk assessment shall initially be conducted for assets that NASA Center Directors, and/or Project Offices/Project Managers have determined are part of the NCI established under Homeland Security Presidential Directive (HSPD) 7, “Critical Infrastructure Identification, Prioritization, and Protection” as outlined in NPR 1600.1, NASA Security Program Procedural Requirements, with Change 2, Chapter 8, paragraph 8.4 and Appendix H,.

2.2.3 The physical security vulnerability risk assessment can also be used to assist Centers in meeting the intent of PDD 67, “Enduring Constitutional Government and Continuity of Government Operations” and PDD 62, “Countering Terrorism.”

2.2.4 Subsequent physical security vulnerability risk assessments shall be conducted on all NASA asset categories in a timely manner in accordance with the following:

a. When an activity is activated.

b. When an organization permanently relocates to a new site or facility.

c. When no formal record exists of a prior risk assessment.

d. Every 3 years or more frequently at the discretion of the Center Director.

e. During the acquisition and planning stages of new facilities, additions to facilities, and facility renovations.

f. When an incident occurs in which an asset is compromised.

2.2.5 The physical security vulnerability risk assessment shall be conducted jointly by the Center Protective Services Office and designated representatives of the using organization.

2.3 Implementation of Physical Security Vulnerability Risk Assessments

2.3.1 Based on the physical security vulnerability risk assessment results, the organizational head, in coordination with the Center Protective Services Office, shall implement security measures described in the chapters found in this NPR.

2.3.2 Implemented physical security and terrorism counteraction measures shall be recorded in writing.

2.3.3 Copies of these records shall be maintained by the Center Protective Services Offices and the organization concerned.

CHAPTER 3: Physical Security Requirements for NASA Assets by Category

3.1 General

3.1.1 This chapter classifies common types of NASA property in readily understandable categories for quick reference.

3.1.2 Paragraphs 3.2 through 3.20 outline LOPs for specific categories of property by FSL established using the risk assessment procedure in NPR 1620.2, Physical Security Vulnerability Risk Assessment.

a. FSL I physical security measures are considered as baseline LOP.

b. Required physical security measures are designed to mitigate UDEs to an asset that could result in temporary or permanent loss of the asset.

3.1.4 Chapter 4 of this NPR outlines LOP for other specified non-critical categories of property.

3.1.5 Although the asset categories of NASA property described in Chapter 4 do not necessarily require the performance of a physical security vulnerability risk assessment, risk factors, property vulnerability, and appropriate protective measures shall be considered and employed where circumstances warrant.

3.1.6 Perimeter fencing at all NASA Centers shall meet standard minimum requirements established in Chapter 6, section 6.6 of this NPR.

3.1.6.1 Modifications to interior physical security fences shall not be made solely to conform to the requirements of this NPR if the CCPS determines the existing fence provides a comparable deterrent to penetration, and other compensatory measures, including electronic monitoring and sensing equipment are incorporated, where appropriate.

3.1.6.2 Perimeter fences not meeting the standard requirements established in Chapter 6, section 6.6 of this NPR, shall be properly prioritized for replacement by Center management based on the criticality of the asset, its level of vulnerability, and any reasonable and sustainable compensatory security measures that, when implemented, mitigate or reduce the vulnerability to manageable levels. Otherwise, the fence must be replaced at the earliest possible time, but not to exceed 24 months from time of determination.

3.1.7 For assets situated off NASA Centers, or in foreign countries, physical security measures outlined in Chapter 1, section 1.3 of this NPR shall apply, at a minimum.

3.1.8 Current national industry requirements, as established by the Illuminating Engineers Society (IES) Lighting Handbook, shall be consulted as a guide for minimum lighting levels. Lighting should be sufficient to illuminate potential areas of concealment, enhance the observation of security officer patrols, and provide for the safety of personnel coming between adjacent parking areas, streets, alleyways, and around the facility.

3.1.9 The CCPS shall ensure requirements for NASA PIV Smartcard/EPACS, intrusion detection systems (IDS), closed circuit television (CCTV), and other types of electronic physical security systems are coordinated with the OPS, Security Management Division, to ensure appropriate systems integration and Agency-wide system operations capability.

3.1.10 Conflicts between security and safety requirements must be identified and resolved in writing. Every effort shall be made to accomplish implementation of physical security requirements while ensuring safety issues are appropriately addressed. Waiver or exception requests must be processed jointly by the Center Protective Services Offices and Safety Offices in accordance with Chapter 1, paragraph 1.3, of NPR 1600.1 w/Change 2.

3.2 Categories of NASA Physical Assets

3.2.1 A NASA asset may not always correspond exactly to the categories listed in paragraphs 3.3 through 3.17. If the identified asset does not fall within one of the categories listed in table 2-1, NPR 1620.2, Physical Security Vulnerability Risk Assessment, or if it falls within more than one category, select the category which most closely describes the asset, and note the difference in the asset description. If none is appropriate, the organization head, in conjunction with the CCPS, shall develop and carry out those physical security measures deemed appropriate to safeguard the asset.

3.4 NASA Aircraft and Components Not at NASA Aviation Facilities

3.4.1 At a minimum, physical security protective measures for FSL II in subparagraph 3.3.1 above shall be implemented. In addition, the physical security procedures indicated below apply:

a. Aircraft shall be parked, whenever practical, at a Government airfield or civilian airport with an active physical security program. If a location has no security program and a crewmember cannot remain with the aircraft, the aircraft commander must advise aviation facility and local law enforcement authorities of the aircraft location, identification, length of stay, and ways to contact crewmembers.

b. The aircraft shall be checked at least once daily by a crewmember for any evidence of tampering, sabotage, placement of explosive devices, and loss or damage to aircraft or mission components.

c. When utilized for Ferry Flight operations, the Shuttle Carrier Aircraft shall be provided with physical security measures as identified in the KSC Security Handbook (KHB 1610.1) and DDMS FUNCPLAN 3610.

3.4.2 When appropriate, accessible and easily removable components shall be removed and stored in a location capable of being secured against theft, sabotage, or vandalism.

3.5 NASA Vehicles and/or Watercraft and Components

3.5.1 When not in use, vehicles shall be parked in motor pools to the maximum extent practicable.

3.5.2 The motor pool shall be protected by a standard physical security perimeter fence or adequately monitored to preclude theft or vandalism. Watercraft shall be secured to docking facilities.

3.5.3 All measures required for FSL I shall be implemented and minimum FSL II for this type of NASA asset.

Vehicles parked on the installation or watercraft docked at docking facilities shall be secured with a locking mechanism. Vehicles and watercraft will be secured as follows:

a. Commercially-designed vehicles. Activate manufacturer installed door and ignition locking device(s).

b. Non-commercial-design vehicles and watercraft. Immobilize steering wheel with a chain and a U.S. Government approved padlock as specified in local policies. Activate installed door and ignition-locking devices. Hood, spare tires, and fuel tank shall also be secured with approved locking devices if the local environment warrants this action. High-security padlocks supplied with vehicles may be used to secure vehicles as long as other physical security measures required by applicable directives are followed.

c. Material handling equipment. Material Handling Equipment (MHE) and other NASA vehicles that cannot be secured as indicated in (a) and (b) above shall have the steering mechanism immobilized or transmission lever locked in the neutral position. Alternatively, these vehicles may be stored in secure structures.

d. Signs. “Off Limits To Unauthorized Personnel” signs shall be posted at the activity entrances.

e. Where security officers or roving security patrols are available, motor pools and docking areas shall be checked for tampering, sabotage, loss, and damage not less than once every 4 hours.

f. Privately-owned vehicles shall not be permitted in motor pools except those of organizations and personnel engaged in deployments. These persons may store privately-owned vehicles in the motor pool at the discretion of the Center Director or his/her designee, provided physical security measures are taken to safeguard NASA vehicles and components remaining in the motor pool.

3.5.3 FSL III

a. All measures required for FSL I through II shall be implemented.

b. Vehicle parking areas, except those for empty trailers, and watercraft docking facilities, shall be lighted during the hours of darkness.

c. Vehicles shall be parked at least 20 feet from the perimeter of the parking area or as far from the perimeter as possible.

d. Entry to and exit from motor pools and docking facilities shall be limited and controlled. Control of entry and exit may be by security officers or locks on gates. Organization personnel working within the motor pool or on the dock may be considered an alternative to security officers.

e. Types of vehicles particularly vulnerable to theft, misappropriation, or damage in the motor pool, shall be segregated.

f. These vehicles shall be placed where organizational personnel can see them during operating hours and where roving security officer patrols can see them during non-operating hours.

g. Security Officers shall conduct physical security checks on the motor pool and/or docking facility on an irregular basis, but not less than once every 2 hours.

3.5.4 FSL IV

a. All measures required for FSL I through III shall be implemented.

b. Ground anchors shall be constructed for trailers, semi-trailers, and other towed equipment or a cable should be run through all items of such equipment and a lock mustl be affixed to one end.

c. Vehicles particularly vulnerable to theft, misappropriation, or damage shall be placed in secured garages and motor sheds to the maximum extent practicable.

d. The motor pool/docking facility shall be designated a “NASA Controlled Area” (formally known as “Restricted” area).

e. Personnel must have written authorization from organization heads or designee, before vehicles/watercraft can be dispatched.

f. Operators shall be checked for possession of a valid operator's permit by motor pool or dock personnel or security officers before they use the vehicle or watercraft.

g. Continuous surveillance shall be made of the motor pool/docking facility by armed security officers.

h. Continuously monitored CCTV and other detection equipment may be installed as an alternative to providing continuous surveillance by armed security officers.

3.5.5 Exceptions. Exceptions to this policy are as follows:

a. Vehicles/watercraft actively employed in field operations, or pending turn-in through property disposal channels.

b. Dispatched emergency, security police, courtesy patrol, and interior security officer vehicles/watercraft for brief periods when response time is critical for the successful performance of operator or crew duties. Ignition keys shall be removed from unaccompanied vehicles.

c. Trailers, semi-trailers, towed trailer systems, and other non-self-propelled vehicles.

d. Inoperable, unserviceable vehicles/watercraft. Procedures shall be implemented to protect vehicles/watercraft from cannibalization, vandalism, etc.

e. Vehicles/watercraft without installed locking mechanisms, under the continuous surveillance of a security officer or located in a secure location.

f. NASA vehicles outside the United States when so designated by the project manager.

g. Fuel tanker vehicles when, in the judgment of management personnel or the CCPS, locking would create a potential unacceptable hazard to life or property. In this case, compensatory security measures, established jointly by the CCPS and management, shall be taken.

h. Accessible and easily removable components. These components, vulnerable to theft because of value or utility, shall be removed and secured separately.

i. Additional physical security for components shall be provided by one of the following methods:

(1) Storing in a securable storage structure.

(2) Storing in a locked, totally enclosed truck or van.

(3) Storing in a locked equipment box or similar container secured to an open bed vehicle; for example, in a locked toolbox chained to the bed of a truck.

(4) Securing the item directly to the vehicle by a locally fabricated method.

i. Master-keyed locksets. Use of master-keyed locksets to secure NASA vehicles or motor pools is prohibited except under the following conditions:

(1) When the lockset is used within one vehicle to secure the vehicle and its' various storage compartments. Master-keyed locksets shall not be used to secure more than one vehicle.

(2) When the lock-set is used to secure the manifold access doors and hatches of petroleum, oil and lubricants (POL) trucks (one set per truck) and, if they have hardened steel shackles, for the storage compartments of wreckers, heavy equipment, etc. (one set per vehicle). The same set shall not be used on more than one vehicle. Master-keyed locks will not be used to secure vehicle steering wheels.

j. Keys and locks. Keys and locks shall be controlled according to Chapter 5, of this NPR.

k. Items used to defeat security measures. Items that can be used to defeat physical security measures, such as bolt cutters, hacksaws, oxyacetylene torches, axes, or steel rods or bars, shall be secured in respective tool kits or other secure locations when not in use.

3.6 NASA Vehicles, Watercraft, or Aircraft with On-Board Classified or Sensitive Equipment

3.6.1 NASA vehicles or aircraft with CNSI components or equipment at the CONFIDENTIAL or SECRET level mounted either internally or externally on the vehicle or aircraft; located on NASA installations or facilities, shall be secured with FSL IV physical protective and physical security procedural measures established in paragraph 3.3, above.

3.6.2 When located at other than NASA owned and operated facilities, NASA vehicles or aircraft with CNSI components or equipment at CONFIDENTIAL or SECRET level mounted internally or externally shall be secured with at least the minimum physical security measures.

3.6.3 These vehicles and aircraft shall be guarded at all times by an appropriately cleared and armed crewmember or dedicated armed security officer.

3.6.4 NASA vehicles or aircraft with CNSI components or equipment at the TOP SECRET level onboard shall be under constant surveillance by appropriately cleared and armed personnel regardless of location.

3.6.5 Equipment or components shall not be removed from vehicles or aircraft solely to fulfill a secure storage requirement. Frequent removal may cause increase of equipment damage or maintenance and may degrade operational readiness. However, classified equipment or components that can be readily dismounted without probable damage must be dismounted and placed in secure storage, meeting local requirements established by the CCPS.

3.6.6 In environments or unusual circumstances not clearly defined as requiring specific physical security measures under this NPR, the CCPS shall establish appropriate physical security measures to protect the classified equipment or components.

3.6.7 Non-cleared personnel, cleared personnel without a “need-to-know,” and FNs, shall not be given access to CNSI or sensitive information or equipment without proper coordination with the appropriate Center Security personnel.

3.7 Petroleum, Oils, Lubricants (POL) at Bulk Storage Facilities

3.7.1 All measures required for FSL I shall be implemented and minimum FSL II for this type of NASA asset.

a. When not under the surveillance of personnel authorized to dispense the products, POL pumps shall be locked and electrical power will be turned off. The electrical power shutoff must be secured.

b. Hoses to pumps shall be secured to prevent loss of POL through gravity feed. These measures are not required if pumps are activated by a credit card or key prompt type device.

c. Packaged POL shall be stored in structures capable of being secured against unauthorized entry.

d. Large POL packages (for example, 55-gallon drums) shall be stored to preclude their use as hiding places for pilfered items.

e. Written instructions to POL-dispensing personnel shall include procedures for determining if patrons entering the facility are authorized.

f. When unattended, the facility shall be checked at least once every 4 hours.

g. POL credit cards, identification plates, and aviation fuel plates shall be centrally controlled.

h. Privately-owned vehicles shall not be permitted in POL storage facilities.

i. All issues of fuel shall be accounted for and supervised by authorized personnel.

j. Hoses or other devices to siphon fuel shall be secured. All containers that can be used to carry fuel also shall be secured.

k. Containers storing used POL shall be marked and stored separately.

l. Keys to POL storage areas, equipment, and buildings shall be controlled per Chapter 5 of this NPR.

3.7.2 FSL III

a. Measures required for FSL I and II shall be implemented.

b. Storage facilities shall be bound by a standard perimeter physical security fence.

c. Gates and openings shall be closed and locked when not used.

d. “Off Limits to Unauthorized Personnel” signs shall be posted at the perimeter.

e. Facility attendants shall verify all POL quantities issued by personally reading the meter.

f. When unattended, the facility shall be checked at least once every 2 hours.

3.7.3 FSL III

a. Measures established for Risk I and II shall be implemented.

b. Shall be designated a “NASA Limited Area”.

c. Storage facilities shall be lighted during the hours of darkness.

d. Seals shall be placed on all points of fuel storage that may allow extraction of fuel by any means. A broken seal may indicate tampering.

e. Continuous surveillance shall be made of the facility by security officers.

f. IDS and/or CCTV may be installed as an alternative to continuous surveillance by security officers.

3.7.4 POL not at bulk storage facilities.

a. FSL I physical security protective measures and security procedures in subparagraph 3.7.1 above, shall be implemented. In addition, the following security procedures shall be implemented:

3.7.4.1. POL tank trucks that contain fuel and that are not under the surveillance of the operator or a dedicated security officer force shall have:

a. Locked hatch covers where possible.

b. Locked manifold access doors.

c. Each manifold valve shall be secured with a transportation seal if a manifold access door cannot be locked.

d. Approved padlocks as specified (e.g., non-sparking brass locks for safety), if available.

e. Fuel pods on vehicles and fuel vehicle tanks shall be secured with approved padlocks when the vehicles or tanks are carrying fuel and are not under the surveillance of the operator.

f. Fuel-carrying vehicles shall be parked in lighted areas of airfields or in motor pools protected by locked perimeter barriers or security officers.

g. Dome covers and manifold system shutoff valves of tanker rail cars with POL products aboard shall be locked when they are located on an installation for unloading and when POL handling personnel do not have the equipment under surveillance.

h. Rail cars with packaged POL products aboard shall be secured by locking all doors.

i. Packaged POL not onboard a vehicle or rail car shall be safeguarded in such a manner as to preclude theft or tampering. To increase the security posture above minimum the area may be protected by security lighting, perimeter fence, security officers, or IDS.

j. The need for implementing these additional measures shall be determined by local threat and vulnerability assessments.

3.11 Facility Engineering Supply and Construction Material Storage Areas

3.11.1 FSL I

a. Buildings storing supply and portable construction material shall be securable against unauthorized entry.

b. Outside storage areas shall be enclosed by a perimeter fence.

c. “Off-Limits to Unauthorized Personnel” signs shall be posted at facility entrances.

d. Access to the facility and to keys, padlocks, and protective seals protecting access shall be controlled in accordance with Appendix I, NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.

e. Supplies shall be issued only to authorized personnel.

f. Incoming shipments of supplies shall be checked for improvised explosives devices (IED's).

g. Work orders shall be reviewed to determine if the recipient has requested excessive supplies for the job to be done.

h. Entry of privately-owned vehicles into the storage building or outside storage areas shall be prohibited.

i. Entry of unchecked packages into the storage area shall be prohibited.

3.11.2 FSL II.

a. Measures required for FSL I shall be implemented.

b. Portable and easily pilferable items shall be separated from other supplies and construction material and stored in a separate room, building, or container with controlled access.

c. Outside storage areas shall be lit during the hours of darkness.

d. Small and easily pilferable supplies, construction material, and other items showing unexplained inventory loss shall be inventoried once each month. A copy of the inventory must be kept until the next inventory.

e. Bulk packaged items securely crated, banded, or sealed shall remain in their original configuration and not broken until they are issued.

3.11.1.3 FSL III or IV

a. Measures required for FSL I and II shall be implemented.

b. Buildings storing supplies and portable construction material shall be lit during the hours of darkness.

c. An IDS shall be installed in the storage building, if it is fully enclosed.

d. Landscaping features greater than 1 foot in height and other features that may obstruct views around the facility and provide concealment for aggressors shall be eliminated within 20 feet of the facility.

e. Access to storage areas shall be limited to facility personnel authorized to issue stock.

f. The storage building and outside storage areas shall be checked at least every 2 hours by a roving security officer patrols during hours that the facility is not operational.

3.12 Rocket Engine, Wind Tunnels, Simulators, and Other High-Speed Testing Facilities and Equipment

3.12.1 All measures required for FSL I shall be implemented and minimum FSL II for this type of NASA asset.

3.12.2 FSL II, III and IV

a. FSL II shall be designated a “NASA Controlled Area”.

b. FSL III shall be designated a “NASA Limited Area”

c. FSL IV shall be designated a “NASA Exclusion Area”

d. NASA PIV Smartcard/EPACS shall be used to identify and control access of authorized personnel at all times.

e. NASA PIV Smartcard/EPACS shall be used to identify and control access of authorized personnel at all times.

f. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible.

g. Existing facilities shall not be retrofit to meet these requirements when other compensatory measures could be implemented.

h. Outside testing facilities shall be surrounded by a physical security fence meeting the minimum requirements stated below:

(1) Unless otherwise specified, interior perimeter fencing shall meet standard minimum requirements as established in Chapter 6 of this NPR.

(2) Modifications to existing interior perimeter fences shall not be made solely to conform to the requirements of this regulation if the CCPS determines existing fencing provides a similar deterrent to penetration, and other compensatory measures, including electronic monitoring and sensing equipment are incorporated, where appropriate.

i. Access to the facility shall be controlled at all times via NASA PIV Smartcard/EPACS or armed security officers. An IDS/CCTV system must be installed/integrated to ensure

accountability during all hours of activity and to allow for real-time assessment and response of suspicious events.

j. Lighting of the exterior of the facility should be sufficient to illuminate potential areas of concealment, enhance the observation of security officer patrols and enhance CCTV capability.

k. All visitors (U.S. citizens and FN) shall be escorted if facility is designated NASA NCI, as established in Chapter 7, NASA Security Program Procedural Requirements, NPR 1600.1 W/change 2.

l. If the facility is not designated NASA NCI, escort of U.S. citizen and FN visitors shall be according to local policy.

m. Foreign national contractor employees shall be properly screened in accordance with NPD 1371.5A and NPR 1371.2B prior to accessing facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.13 Research and Associated Facilities

3.13.1 FSL I.

a. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible.

b. Existing facilities shall not be retrofit to meet these requirements, when other compensatory measures could be implemented.

c. Facilities shall be locked during non-duty hours to preclude unauthorized entry.

d. Lighting of the exterior of the facility should be sufficient to illuminate potential areas of concealment and enhance the observation of security officer patrol.

3.13.1.2 FSL II and III

a. All measures for FSL I shall be implemented.

b. The facility shall be designated a “NASA Controlled Area” (formerly known as “Restricted Area”) as a minimum designation.

c. NASA PIV Smartcard/EPACS shall be used to identify and control access of authorized personnel.

d. An IDS/CCTV system shall be installed/integrated to ensure accountability during all hours of activity and to allow for real-time assessment and response to suspicious events.

e. All visitors (U.S. citizens and FN) shall be escorted if facility is designed NASA NCI, in accordance with Chapter 7, NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.

f. If facility is not designated NASA NCI, escort of U.S. citizen visitors only shall be according to local policy.

g. Foreign national contractor employees shall be properly cleared in accordance with NPD 1371.5A and NPR 1371.2B, prior to accessing the facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.15 Spacecraft (Shuttle, ISS, Etc.) and Associated Equipment

3.15.1 All measures required for FSL I shall be implemented and minimum FSL II for this type of NASA asset.

3.15.1.2 FSL II and III

a. FSL II shall be designated a “NASA Controlled Area”.

b. FSL III shall be designated a “NASA Limited Area”.

c. Facilities housing these assets shall meet the physical security and anti-terrorism construction considerations identified in NPR 8820.2, to the maximum extent possible.

d. Existing facilities shall not be retrofit to meet these requirements, when appropriate alternative compensatory security measures could be implemented.

e. While on a launch pad, the asset shall be protected by a perimeter physical security fence capable of preventing unauthorized access. Area lighting shall be sufficient to illuminate potential areas of concealment, enhance the observation of security officer patrols, and provide for the safety of personnel moving about the site and between adjacent areas.

f. NASA PIV Smartcard/EPACS or armed personnel shall be used to identify and control access at all times.

g. An EPACS integrated IDS/CCTV system shall be installed to ensure accountability during all hours of activity, and to allow for real-time assessment and response to suspicious events.

h. While in transit to and from maintenance facilities and launch pads, the spacecraft shall be escorted by armed security officers at a minimum.

i. All visitors (U.S. citizens and FN) shall be escorted, if facility or asset is designated NASA NCI, as established in Chapter 7, NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.

j. If facility or asset is not designated NCI, escort of U.S. citizens and FN visitors shall be according to local policy.

k. Foreign national contractor employees shall be properly cleared in accordance with NPD 1371.5A and NPR 1371.2B prior to accessing facility. Escort requirements are per Chapter 4, paragraph 4.14, NPR 1600.1, NASA Security Program Procedural Requirements.

3.15.3 Terrorism counteraction measures specifically for NASA Spacecraft Launch Operations.

3.15.3.1 NASA Spacecraft, most notably the Shuttle Transport System (STS) and future spacecraft, are NASA's most recognizable physical assets and as such are a potential target of terrorist intent on attacking the prestige of the United States. Launch preparations shall, at a minimum, include the following:

a. Long and short-term analysis of intelligence information for indications of specific threats directed against the Launch Vehicle.

b. Development and implementation of written security operation plans for each launch.

c. Continuous evaluation of status of key personnel (astronauts, families, launch/mission control personnel, etc.), to ensure appropriate levels of protection are in place and effective.

3.15.3.2 On-site and in-transit protection and accountability for Shuttle program components (e.g., solid rocket boosters, external tanks, etc.) shall be coordinated with the appropriate contractor organization, to ensure the level of protection afforded is commensurate with the threat and vulnerability determination.

3.16 Industrial and Utility Facilities and Equipment

a. This category includes facilities that house diesel or back-up generators, uninterrupted power supplies, etc.

3.16.1 FSL I and II

a. Access into the area where the equipment is located shall be controlled to prevent unauthorized entry.

b. Keys to facilities and equipment shall be controlled per Chapter 5, Physical Security Requirements for NASA Facilities and Property, NPR 1620.3.

c. The area shall be designated a “NASA Controlled Area” (formerly known as “Restricted Area”) as a minimum designation.

3.16.2 FSL III

a. Measures for FSL I and II shall be applied and equipment must be checked by roving patrols, at intervals not to exceed every 4 hours when the facility is unattended.

b. Shall be designated a “NASA Limited Area”.

c. Measures for FSL I and II shall be applied, except that checks by roving patrols, must be every 2 hours when the facility is unattended.

d. If the equipment is not located within a structure, the area or vulnerable items of equipment shall be surrounded with an 8-foot-high reinforced concrete or masonry perimeter wall or surrounded by a physical security fence meeting the minimum requirements of Chapter 6, Section 6.6, of this NPR, and monitored by a centrally managed CCTV system.

e. If the equipment is located within a structure, the structure shall be equipped with centrally monitored IDS.

f. Utility systems shall be located at least 25 feet away from loading docks, entrances, and uncontrolled parking.

g. Standoff or hardening and venting methods shall be implemented to protect utilities.

3.17 Arms, Ammunition, and Explosives (AA&E)

3.17.1 At a minimum, AA&E, including pyrotechnics, shall be controlled/stored in accordance with the requirements in NPR NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2, Chapter 7, paragraphs 7.9.5 and 7.9.17, and 7.9.21 respectively. If deemed appropriate, Centers may adopt more stringent measures then those established in this NPR.

3.17.2 Organizations having access to and responsibility for AA&E, including pyrotechnics, shall establish strict accountability and inventory procedures.

3.17.3 Procedures shall include:

a. Issue and turn-in.

b. Monthly inventory.

c. Inspections.

d. Proper storage and use of “shelf stock.”

3.18 Mission-Critical and High-Risk Personnel

3.18.1 The NASA Assistant Administrator for Office of Protective Services, or his/her designee, in coordination with appropriate enterprise associate administrators, shall designate mission-critical and high-risk personnel.

3.18.2 All measures required for FSL I shall be implemented and minimum FSL II where mission-critical and high-risk personnel are located.

3.15.1.2 FSL II and III

a. FSL II shall be designated a “NASA Controlled Area”.

b. FSL III shall be designated a “NASA Limited Area”.

c. NASA PIV Smartcard/EPACS shall be used to identify and control access of authorized personnel.

d. An EPACS integrated IDS/CCTV system shall be installed to ensure accountability during all hours of activity, and to allow for real-time assessment and response to suspicious events.

e. Lighting of the exterior of the facility should be sufficient to illuminate potential areas of concealment and enhance the observation of security officer patrols.

3.18.3 FSL IV

a. FSL IV shall be designated a “NASA Exclusion Area”.

b. Access to the area surrounding the facility shall be controlled during times when the facility is occupied.

c. Specific threats shall be evaluated immediately by the CCPS and enhanced security provided, if determined appropriate.

d. Visitors to the facility who require entry into areas in which mission-critical or high-risk personnel are located shall be searched for prohibited items such as, weapons and explosives on at least a random basis.

e. Continuous surveillance of the area surrounding the facility shall be provided at all times, when the facility is occupied.

3.20 Administrative Support Facilities

3.20.1. Security procedural measures.

a. All measures required for FSL I shall be implemented and minimum FSL II for this type of NASA asset.

3.20.1.2 FSL II and III

a. Use of NASA PIV Smartcard/EPACS to facilitate entry of authorized personnel.

b. An EPACS integrated CCTV system shall be installed to ensure accountability during all hours of activity, and to allow for real-time assessment and response to suspicious events.

c. Where appropriate to the situation, implement terrorism counter-measures identified in Section 3.20.

3.21 Terrorism Counteraction Measures

3.21.1 Design-Basis Threat (DBT) analysis should be used when formulating terrorism counteraction measures as identified in NPR 1620.2, Physical Security Vulnerability Risk Assessment.

3.21.1.1 FSL I

a. Parking beneath facilities shall be eliminated where possible, and controlled where more practical to prevent unauthorized access and ensure only authorized personnel have access.

b. Parking exterior to the facility shall be kept as far away from the facility as possible, but at least 30 feet.

c. Trash receptacles, landscaping features, and other features greater than 1 foot in height that potentially provide concealment for aggressors or bombs shall be kept at least 50 feet from the facility and routinely examined by security patrols.

d. During periods of heightened security alerts and where feasible, containers and receptacles shall be removed.

e. Where feasible, locate mission-critical or high-risk personnel and/or assets in the interior of the facility as far from the perimeter of the facility as possible.

3.21.1.2 FSL II through IV

a. Forced entry resistant windows shall be utilized in areas occupied by mission-critical or high-risk personnel and/or assets.

b. Windows and doors into areas occupied by mission-critical or high-risk personnel and/or assets shall be locked and protected with IDS when the facility is unoccupied.

c. Duress alarms shall be installed in areas occupied by mission-critical and high-risk personnel and/or assets.

d. The facility shall be protected by a physical security fence meeting the minimum requirements of paragraph 3.1.6., at a setback distance from the facility of at least 50 feet.

e. Vehicle barriers (e.g., bollards, jersey barriers, etc.) shall be employed to provide adequate standoff distance.

CHAPTER 4: Minimum Physical Security Requirements for Other Categories of NASA Property Not Necessarily Subject to Risk Assessment

4.1 Miscellaneous Pilferable Assets (Includes Hand-Held Precision Tools, Laptop Computers)

4.1.1. Tool sets and kits with lockable toolboxes.
a. These items, when not in use, shall be secured with a U.S. Government approved key-operated tumbler-type lock, consisting of either a padlock (including brass padlocks issued with the tool boxes) or a factory installed built-in key-operated tumbler-type lock.
b. The individual who signed for the set or kit shall retain the key. A duplicate key may be held by the supervisor, if it is stored in a locked container with controlled access.
4.1.2 Portable hand tools (e.g., electronic tools, tool sets or kits, and shop equipment).
a. Portable hand tools, tool sets or kits, and shop equipment. These items, when not in use and not under the surveillance of a responsible person (user, tool room keeper), shall be stored in a secured location.
b. Non-portable items shall be secured in the building or van in which they are located.
c. Doors and windows shall be closed and locked. Secure locations for portable items include:
4.1.2.1 A locked building or room or a locked metal equipment cage in a secured building.
4.1.2.2 A locked built-in cabinet, bin, or drawer in a secure room or building.
4.1.2.3 A locked drawer or compartment of a furniture item (wall locker, desk, etc.) in a secured room or building.
4.1.2.4 Attached to the building structure with a 5/16-inch chain or equivalent cable and a low security padlock or permanently fastened to a working surface.
4.1.2.5 Locally fabricated, lockable racks that, when locked, prevent toolbox lids from being opened or individually placed larger tools from being removed.
4.1.2.6 A locked enclosed truck, van, or vehicle trunk.
4.1.3 Common tools and portable shop equipment (includes power tools).
a. These items, when not on hand receipt to a user, shall be controlled through a locally devised receipt, sign-in/sign-out log, or exchangeable tag system. Tool checks (metal disks that can be stamped or etched with an employee’s identification) are available through supply channels under national stock number (NSN) 9905-00-473-6336.
4.1.4 Access.
a. Access to tools and shop equipment shall be controlled to the maximum extent practical.
b. If possible, access shall be limited to the user, the individual designated as responsible for items when not in use, and supervisory personnel.
4.1.5 Keys and locks used to safeguard tools.
a. Keys, locks, and protective seals used to safeguard hand tools, tool sets or kits, shop equipment, and the facilities in which they are stored or located shall be managed per Chapter 5 of this NPR.
b. Master-keyed or keyed-alike lock-sets shall not be used to secure these items.
4.1.6 Special accountability.
a. Precision hand-tools that are made for a specific purpose, and are usually expensive to replace, shall be placed under special accountability.

b. Consideration shall be given to marking these items for identification and accountability.

4.2 Administrative and Housekeeping Supplies and Equipment

4.2.1 Minimum physical security requirements for furniture and office equipment.
a. Office buildings or rooms in which these items are located shall be secured when no responsible member permanently assigned to that particular activity is present.
4.2.2 Minimum physical security requirements for office machines.
4.2.2.1 Buildings, rooms, and offices in which office machines are located shall be secured, whenever an individual permanently assigned to the activity is not present.
4.2.2.2 Security shall consist of closing and locking appropriate doors and windows, as a minimum.
4.2.2.3 Automated systems, including word processing systems, shall be secured to preclude theft.
4.2.2.4 When size and weight allow, small office machines such as hand-held calculators and portable laptop computers (including U.S. Government issued technologies such as Blackberries, iPhones and iPads) shall be locked in a desk or cabinet.
4.2.3 Minimum physical security requirements for expendable and consumable supplies.
4.2.3.1 At the office levels, items not issued for actual use shall be centrally stored in secured cabinets, containers, rooms, or buildings.
4.2.3.2 Keys, locks, protective seals, and access to storage facilities shall be controlled.
4.2.3.3 Pilferable items (e.g., pens, pencils, etc.) shall be stored in a central supply closet or securable metal cabinet, and issued when needed.

4.3 Precious Metals/Materials

4.3.1 Physical Security Protective Measures.
a. Precious metals/materials shall be stored in secured containers within a locked room or a secured storage area.
b. Large quantities shall be provided with additional protective measures, such as IDS and CCTV.
4.3.2 Security procedural measures.
4.3.2.1 Users of precious metals/materials shall establish an accountability system, if not required under other regulations, to properly control the metal/materials.
4.3.2.2 The system shall include:
a. Inventory log.
b. Inspection process.
c. Issuance and turn-in process.
4.3.2.3 The Center Protective Services Offices, Logistics, and users of precious metals/materials shall jointly conduct inspections of stocks to ensure storage, protection, and usage procedures are properly followed.

4.4 Mailrooms

4.4.1 Minimum physical security requirements for mailrooms.
4.4.1.1 Facilities housing these assets shall meet physical security requirements necessary to preclude unauthorized access.

4.4.1.2 Existing facilities shall be retrofit to meet these requirements or other compensatory measures (e.g., access control system, IDS, etc.) implemented.
4.4.1.3 Installation of metal caging inside of a structure shall be considered for separation and control of mailroom areas.
4.4.2 Physical Security Measures.
4.4.2.1 Use of NASA PIV Smartcard, EPACS shall be implemented to identify and control access of authorized personnel to the mailroom.
4.4.2.2 Installation of IDS is recommended for after-hours protection.
4.4.2.3 The exterior of the facility shall be appropriately lit during the hours of darkness, to allow security officer patrols the opportunity to detect unauthorized personnel or activities.
4.4.2.4 The facility or room shall be designated a “NASA Controlled Area” (formerly “Restricted Area”), as a minimum designation.
4.4.2.5 In coordination with the CCPS, the mail handling activity shall develop a mail security plan, as required under 41 CFR Part 101-9, Part 102-192.85.
4.4.2.6 A photo-ID system shall be used to identify authorized personnel.
4.4.2.7 Visitors shall be escorted at all times.
4.4.2.8 Mailroom operations shall include the use of package screening devices for explosives and chemical/biological agent detection.
4.4.2.9 Any mail identified as suspect shall be reported immediately to security personnel.
4.4.2.10 Centers shall consider establishing a “centralized” shipping and receiving activity to preclude direct customer receipt of threatening or dangerous mail/packages.
4.4.2.11 Self-contained air-handling equipment shall be installed to ensure contaminated air is properly mitigated.
4.4.2.12 Procedures shall be in place for local evacuation of the mailroom facility, and if applicable, the shutdown of the air handling equipment for the mailroom.
4.4.2.13 Where appropriate, Center safety and security organizations shall collaborate on all facility and equipment design aspects of mailroom construction or modifications, to ensure designs meet safety and security operational expectations commensurate with existing threats.

4.5 Security of Medical Supplies and Equipment at Medical Facilities

4.5.1 Security Policy
4.5.1.1 Facilities, vaults, and containers used for storage of controlled medical substances or medically sensitive items shall not be used for storage of CNSI.
4.5.1.2 A Serious Incident Report shall be submitted per Chapter 7, NASA Security Program Procedural Requirements, NPR 1600.1. w/change 2, for significant theft, loss, or recovery of Government-owned or possessed narcotics, dangerous drugs, controlled substances, precious metals, radioactive or other sensitive materials, including sensitive medical material or equipment, or mismanagement of stock records or recovery procedures for those items that prevent a determination of loss.
4.5.1.3 Schedule I drugs and substances shall be secured in the same manner prescribed controlled substances.
4.5.2 Personnel who are assigned duties that require access to controlled medical substances and sensitive items storage areas, including volunteers or those who have custodianship or possession of keys and combinations to locks securing such areas,

shall be carefully selected and appropriately screened per Chapters 3 or 4, NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.
4.5.2.1 Criteria for selection of these personnel shall include moral character, prior employment history, maturity, and trustworthiness. Prior to assuming these duties:
a. Designated persons shall have undergone a personnel suitability investigation and favorably adjudicated at the Minimum Background Investigation (MBI) level.
b. Personnel exhibiting financial irresponsibility shall be excluded from consideration.
c. Non-Government workers (e.g., volunteer workers) shall not be given unsupervised access to controlled medical substances and sensitive items.
d. For new Government employees, a favorable adjudication of the required investigation shall be completed prior to granting them unescorted access.
e. An interview, by an appropriate Center Protective Services Office security official, with the lowest level manager having managerial responsibility for the security of subject items is required. The purpose of the interview is to appraise the individual's character, judgment, reliability, attitude, emotional or mental maturity, and sense of responsibility. The interview shall be documented in writing.
4.5.2.2 The names and duty positions of personnel authorized unaccompanied access to controlled medical substances and medically sensitive items storage areas shall be depicted on a roster
4.5.2.3. The roster shall be continuously reviewed and kept up-to-date and posted inside the storage area.
4.5.2.4 Access to controlled substances denied to individuals undergoing investigation, treatment, rehabilitation, judicial or administrative action as a result of actual or suspected drug use may be reinstated when--
a. Suspicions or allegations against the individual are determined to be unfounded.
b. Rehabilitation is successful.
4.5.3 Physical security during shipments of controlled medical substances and medically sensitive items shall be per appropriate NASA directives. In any event, in-transit security must be such that the requirements of this NPR are not violated and that controlled medical substances and medically sensitive items are protected from unauthorized possession, use, and theft.
4.5.4 Disposal of controlled medical substances and items shall be in accordance with provisions of the appropriate NPD and NPR.
4.5.5 Controlled medical substances or sensitive medical items shall be stored in secured storage locations or in locked containers.
4.5.5.1 Containers shall be locked at all times, except during restocking, inventory, or dispensing operations.
4.5.5.2 As a minimum, storage shall be in a location designated as a "NASA Controlled Area" (formerly "Restricted Area"), and
4.5.5.3 Potection provided shall be consistent with the type of item and perceived local threat of theft or diversion to unauthorized use.
4.5.6 At the close of business, designated personnel shall perform a security check prior to departure from rooms or facilities in which controlled medical substances and sensitive medical items are stored.
4.5.7 The security checks shall be documented daily on Standard Form 701, Activity Security Checklist, as a minimum. This form will ensure that:

4.5.6.1 No controlled items remain unprotected or exposed and that they are secured in designated containers.
4.5.6.2 Security containers are locked and checked properly with such action recorded on an SF 702 (Security Container Check Sheet).
4.5.6.3 All windows, doors, and other openings are secured to deter access to rooms in which containers are located.
4.5.6.4 Other vulnerable equipment or property is stored properly and secured.
4.5.6.5 When the medical facility is not occupied, security checks shall be conducted by security officer patrols at irregular intervals, not to exceed every 4 hours to avoid establishing a pattern. IDS may be installed to augment security officer patrol checks.
4.5.6.6 If used, the IDS shall consist of at least two types of intrusion sensors, a means of alarm annunciation at a central monitoring location, from which an armed response force can be dispatched, and electronically supervised circuitry between the two.
4.5.6.7 If the substances are entirely within a container, detection may include a capacitance sensor on the container itself.
4.5.6.8 If the substances are not entirely within a container, IDS and CCTV shall be utilized.
4.5.6.9 Installation of IDS and/or CCTV equipment shall be in compliance with applicable local specifications. When local conditions dictate, a duress switch or holdup button may be added. Design reviews apply.
4.5.6.10 An SOP for the activation, deactivation, and daily testing of the IDS shall be published by Center Protective Services Office.
4.5.6.11 The SOP shall include instructions for maintaining an accurate IDS log.
4.5.7 All instances of suspected theft, loss, illegal entry, open or unlocked facilities or containers, and other incidents of a suspicious origin shall be reported immediately to designated authorities.
4.5.8 Surveillance shall be maintained, until responding personnel arrive at the scene.
4.5.9 Storage areas shall be provided with operational interior and exterior lighting, at all times during the hours of darkness sufficient to illuminate and enhance security officer patrols and the monitoring of CCTV.
4.5.10 Medical Facility security coordinators shall establish procedures for the protection of locks, keys, and combinations used to secure facilities, vaults, and containers in which controlled medical substances and sensitive items are stored.
4.5.11 Access to keys and combinations shall be limited to the minimum necessary for efficient operations.
4.5.12 Provisions listed in Chapter 5 of this NPR shall be followed in establishing key control procedures.
4.5.13 Clinics and veterinary (animal care) facilities shall conform to the physical security requirements listed below.
4.5.13.1 When duty personnel are in attendance 24 hours a day, normal operating quantities of controlled medical substances and sensitive medical items shall be stored in double-locked containers. Containers must be constructed so that tampering and forced entry is readily apparent to visual examination.
4.5.13.2 When duty personnel are not present 24 hours a day, normal operating quantity of controlled medical substances and sensitive medical items shall be stored in a GSA-approved Class 5 safe

4.5.13.3 An additional barrier shall be provided, such as locating safes inside a locked room.
a. Normal operating quantities of controlled medical substances and sensitive medical items shall be stored according to the criteria in paragraph 4.5.12.1.
b. If this is not possible, containers constructed of a minimum of 26-gauge steel with a single lock may be used, provided additional security measures are taken (for example, increased surveillance or improved lighting), and provided the steel container is secured inside a locked room.
4.5.14 All storage containers for controlled medical substances and sensitive medical items shall be located in areas designated as a “NASA Controlled Area” (formerly “Restricted”) per Chapter 7, NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.
4.5.15 Containers shall be secured after duty hours.
4.5.16 To prevent loss or theft during operating hours, containers shall be unlocked only when property is being inserted, removed, or when the container is under the constant observation of designated personnel.
4.5.17 Unit dose carts containing controlled substances shall be kept in the “NASA Controlled Area” when not in use.
4.5.18 To prevent loss or theft during the administration of medications, unit dose carts shall be kept under the physical control or unobstructed observation of designated personnel.
4.5.19 Storage areas shall be sufficiently illuminated with operational interior and exterior lighting at all times during the hours of darkness.
4.5.20 The number of crash carts and emergency trays (essential emergency assemblages) that contain controlled substances shall be kept to a minimum, and must be provided with maximum security consistent with requirements for immediate availability.
4.5.21 Controlled medical substances or items issued to emergency medical team personnel assigned to ambulance or emergency vehicle response duties shall not be left in the vehicle unattended.
4.5.22 Controlled substances and items must remain under constant control or observation of responsible medical personnel at all times and shall be stored in a “NASA Controlled Area” when not in use..
4.5.23 Locking devices on emergency assemblages that hinder immediate availability to controlled medical substances and sensitive items by medical treatment personnel shall not be used.
4.5.24 Appropriate sealing devices may be used to indicate tampering and to assist in inventory, but they must be easily opened without the use of a key, combination, or other time-delaying device.
4.5.25 Emergency assemblages containing controlled medical substances shall be sufficiently protected, but must not hamper ready and authorized visual inspection and immediate removal for use by authorized medical personnel.
4.5.26 Accountability and control requirements are per applicable organization policy.
4.5.27 Unused needles, syringes, and other medically sensitive items shall be stored in a locked container.

4.5.28 Used and unused needles and syringes shall not be stored in the same cabinet or container.
4.5.29 Pending final destruction, used needles and syringes may be temporarily stored in closed one-way puncture resistant receptacles (“Sharps” containers).
4.5.30 “Sharps” containers must be of a tamper-resistant design, and must be either:
4.5.30.1 Locked to a mounting device that is securely fastened to the building structure.
4.5.30.2 Located in a room or area that is locked or under continuous visual surveillance of ward or clinic personnel.

4.6 NASA Visitor Centers and Outdoor Exhibit Displays

4.6.1 NASA Visitor Centers traditionally house one-of-a-kind, irreplaceable items of historical significance. Such items are generally considered invaluable because they are irreplaceable and shall be considered sensitive property.
4.6.1.2 They shall be protected in accordance with the following.
4.6.1.3 The degree of protection necessary must be determined locally and in partnership between the NASA COTR, Visitor Center Manager, CCPS, and supporting facility engineers.
4.6.1.4 Visitor Center buildings and apertures providing access to the building shall be modified or constructed so as to provide resistance/deterrence of unlawful entry and delay an intruder(s) long enough for a security force response.
4.6.2 Security measures shall be implemented for those facilities and assets protected under the National Preservation Act of 1966 to the extent permitted.
4.6.2.1 Consistent with this Act, IDS and CCTV coverage shall be included for all perimeter entry/exits, windows and doors.
4.6.3 Personnel assigned or attached (including special duty personnel) to staff NASA Visitor Centers must have favorably adjudicated personnel suitability investigation (minimum NACI) established in NASA Security Program Procedural Requirements, NPR 1600.1 w/change 2.
4.6.3.1 At a minimum, a favorable National Agency Check w/ Inquiries (NACI) shall be completed by the Center Protective Services Office before personnel are assigned or attached (including special duty personnel) to Visitor Center duties.
4.6.4 The Visitor Center director, or designee, shall be designated the key custodian, whenever feasible.
4.6.5 Exterior doors used for access to Visitor Centers shall be secured with U.S. Government-approved padlocks (grade II, hardened steel shackle and body), deadbolt or other locks equal to these devices, as determined by the servicing facility engineer, if installation does not detract from the aesthetic value of the facility.
4.6.6 The number of exterior doors with exterior exposed padlocks shall be kept to the absolute minimum. All other exterior doors shall be secured on the inside.
4.6.7 Visitor center keys shall be maintained separately from high-value item storage IDS keys.
4.6.7.1 Keys shall never be left unattended or unsecured.
4.6.7.2 The use of a master or multiple key systems shall be in accordance with Chapter 5 of this NPR.
4.6.8 Where a NASA Visitor Center or exhibit is protected by approved IDS, and the IDS is operational, museum personnel, as authorized by the Visitor Center manager, may

remove the keys to the Visitor Center or exhibit from the installation at which the Visitor Center or exhibit is located.
4.6.9 Unless authorized by the CCPS, where an approved IDS is not installed, the Visitor Center keys shall not be removed from the installation, but shall be locked in a secure strongbox in a secured location on Center, such as the Protective Security Office dispatch office. Visitor Center personnel, as authorized by the Visitor Center Manager, may retain custody of the keys in this strongbox.
4.6.10 Duplicate keys shall not be kept with operational keys. They shall be maintained by the Visitor Center manager, Center locksmith, or placed in a secure location where they may be accessed by authorized personnel only.
4.6.11 Where combination locking devices are used to secure items such as containers and display cases, the combination shall be controlled and safeguarded to preclude unauthorized access.
4.6.12 Interior and exterior lighting shall be provided in all Visitor Center buildings in which sensitive property is located.
4.6.13 Lighting around artifacts shall have proper UV filtering for artifact conservation. Sensitive property is property requiring a high degree of protection and control because of its vulnerability to theft or potential for use in an illegal activity, or for its historic value. As a minimum, all entrances shall be sufficiently illuminated during hours of darkness.
4.6.14 Installation of IDS may supplement existing security measures or provide a commensurate degree of protection. Established Center requirements for IDS and access control systems shall apply.
4.6.15 The viewing surfaces of exhibit or display cases shall be constructed of at least 1/4 inch-thick plate glass, transparent acrylic plastic, or transparent poly-carbonate plastic, securely fastened into frames or into the container.
4.6.16 UV acrylic shall be used to facilitate artifact conservation.
4.6.16.1 Where plate surfaces join at an angle, the edges shall be bonded and rounded to prevent insertion of a pry tool. UV acrylic shall be used to facilitate artifact conservation.
4.6.16.2 Cases with hinged openings must have all hinge butts concealed or spot welded, or use a comparable security measure.
4.6.16.3 Non-viewing surfaces of cases shall be constructed to offer a higher degree of protection than the viewing surface.
4.6.17 Workshops used by museum personnel for maintenance or restoration work shall be secured at the close of each business day.
4.6.18 Each Visitor Center shall be attended by at least one member of the Visitor Center staff, who is tasked with Visitor Center security while it is open to the public. This function can be combined with other duties.
4.6.18.1 Visitor Centers that are organized within several separate, non-connecting buildings shall have Visitor Center or security personnel in each facility, an electronic monitoring system, or security personnel must conduct periodic checks of facilities and displays.
4.6.18.2 The Visitor Center attendant shall be especially alert to detect pilferage, damage, or theft.
4.6.19 To ensure adequate surveillance of all parts of the Visitor Center, the installation of one-way mirrors and electronic sensing devices shall be considered and installed.

4.6.20 NASA CCPS shall ensure that all Visitor Centers are on an assigned security officer patrol route, and that special orders include an unscheduled check at least once every 4 hours by a security officer patrol during non-duty hours on a daily basis.
4.6.21 Large items of historical property that are displayed outdoors in Visitor Center parks shall be anchored to prevent theft.
4.6.21.1 Pilferable component parts shall be secured to the display or removed at the close of each business day.
4.6.21.2 Visitor Center parks and exterior displays shall be provided electronic and/or CCTV surveillance where warranted, and checked periodically by security officer patrols.
4.6.22 Loss of historical property shall be reported to the Center Protective Services Office for appropriate investigation.

4.7 TV, VCR, DVD, Cameras, Bicycles, and Other Sensitive Items

a. Center management shall ensure items of value, as defined in NPR 4200.1G, Equipment Management Procedural Requirements, are provided protection commensurate with local theft conditions and accountability practices.

CHAPTER 5: Keys, Locks, Locking Devices (Including Hasps and Chains), and Protective Seals

5.1 Key Issuance

a. Keys shall be signed out to authorized personnel only, as needed, on a key issue form.

b. Only authorized Government personnel, branch head or higher, and their designees, may approve the issuance of keys to organizational personnel for facilities under their control.

c. Keys for contractor personnel shall also be issued in accordance with paragraph b. above.

d. Office keys shall be issued to occupants of that office only.

5.2 Master Keys

a. Issuance of building master keys shall be kept to the absolute minimum.

b. No more than the minimum number of building master keys shall be issued, and then only to key personnel in that facility.

c. Center master keys shall be issued only to security, fire, and when appropriate, other authorized personnel.

5.3 Key Depository

a. A lockable container, such as a safe, filing cabinet, or a key depository made of at least 26-gauge steel, equipped with a tumbler-type or touch-pad locking device and permanently affixed to a wall, shall be used to secure keys.

b. The key depository shall be located in a room where it is kept under 24-hour surveillance or in a room that is locked when unoccupied.

c. The locksmith shop key and records storage area shall be protected by IDS.

5.4 Locks

a. The use of a master key system or a multiple key system shall be strictly managed by the installation locksmith.

b. Management of NASA-owned buildings shall not procure coring and keying services of outside companies.

c. U.S. Government key-operated, pin-locking deadbolts or deadbolts that project at least 1 inch into the door frame or tumbler-type padlocks shall be used to safeguard unclassified and non-sensitive NASA supplies and equipment, if a lock is required.

(1) Selection shall be based on the value of items protected, mission essentiality, and vulnerability to threats.

(2) All questions regarding approved locks and locking devices shall be addressed to the individual Center Protective Services Office and locksmith.

d. Padlocks and keys not in use shall be secured in a locked container that does not contain or store CNSI, or in a locked room. .

e. Use of NASA PIV Smartcard/EPACS shall be used to identify and control access of authorized personnel at all times.

5.5 Key and Lock Accountability

a. Keys and combinations to locks shall be accounted for at all times.

b. Individually-issued keys to offices shall not be duplicated nor loaned out.

c. High security padlocks and their keys shall be inventoried by serial number semiannually.

d. A written record of the inventory shall be retained until the next inventory is conducted.

e. When a key to a high security padlock is lost or missing, an inquiry shall be conducted and the padlock replaced or re-cored immediately, if the situation warrants replacement.

f. A key and lock inventory shall be maintained, which includes a list of all of the following:

(1) Keys.

(2) Locks.

(3) Key serial numbers.

(4) Lock serial numbers.

(5) Location of locks.

(6) The number of keys maintained for each lock. This list shall be maintained and secured in the locksmith shop.

e. In coordination with the locksmith, facility service managers (FSM) shall conduct yearly inventories of keys for their facility and provide a copy of the inventory results to the locksmith. Discrepancies will be rectified with the locksmith.

f. Rekeying and recoring of individual facilities shall be conducted when:

(1) Control and accountability of keys has been compromised.

(2) Requests for replacement of lost keys are equal to or greater than 25% of total issued keys for that facility or door in the facility. The organization responsible for the facility shall fund the rekey/recore activity.

(3) The facility is vacated and issued keys have not been recovered. The new occupant shall fund the rekey and recore activity.

g. High-security padlocks and keys that do not have a serial number shall be assigned one. This number must be inscribed on the lock or key.

5.6 Additional Key and Lock Controls for Key Containers

a. Keys to key containers shall not be removed from the installation except to provide for protected storage elsewhere.

(1) Keys to locks securing key containers shall be afforded physical protection equivalent to that provided by the key container itself.

(2) Keys to containers shall be maintained separately from other keys,

(3) Keys to containers shall be accessible only to those individuals whose official duties require access to them.

b. At no time shall keys be in the custody of a person not authorized to have them.

c. Under no circumstances shall keys and locks or alternate keys or locks be placed in any security container that contains or stores CNSI.

(1) When arms and ammunition are stored in the same areas, keys to those storage areas shall be maintained together, but separately from other keys that do not pertain to AA&E storage.

(2) The number of keys shall be held to the minimum essential.

(3) Keys shall not be left unattended or unsecured at any time.

(4) Keys required for maintenance and repair of IDS, including keys to the control unit door and monitor cabinet, shall be kept separate from other IDS keys.

(5) Access shall be permitted only to authorized maintenance personnel.

(6) IDS keys shall be stored in containers of at least 20-gauge steel equipped with GSA-approved low security padlocks or GSA-approved built-in three-position changeable combination locks, or in GSA-approved Class 5 or Class 6 containers that do not contain or store CNSI.

(7) Combinations shall be recorded on SF 700 (Security Container Information), sealed in the envelope provided, and stored in a separate container.

(8) Security containers weighing less than 500 pounds shall be fastened to the structure with bolts or chains equipped with secondary padlocks to preclude easy removal.

d. In the event of lost, misplaced, or stolen keys, an administrative investigation shall be conducted immediately.

(1) The affected locks or cores to locks shall be replaced when practicable.

(2) Replacement or reserve locks, cores, and keys shall be secured to preclude access by unauthorized individuals.

e. Replacement of lock cylinders and broken keys for high-security locks shall be coordinated with the local Office of Protective Services locksmith

5.7 Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas

a. Combination to locks on GSA-approved Class 5 or Class 6 security containers used for storage of CNSI or vaults such as a Sensitive Compartmented Information Facilities (SCIF) certified and accredited to store CNSI shall be changed when the container (or lock) is first put into service.

b. Combinations shall be changed when there is a change of any person having knowledge of the combination, or when there is compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked or unattended.

c. Combinations shall be changed upon the termination of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.

d. Combination shall be changed at other times when deemed necessary by the CCPS.

(1) The combination shall be recorded using SF 700, sealed in the envelope provided, marked with the highest classification of material authorized for storage in the container, and safeguarded in accordance with the highest classification of the material stored in the container or SCIF.

(2) No other written record of the combination shall be kept unless it is appropriately marked and handled in accordance with the highest classification of the material authorized for storage in the container or SCIF.

(3) Controls shall be established to ensure that the envelopes containing combinations to locks are not made available to unauthorized personnel.

e. Replacement of lock cylinders and broken keys for high-security locks shall be coordinated with the local security office locksmith.

5.7 Additional Key and Lock Requirements

a. Aircraft and vehicle storage facilities in which vehicles or aircraft are permanently based with sensitive items onboard shall be outfitted with security doors and frames (i.e., steel frames, metal-clad solid core doors), and secured with approved secondary high-security hasps and padlocks. Existing hangar doors are considered sufficient if properly employed at the end of each workday.

5.8 Chains

a. When a chain is required for security of CUI or equipment and supplies, specifications for approved chains shall be obtained from the local Center Protective Services Office.

5.9 Use and Control of Protective Seals

a. Purpose of the seal. The purpose of the seal is to show whether the integrity of a storage facility, vehicle, rail shipment, or container has been tampered with or compromised.

b. A plain seal is not a lock, although combination items referred to as “seal-locks” are available.

c. The purpose of a seal, no matter how well constructed, is defeated if strict accountability and disciplined application are not maintained.

d. Ordering and storing seals. Seal construction specification shall include--

(1) Durability. Seals must be strong enough to prevent accidental breakage during normal use.

(2) Design. Seals must be sufficiently complex to make unauthorized manufacture of a replacement seal difficult.

(3) Tamperproof. Seals must readily provide visible evidence of tampering and be constructed in a way that makes simulated locking difficult once the seal has been broken.

(4) Individually identifiable. Seals must have embossed serial numbers and owner identification.

(5) Ordering and issuing. A single office on an installation shall be responsible for ordering and issuing seals. The source for the seals will be instructed to ship the seals to the attention of a seal custodian in that office.

(6) Unused seals. Seals not issued for actual use shall always be secured in a locked, metal container with controlled access. Only seal custodians and alternates will have access. Recorded monthly inventories will be conducted to preclude undetected loss of seals.

e. Accounting for seals. Seal custodians shall maintain an IT-based seal logbook.

(1) The issuance process of seals to a using office, unit, or activity custodian shall reflect date of issue, name of recipient, and seal serial numbers.

(2) The issuance process of a seal for actual use by a custodian shall reflect the seal number, date and time applied, identification of items to which applied (and location on item if other than main door(s)), and the name of the person applying the seal.

(3) For outbound loaded trailers, railcars, and container shipments, the appropriate trailer, railcar, or container number and load destination shall be noted.

f. Application of seals.

(1) Seal all doors and openings, not merely the main one.

(2) Run seal straps through hasp only once. Seals wrapped around several times become illegible.

(3) Listen for “click” when inserting point of seal into sheath.

(4) To ensure positive closure, tug down on strap, and twist the point section inserted into the locking mechanism.

g. Checking seals. Centers using seals shall develop procedures for checking them.

(1) These procedures shall include actions to be taken to break a seal, and actions to be taken upon finding a broken seal.

5.10 Disposition of Used Seals

a. All shipping documents shall reflect seal number(s).

b. All seals shall be verified with seal log, shipping documents, or other appropriate documents before removal and disposal.

c. Seals must be defaced sufficiently upon removal, so that they cannot be used to simulate a good seal. They shall be disposed of in normal trash.

d. If the user seal log is located on the same installation, the custodian shall be advised of the destruction of the seal, or the seal will be returned to the custodian.

e. The custodian shall annotate the date and time removed, and the name of the individual removing the seal across from the original entry on the seal log.

5.11 Changing Seals

a. If used, the colors of seals shall be changed periodically, as an additional physical security measure.

CHAPTER 6: Center Perimeter Physical Security and Barrier Requirements

6.1 Purpose

6.1.1 To establish standardized NASA minimum perimeter physical security requirements for Centers.
6.1.2 To establish minimum LOP criteria for physical security barriers and openings at NASA Centers.
6.1.3 Additionally, facilities and operations, when established under the provisions of the NCI, must meet specific criteria established in Chapter 6 of this NPR.
6.1.4 Physical barrier requirements are designed to deny, impede, or discourage access to NASA areas by unauthorized vehicles, personnel or groups. This is accomplished by one or more of the following:
6.1.4.1 Defining the perimeter of the installation and any security areas.
6.1.4.2 Creating a physical and psychological deterrent to entry, as well as making a legal statement that entry is not permitted.
6.1.4.3 Delaying intrusion into security areas, thus making more likely the detection and apprehension of intruders by protective forces.
6.1.4.4 Facilitating the effective and economical utilization of armed security officers.
6.1.4.5 Directing the flow of personnel and vehicles through designated portals, in a manner that permits efficient operation of a personnel identification and control system.

6.2 NASA Standard Perimeter Physical Security Requirements

6.2.1 Employ fencing as described in Section 6.7 around the Center site perimeter. The Center site perimeter is defined as the physical land area controlled by the Government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a NASA federal facility is placed. The Center perimeter is further defined as the outermost boundary of the Center.
6.2.2 Identify, with signage attached to fencing as described in Section 6.14.
6.2.3 Establish unobstructed or clear zones of 10 feet on either side of the fencing to allow for service and security patrol vehicle access.
6.2.4 Establish and document random security officer patrols of the perimeter fence at least 2 times every 8 hours. See section 6.13.
6.2.5 The CCPS shall establish annual perimeter fence line survey that includes a security posture study.
a. The security posture study shall include crime statistics for the Center and the surrounding area.
6.2.6 Limit vehicle and pedestrian access points to the minimum number required.
6.2.7 Perimeter Security Officer Posts.
a. Establish security officer posts at vehicle and pedestrian access points.
b. Security officers shall be appropriately equipped with handheld radios.
c. Flashlights and other appropriate equipment deemed necessary by the CCPS shall be provided.
d. Security officer posts shall have either duress call buttons or direct landline capability to the security operations office.
e. Posts shall have landline capability to dial on and off Center for the purpose of conducting official duties.

f. In the interest of security officer safety, when exterior posts are manned, CCTV shall be monitored by security operations office and recorded.
g. During Center business hours, those access points shall be manned with a minimum of 2 security officers. During Center non-business hours, one security officer is authorized when the access point and security officer is under constant CCTV observation by the security operations office.
6.2.8 Pedestrian (foot) traffic.
a. Pedestrians shall be required to present to a security officer NASA PIV Smartcard or other Center specific identification badge for visual inspection prior to entry.
b. During heightened security alerts, random searches of personal belongings may be implemented by the CCPS.
6.2.9 Vehicle traffic.
a. Prior to granting entry of a vehicle, all occupants must present to a security officer NASA PIV Smartcard or other Center specific identification badge for visual inspection.
b. Cursory visual inspections of vehicles (exterior and interior) shall be performed by security officers prior to entry.
c. Security officers shall be on the lookout for prohibited items and or any suspicious activity on or within the vehicle.
d. Establish a random vehicle inspection (RVI) program. The program shall include a designated vehicle inspection area that does not interfere with vehicular traffic or pedestrian flow on and off Center to ensure the safety of security officers as well as employees and the general public. Preferably and where design allows, the vehicle inspection area should be established before entering a NASA Center and away from any buildings or employees.
e. The vehicle inspections shall be conducted by trained security officer screening or by use of K-9.
f. During heighted security alerts, CCPS may implement more rigorous vehicle inspections, not of a random nature.

6.3 Types of Barriers

6.3.1 Protective barriers are divided into two major categories: natural and structural.
6.3.1.1 Structural barriers are manmade devices such as fences, walls, floors, roofs, grilles, bars, roadblocks, bollards, trenches, berms, static barriers, sculptures, and street furniture or other structures that deter penetration.
6.3.1.2 Natural barriers may be plantings, trees, boulders, ponds and water basins, rivers, swamps, beaches, or other terrain difficult to traverse.

6.4 General Considerations

6.4.1 Established physical security barriers at NASA Centers are not designed to stop a determined intruder, but rather to deter or delay.
6.4.2 Depending on the FSL, barriers should be augmented by security personnel and IT-based surveillance and monitoring systems, when warranted.
6.4.3 When planning or establishing security barriers at NASA Centers, the CCPS shall consider the following, prior to recommending security barriers:
6.4.3.1 Physical barriers that are as personnel-proof as economically feasible should be established around all security areas. The type of barrier used should be determined after a posture study of local conditions has been made by the CCPS and facilities engineering professionals with security engineering backgrounds.

6.4.3.2 In some instances, the temporary nature of the security interest makes the construction of costly permanent physical barriers impracticable and unjustifiable. In such cases, the security interest must be protected by other means, such as use of temporary barriers, additional protective forces, patrols, and other risk mitigating protective measures.
6.4.3.3 In cases of extreme criticality and vulnerability of NASA facilities, it may be necessary to establish two lines of physical barriers at the security area to be protected.
6.4.3.4 The site perimeter of a NASA Center and any specific designated security area shall be fenced.
6.4.3.5 As a minimum, “U.S. Government-No Trespassing” signs with appropriate prosecution warnings shall be attached not more than 100 feet apart along, and at each corner of, the boundaries of the land. This defines the perimeter, provides a buffer zone, facilitates control, and makes accidental intrusion unlikely.
6.4.3.6 In establishing any perimeter barrier at a NASA Center, due consideration must be given to providing emergency entrances and exits in case of fire.
6.4.3.7 The size of an individual internal security area shall depend on the degree of sensitivity required and the complexity of the area. As a rule, size should be kept to a minimum consistent with operational efficiency.
6.4.3.8 Positive barriers at NASA Centers shall be established for:
a. Controlling vehicular traffic flow. Center circulation design should prevent high-speed approaches by vehicles, and use barriers or offset vehicle entrances from the direction of a vehicles approach to force a reduction in speed.
(1) Conducting random vehicle checks.
(2) Maximum clear spacing between vehicle barriers is 4 feet on center. Minimum barrier height is 30 inches.
(3) Vehicle barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, or SD-STD-02.01, Revision A, Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates.
b. Controlling pedestrian access. The level of protection afforded by the barriers should be commensurate with the need to limit pedestrian access. Lower levels of protection intended to guide pedestrians, can be achieved using shrubbery, decorative fencing, or knee walls. Higher levels of protection, intended to prevent determined intruders, are achieved using other methods, such as anti-climb fencing.
(1). Checking identification of personnel entering or departing.
c. Defining a buffer zone for critical, classified or sensitive areas, such as designated NASA Limited or NASA Exclusion Areas.
6.4.4 Center geographical and environmental characteristics, specifically water and marshland boundaries, present special security problems. Such areas at any Center should be defined by appropriate fencing and signs.
6.4.5 Construction of new security barriers and removal of existing barriers and related work must be approved by Center Protective Services Office, and scheduled to provide a continuous level of security for the activity/program.

6.5 Temporary Barriers

6.5.1 In some instances, the temporary nature or infrequent existence of a sensitive program/project requiring security constraints does not justify the construction of more permanent physical perimeter barriers.

6.5.2 In such cases, a Center-designated “NASA Limited Area” or “NASA Exclusion Area” (formerly “Closed area”) of temporary nature and short duration may be established, in which the reduction of security resulting from deficiencies in physical barriers is mitigated for by additional security forces, patrols, and other security measures, during the period of restriction.

6.5.3 Barricade requirements include jersey barriers, blast resistant concrete wall construction, and security fencing.

6.5.4 In any case, a designated temporary security area shall not exceed 30 days from date of installment without specific authorization from the CCPS.

6.5.5 The use of wire barriers or similar construction for temporary enclosures is recommended as being both expeditious and effective, with a minimum use of security forces required to control and safeguard the area.

6.6 Security Fences

6.6.1 Security fences at NASA Centers should enclose the perimeter and all designated security areas, and shall be constructed in such a manner that they are reasonably impassable.

6.6.2 The nature of the security area shall determine the degree of restriction of movement of personnel, vehicles, and equipment necessary for adequate security.

6.6.3 The CCPS must approve all security fence requirements and, prior to approval, shall assess the permanency of the security area, availability of materials, presence of natural aids to security, Center security personnel, security vulnerabilities and UDEs, and the degree of security required.

6.7 Security Fence Standards

6.7.1 Security fences will not stop a determined intruder. To be effective, such barriers must be augmented by security force personnel and other means of protection, detection, delay and assessment. Security fences are used primarily to:

a. Define the perimeter of a NASA Center

b. Provide a physical and psychological deterrent to entry while serving notice that entry is not freely permitted.

c. Prevent accidental entry

d. Optimize security force operations

e. Enhance detection and apprehension of intruders

f. Channel and control the flow of personnel and vehicles through designated portals.

6.7.2 Chain-link fencing shall be the type of structural barrier most commonly used and recommended for security purposes at NASA Centers, and should enclose the perimeter of a NASA Center and all designated security areas.

6.7.3 The following fence standards shall apply.

6.7.3.1 Fabric. The standard fence fabric shall be at least 9-gauge zinc- or aluminum-coated steel-wire-chain link with mesh openings not larger than 2 inches per side and a twisted and barbed selvage at top and bottom.
6.7.3.2 Fabric ties. Only 9-gauge-steel ties with coating compatible with the fabric shall be used. In lieu of wire ties on fence posts, approved fabric clamps can be used. In lieu of wire ties on bottom and top taut wires, hog clamps may be used. Spacing between ties should not exceed 12 inches.
6.7.3.3 Height. The preferred height of any NASA security fence is 9 feet. This includes, at a minimum, a fabric height of 8 feet, plus a 1-foot barbed-wire top-guard. Concertina (Razor) wire may be used in lieu of the barbed-wire top-guard to provide added protection against intrusion for areas of high sensitivity. Building connections shall be higher. Fencing 12 feet high from the connection point of the building to the distance of 12 feet from the building is recommended, unless the building wall itself is less in height.
6.7.3.4 Fencing posts, supports, and hardware. All posts, supports, and hardware for security fencing shall meet the requirements of Federal Specification RR-F-191K May 29, 2001, unless superseded by later issuance.
6.7.3.5 All fastening and hinge hardware shall be secured in place by penning or spot welding to allow proper operation of components, but prevent disassembly of fencing or removal of gates.
6.7.3.6 All posts and structural supports shall be located on the inner side of the fencing.
6.7.3.7 Posts shall be positively secured into the soil to prevent shifting, sagging, or collapse. Fence posts should be placed no more than 10 feet apart and mounted in concrete 36 inches deep. The diameter of the concrete must not be less than 10 inches for line posts, and not less than 12 inches for corner and gate posts.
6.7.3.8 Reinforcement. Taut reinforcing wires (at least 9 gauges) shall be woven through, or affixed with, the fabric along the top and bottom of the fence for stabilization of the fence fabric. Top and center rails should not be used, as they may provide added assistance for climbing.
6.7.3.9 Ground clearance. The bottom of the fence fabric must be within 2 inches of firm soil, or buried sufficiently (concrete footings or gravel may be used) in soft soil to compensate for shifting soil.
6.7.3.10 Culverts and openings. Culverts under or through a fence shall be of 10-inch pipe or of clusters of such pipe or its equivalent.
6.7.3.11 Openings under or through a fence shall be secured with material equal or greater in strength than the overall barrier.
6.7.3.12 Fence placement. No fence should be located so that the features of the land (its topography) or structures (buildings, utility tunnels, light and telephone poles, fire escapes, ladders, etc.) defeat its purpose by allowing passage over, around, or under the fence.
6.7.3.13 Top guards. Top guards are constructed on perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire along the top of a fence, facing upward and outward, at approximately a 45-degree angle. Top guard supporting arms shall be permanently affixed to the top of fence posts to increase the overall height of the fence by at least 1 foot. Three strands of 12-gauge barbed wire, spaced no more than 6 inches apart, must be installed on the

supporting arms. The top guard of fencing adjoining gates may range from a vertical height of 18 inches to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gates adequately.

6.8 Barriers

6.8.1 Buildings, structures, waterfronts, and other barriers used instead of (or as a part of) a fence line should provide equivalent protection to the fencing required for that area.

6.8.2 All windows, doors, and other openings must be provided adequate protection (e.g., wire mesh caging), or properly secured.

6.8.3 Walls

6.8.3.1 Where walls, floors, or roofs serve as barriers, they should be constructed and arranged to provide uniform protection equivalent to that provided by chain-link fencing as specified.

6.8.3.2 In this connection, windows and other openings in perimeters of security areas in any of the following categories should be protected by securely fastened bars, grills, or other equivalent structural means.

a. Openings less than 18 feet above uncontrolled ground, roofs, ledges, etc.

b. Openings less than 14 feet directly or diagonally opposite uncontrolled windows in other walls, fire escapes, roofs, etc.

c. Openings less than 6 feet from uncontrolled openings in the same wall.

6.8.4 Perimeter Openings

6.8.4.1 Openings in perimeter barriers shall be kept to the minimum necessary for the safe and efficient operation of the Center.

6.8.4.2 The CCPS, in coordination with facilities engineering, safety and fire, shall approve all openings.

6.8.4.3 Authorized barriers shall be constantly locked, controlled by authorized personnel, or otherwise secured to prevent unauthorized entry or exit.

6.8.4.4 Those areas that cannot be secured because of safety/fire hazards may be secured utilizing lead seals.

6.8.4.5 When locked and not under constant surveillance, they shall be subject to periodic checks by protective forces or other designated personnel and/or monitored by CCTV.

6.8.5 Gates.

6.8.5.1. Gates are designed to facilitate the entrance and exit of authorized personnel and vehicle traffic, and to control its flow.

6.8.5.2. The CCPS, in coordination with facilities engineering, safety and fire, shall establish gate operations and designations.

a. Designated gates shall be limited to the number consistent with efficient operations and traffic flow.

b. Alternative gates, which are closed except during peak movement hours, may be provided, so that heavy traffic flow can be expedited.

c. When open or operating, all gates shall be under continuous positive control.

d. Gates shall provide protection equivalent to the outer fences or barriers of which they are a part when not in use.

e. Gates shall be locked to form an integral part of the established perimeter when secured.

6.8.6 Pedestrian gates.
a. Approved pedestrian gates and turnstiles shall be channeled in such a manner that allows only one person entering or departing to approach the custodial sentry at a time.
b. Some channels may be closed between peak use hours.
c. Where possible, pedestrian and vehicular gates should be clearly separated.
d. All vehicle gates shall be equipped with a center stabilizing rod and hole.
6.8.7 Vehicle Gates.
6.8.7.1 Where feasible, approved vehicle gates should be set well back from any public highway, so that temporary delays caused by identification control checks at the gate shall not cause traffic hazards extending out onto a public highway.
6.8.7.2 There should also be sufficient space at the gate to allow for spot checks, inspections, searches, and temporary parking of vehicles, without impeding the flow of traffic.
6.8.8 Inspection
6.8.8.1 When gates are not in active use, they shall be locked and frequently inspected by security personnel.
6.8.8.2 Locks shall be serviced as required.
6.8.8.3 The CCPS shall assure security and accountability for the keys to locks on these gates per Chapter 5 of this NPR.

6.9 Doors, Windows and Skylights
6.9.1 FSL I
a. Building or egress doors at NASA Centers or at the area perimeter shall be protected with non-removable hinges and high-security mechanical or electronic locks. Emergency exit doors should be secured using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.
b. At a minimum, all operable ground floor windows should be locked.6.8.2.
6.9.2 FSL II and III
a. Use of NASA PIV Smartcard/EPACS shall be used to control access of authorized personnel for entry doors. Armed security officers may be used to authenticate and authorize access in lieu of EPACS.
b. For all FSL III and FSL IV assets, use of CCTV shall be required.
c. Windows should be provided protection to prevent visual observation into critical areas such as blinds, curtains or other window treatments.
d. Windows, skylights, and other openings that penetrate the perimeter barrier and have a security mesh or grating area of 96 square inches or greater shall be secured with grilles, bars or IDS
e. Use of protective screens is recommended when the threat level is such that the screens could provide the additional value of preventing missiles, such as hand grenades, bombs, and incendiaries, from being hurled through the windows from outside the perimeter.
6.10 Sewers, Culverts and Other Utility Openings
6.10.1 Sewers, air intakes, exhaust tunnels and other utility openings that penetrate the perimeter or security area barrier and have a cross-section area of 96 square inches or greater shall be protected by securely fastened bars, grilles, locked manhole covers, or

other equivalent means that provide security commensurate to that of the perimeter or security area barrier.
6.10.1.1 As a reminder, these bars and grilles across culverts, sewers, storm sewers, etc. are a hazard when susceptible to clogging, and should be considered during planned construction of such bars and grilles.
6.10.1.2 All such areas should be designed to permit rapid clearing or removal of grating when conditions require such action.
6.10.1.3 Removable grates shall normally be locked in place.
6.10.1.4 At a minimum, air intakes should be protected with emergency shutdown, shelter in place (SIP), and evacuation procedures.

6.11 Utility Poles and Trees

6.11.1 Poles and trees located outside or inside of and within 10 feet of the perimeter barrier of the security area present a possible means of illegal entry. To reduce this possibility, the perimeter barrier may be adjusted so as to increase the distance to more than 10 feet and heightened to the extent necessary to prevent entry, or the obstruction must be removed. If these utility poles, signboards, trees, etc. also obstruct the visibility of the security officer, they must be moved (or removed) at least 10 feet outside or inside the perimeter barrier.

6.12 Clear Zones

6.12.1 Designated security areas and protective barriers at NASA Centers shall maintain unobstructed areas or clear zones.
6.12.2 The unobstructed areas or clear zones should be maintained on both sides of and between physical barriers.
6.12.3 This shall be accomplished by removal of all trees, brush, rock piles, etc. within the designated zone and the frequent cutting of vegetation or the use of chemicals designed to control or kill such vegetation.
6.12.3.1 Vegetation shall not exceed 8 inches in height.
6.12.4 These areas shall be kept free of vehicles, structures, and debris.
6.12.5 Protective barriers inside a clear zone should be at least 10 feet from the perimeter.
6.12.6 Where possible and when the sensitivity of the activity requires a larger clear zone, it should be provided to preclude/minimize damage from thrown objects such as incendiaries or bombs.
6.12.7 Protective barriers outside clear zones shall be 10 feet or more from the perimeter fence/protective barrier and any exterior structures, vegetation, or any obstruction to visibility.
6.12.8 Construction of any new protective barrier for security operations having a smaller clear zone must be coordinated with facilities engineering, safety and fire, and approved by the CCS.
6.12.9 Although 10 feet is the permissible minimum criteria for NASA Centers, every effort shall be made to establish a clear zone external to the protective barrier of 75 feet.
6.12.10 The minimum NASA standard clear zone for effective surveillance of the perimeter terrain when planning new activities or expansion of existing activities is 10 feet inside the barrier, 10 feet between barriers/fences, and 10 feet exterior to the boundary fence.

6.12.11 In addition to security, these clear zones also provide the safety feature of a 60-foot-wide fire-break between a Center's operational areas, structures, or storage facilities and the adjoining areas. It is especially important to maintain clear zones during periods of high fire risk.

6.13 Inspection and Repair of Barriers

6.13.1 Center security or other designated personnel shall periodically check designated barriers for defects that would facilitate unauthorized entry. Both Center security and other personnel must be alert to detect the following:

a. Damaged areas (cuts in fabric, broken barbed wire/ posts).
b. Deterioration (corrosion).
c. Erosion of soil beneath the barrier.
d. Loose-fitting barbed wire, outriggers, or fabric fastener.
e. Growth in the clear zones that would afford cover for possible intruders.
f. Obstructions at or on the fence that would afford concealment or aid entry/exit for an intruder.
g. Evidence of illegal or improper entry.
h. Damaged or tampered lead seals in place.

6.14 Signs and Posting of Boundaries

6.14.1 The boundaries of NASA Centers shall be posted with signs having the wording "RESTRICTED AREA - NO TRESPASSING" (NASA Form 1506) in 2-inch red/black letters. (See Appendix G for other signs.)

6.14.2 Signs shall be located on the exterior side of the Center perimeter barrier or mounted on posts along the boundary line.

6.14.3 The interval between signs shall be adequate to permit at least one sign visible and legible during daylight hours to anyone approaching the boundary from outside the Center.

6.14.4 All designated security areas or spaces shall be plainly identified by signs reading "NASA CONTROLLED AREA" (formerly RESTRICTED AREA), "NASA LIMITED AREA," or "NASA EXCLUSION AREA" (formerly CLOSED AREA).

6.14.4.1 These signs shall further bear in small lettering the words, "Unauthorized Persons Who Enter May Be Subject to Prosecution Under 18 U.S.C. 799."

6.14.4.2 Signs shall be placed on the outward edge of the clear zone or security areas and on the perimeter fence.

6.14.4.3 The purpose of this placement is to prevent unintentional approach to the security area barrier through the clear zone.

6.14.4.4 Signs shall be spaced such that they are visible and legible to anyone approaching the security area from any direction.

6.14.5 All roads approaching the security area shall be clearly posted with restrictive-entry signs.

6.14.6 Photography Prohibited signs may be posted as recommended by the Center Protective Services Office.

6.14.7 Avoid making outside locations such as air intakes, fuel supply valves, gas or distribution locations, evacuations assembly areas, etc.

6.14.8 The requirements contained herein are considered the minimum acceptable.

CHAPTER 7: Security Criteria and Level of Protection (LOP)

7.1 Purpose

7.1 The following tables identify the security measures to be applied as part of the baseline LOP (LOP I). Requirements for LOP II through IV are also provided. Requirements for LOP IV shall meet all requirements of LOP III with additional protections as determined by the DBT and the CCPS. Section 7.2 of this NPR provides additional detail of security measures.

a. Site – including the site perimeter, site access, exterior areas and assets, and parking;

b. Structure – including structural hardening, façade, windows, and building systems;

c. Facility Entrances – including employee and visitor pedestrian entrances and exits, loading docks, and other openings in the building envelope;

d. Interior – including space planning and security of specific interior spaces;

e. Security Systems – including IDS, EPACS and CCTV systems; and,

f. Security Operations and Administration – including planning security force operations, management and decision making, and mail handling and receiving.

Table B - Site Security Criteria

Security Criterion	Level I	Level II	Level III	Level IV
Identification as a NASA Federal Facility	No special measures.	Signage identifying a facility as a NASA Federal facility should be posted on the perimeter.	Signage identifying a facility as a NASA Federal facility should be posted on the perimeter.	Signage identifying a facility as a NASA Federal facility should be posted on the perimeter.
Landscaping	Minimize areas of concealment in and around facilities.	Restrict landscaping from obstructing views of the security officers and CCTV cameras, or interfering with lighting or IDS.	Restrict landscaping from obstructing views of the security officers and CCTV cameras, or interfering with lighting or IDS.	Restrict landscaping from obstructing views of the security officers and CCTV cameras, or interfering with lighting or IDS.
Pedestrian Access to Site	No special measures required.	In a campus environment, install fence, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.	Install fence, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.	Install fence, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.
Vehicle Access Points	Limit the number of vehicle access points.	Limit the number of vehicle access points.	Limit the number of vehicle access points.	Limit the number of vehicle access points.
Site Lighting	Install exterior lighting at entrances, exits, parking lots, and garages.	Install exterior lighting at entrances, exits, parking lots, garages, and walkways from parking areas to entrances.	Install exterior lighting at entrances, exits, parking lots, garages, walkways from parking areas to entrances, and around building perimeter areas.	Install exterior lighting at entrances, exits, parking lots, garages, walkways from parking areas to entrances, and around building perimeter areas.
NASA Controlled	NASA Controlled Areas will not be	Additional signage requirement when the	Additional signage requirement when the	Additional signage requirement when the facility or area has

Security Criterion	Level I	Level II	Level III	Level IV
Areas	designated in this LOP category and shall require minimum LOP II security measures.	facility or area has been designated as a NASA Controlled Area.	facility or area has been designated as a NASA Controlled Area.	been designated as a NASA Controlled Area.
NASA Limited Areas	NASA Limited Areas will not be designated in this LOP category and shall require minimum LOP III security measures.	NASA Limited Areas will not be designated in this LOP category and shall require minimum LOP III security measures.	Additional signage requirement when the facility or area has been designated as a NASA Limited Area.	Additional signage requirement when the facility or area has been designated as a NASA Limited Area.
NASA Exclusion Areas	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	Additional signage requirement when the facility or area has been designated as a NASA Exclusion Area.
Control of Parking	No special measures required.	Control vehicle access to underground/in-building parking and on-site surface or structured parking.	Control vehicle access to underground/in-building parking and on-site surface or structured parking.	Control vehicle access to underground/in-building parking and on-site surface or structured parking. Risk/ Vulnerability assessment results may require setback distance.
Authorized Parking	No special measures required.	Limit parking to employee vehicles, authorized visitor vehicles, approved	Limit parking to employee vehicles, authorized visitor vehicles, and approved	Limit parking to employee vehicles, authorized visitor vehicles, and approved government vehicles.

Security Criterion	Level I	Level II	Level III	Level IV
		government vehicles, and other authorized parkers.	government vehicles.	
Vehicle Access to Controlled Parking	No special measures required.	Designate employee and visitor parking areas. Use vehicle gates to limit access of vehicles to authorized vehicles only.	Designate employee and visitor parking areas. Use vehicle gates to limit access of vehicles to authorized vehicles only.	Provide vehicle barriers to protect parking entrances from penetration by an unauthorized vehicle. Vehicle entrances shall be staffed by a security officer who has the ability to raise the barriers quickly in an emergency, or utilize a dual barrier vehicle trap system to prevent piggybacking.
Vehicle Barriers	No special measures required.	Provide vehicle barriers to protect pedestrian entrances from penetration by an unauthorized vehicle.	Provide vehicle barriers to protect pedestrian and vehicle access points, and critical areas/utilities from penetration by an unauthorized vehicle.	Provide vehicle barriers to protect pedestrian and vehicle access points, and critical areas/utilities from penetration by an unauthorized vehicle. Risk/Vulnerability assessment results may require vehicle barriers around the entire facility with appropriate setback distance.
Vehicle Screening	No special measures required.	Visual screening by security officers. Randomly screen employee, visitor and contractor vehicles. During heightened security alerts, screening of all	Randomly screen employee, visitor and contractor vehicles. During heightened security alerts, screening of all vehicles may be directed by the CCPS.	Randomly screen employee, visitor and contractor vehicles. During heightened security alerts, screening of all vehicles may be directed by the CCPS.

Security Criterion	Level I	Level II	Level III	Level IV
		vehicles may be directed by the CCPS.		
Pedestrian Access to Controlled Parking Areas	No special measures required.	Minimize areas of concealment in and around parking areas.	Monitor pedestrian access to parking areas.	Provide barriers to restrict pedestrian access into parking areas to authorized entry points and limit pedestrian access to controlled parking areas to authorized personnel only.
Hazardous Materials Storage	Locate HAZMAT storage in a NASA Controlled Area, at a minimum, away from loading docks, entrances, and uncontrolled parking.	Locate HAZMAT storage in a NASA Controlled Area, at a minimum, away from loading docks, entrances, and uncontrolled parking.	Locate HAZMAT storage in a NASA Controlled Area, at a minimum, away from loading docks, entrances, and uncontrolled parking	Locate HAZMAT storage in a NASA Controlled Area, at a minimum, away from loading docks, entrances, and uncontrolled parking.
Receptacle and Container Placement	No special measures required.	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.

Table C - Structure Security Criteria

Security Criterion	Level I	Level II	Level III	Level IV
Windows	Lock all operable ground floor windows.	Lock all operable windows within 16 feet of the ground or other access points.	Design exterior windows in publicly accessible locations to resist forced entry. Implement IDS on windows. Provide blinds, curtains, or other window treatments in critical areas that can be used to prevent visual observation.	Design exterior windows in publicly accessible locations to resist forced entry. Implement IDS on windows.
Walls and Non-Window Openings	No special measures required.	Protect non-window openings such as mechanical vents and exposed plenums to resist forcible entry.	Protect non-window openings such as mechanical vents and exposed plenums to resist forcible entry.	Protect non-window openings such as mechanical vents and exposed plenums to resist forcible entry.
Protection of Air Intakes	Provide emergency shutdown, SIP, and evacuation procedures.	Provide emergency shutdown, SIP, and evacuation procedures and protect accessible air intakes with fencing. Monitor with CCTV or security officer patrols.	Provide emergency shutdown, SIP, and evacuation procedures and protect accessible air intakes with fencing. Monitor with CCTV or security officer patrols. Where possible, place air intakes on rooftop or on wall at least 30 feet or three stories above grade.	Provide emergency shutdown, SIP, and evacuation procedures and protect accessible air intakes with fencing. Monitor with CCTV or security officer patrols. Where possible, place air intakes on rooftop or on wall at least 30 feet or three stories above grade.
Security of	No special measures	Protect the system	Provide IDS coverage	Provide IDS coverage

Security Criterion	Level I	Level II	Level III	Level IV
Ventilation Equipment and Controls	required.	controls from unauthorized access.	and EPACS into ventilation equipment and control rooms.	and EPACS into ventilation equipment and control rooms.
Location of Utilities and Feeders	No special measures required.	No special measures required.	Locate utility systems at least 25 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect utilities	Locate utility systems at least 50 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect utilities.
Separation of Emergency and Normal Power Distribution	No special measures required.	No special measures required.	Install emergency and normal power distribution systems (including electric panels, conduits, and switchgears) at least 25 feet apart.	Install emergency and normal power distribution systems (including electric panels, conduits, and switchgears) at least 50 feet apart.
Emergency Generator Protection	If an emergency generator is used, secure it against unauthorized access.	If an emergency generator is used, secure it against unauthorized access.	If an emergency generator is used, secure it against unauthorized access and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff,	If an emergency generator is used, secure it against unauthorized access and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff,

Security Criterion	Level I	Level II	Level III	Level IV
			hardening, and venting methods to protect utilities at these locations.	hardening, and venting methods to protect utilities at these locations.

Table D - Facility Entrance Security Criteria

Security Criterion	Level I	Level II	Level III	Level IV
Badge Identification (ID) System	No special measures required.	Require NASA PIV Smartcard badge or other authorized NASA issued ID be worn and visible at all times when in NASA controlled spaces.	Require NASA PIV Smartcard badge or other authorized NASA issued ID be worn and visible at all times when in NASA controlled spaces.	Require NASA PIV Smartcard badge or other authorized NASA issued ID be worn and visible at all times when in NASA controlled spaces.
Regulatory Signage	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.
Employee Access Control	Issue employees keys for access.	Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility. Require ID badge presentation to security officer for visual and physical inspection before entry or EPACS authentication to allow entry.	Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility. Require ID badge presentation to security officer for visual and physical inspection before entry or EPACS authentication to allow entry.	Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility. Require ID badge presentation to security officer for visual and physical inspection before entry or EPACS authentication to allow entry.
Visitor Access Control	Entrances are open to the public during business hours and no special measures required. After hours	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access

Security Criterion	Level I	Level II	Level III	Level IV
	entrances are secured, and have a means to verify the identity of persons requesting access prior to allowing entry into the facility.	escorted at all times. Require visitors to nonpublic areas display a NASA visitor ID badge.	or escorted at all times. Require visitors to nonpublic areas display a NASA visitor ID badge.	or escorted at all times. Require visitors to nonpublic areas display a NASA visitor ID badge.
Employee and Visitor Screening	No special measures required.	Visual inspections by security officers. CCPS determines need for random inspections of personal belongings and parcels during heightened security alerts.	Visual inspections by security officers. CCPS determines need for random inspections of personal belongings and parcels during heightened security alerts.	Visual inspections by security officers. CCPS determines need for random inspections of personal belongings and parcels during heightened security alerts.
Lobby Queuing	No special measures required.	Minimize queuing caused by screening, visitor processing, and access control system throughput.	Minimize queuing caused by screening, visitor processing, and access control system throughput.	Minimize queuing caused by screening, visitor processing, and access control system throughput
After Hours Access Control	No special measures required.	EPACS required for all after-hour access.	EPACS required for all after-hour access.	EPACS required for all after-hour access.
Limit Building Entry Points	No special measures required.	Limit the number of building entry points to the fewest number practical.	Limit the number of building entry points to the fewest number practical.	Limit the number of building entry points to the fewest number practical.
Perimeter Doors & Door Locks	Secure perimeter doors with high-security mechanical locks.	Secure perimeter doors with non-removable hinges and high-security mechanical or electronic locks.	Secure perimeter doors with non-removable hinges and high-security mechanical or electronic locks. Implementation of	Secure perimeter doors with non-removable hinges and high-security mechanical or electronic locks. Implementation of

Security Criterion	Level I	Level II	Level III	Level IV
			EPACS, IDS and CCTV.	EPACS, IDS and CCTV.
Control of Keys and PIV Smartcards	Implement a formal key control program.	Implement a formal key control program and electronically disable lost or stolen NASA PIV Smartcards.	Implement a formal key control program and electronically disable lost or stolen NASA PIV Smartcards.	Implement a formal key control program and electronically disable lost or stolen NASA PIV Smartcards.
Employee Convenience Doors	No special measures required.	Provide EPACS for employee entry doors without a security officer post (including after-hours access) in conjunction with CCTV coverage.	Provide EPACS for employee entry doors without a security officer post (including after-hours access) in conjunction with IDS and CCTV coverage.	Provide EPACS for employee entry doors without a security officer post (including after-hours access) in conjunction with IDS and CCTV coverage.
Emergency Exit Doors	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit (with panic alarm) hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit (with panic alarm) hardware that are compliant with applicable life safety codes and standards.
Delayed Egress	No special measures required.	No special measures required.	Use delayed egress hardware at emergency exits from designated NASA Limited and NASA Exclusion Areas, if fire code allows.	Use delayed egress hardware at emergency exits from designated NASA Limited and NASA Exclusion Areas, if fire code allows.

Table E - Interior Security Criteria

Security Criterion	Level I	Level II	Level III	Level IV
Space Planning	No special measures required.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.	Implement standoff, hardening, and venting methods to protect critical areas near loading docks, entrances, mailrooms, personnel and package screening locations and uncontrolled parking.
Access to Non-Public Areas	Use signage to designate non-public areas and establish procedures to prevent unauthorized access.	Use signage, stanchions, counters, furniture, knee walls, etc., to establish physical boundaries to control access to non-public areas.	Use signage, walls, IDS, EPACS and/or security officers to establish physical boundaries to control access to non-public areas.	Use signage, walls, IDS, EPACS and/or security officers to establish physical boundaries to control access to non-public areas.
Security of NASA Controlled Areas	NASA Controlled Areas will not be designated in this LOP category and shall require minimum LOP II security measures.	Implement use of EPACS and IDS to control and monitor access into NASA Controlled Areas.	Implement use of EPACS, IDS and CCTV to control and monitor access into NASA Controlled Areas.	Implement use of EPACS, IDS and CCTV to control and monitor access into NASA Controlled Areas.
Security of NASA Limited Areas	NASA Limited Areas will not be designated in this LOP category and shall require	NASA Limited Areas will not be designated in this LOP category and shall require	Implement use of EPACS, IDS and CCTV to control and monitor access into NASA	Implement use of EPACS, IDS and CCTV to control and monitor access into NASA

Security Criterion	Level I	Level II	Level III	Level IV
	minimum LOP III security measures.	minimum LOP III security measures.	Limited Areas.	Limited Areas.
Security of NASA Exclusion Areas	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	NASA Exclusion Areas will not be designated in this LOP category and shall require minimum LOP IV security measures.	Implement use of EPACS, IDS and CCTV to control and monitor access into NASA Exclusion Areas.
Building Systems and Roof Access	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with locks.	Secure utility, mechanical, electrical, and telecom rooms and access to interior space from the roof using locks and IDS.	Secure utility, mechanical, electrical, and telecom rooms and access to interior space from the roof using EPACS, IDS, and CCTV monitoring.	Secure utility, mechanical, electrical, and telecom rooms and access to interior space from the roof using EPACS, IDS, and CCTV monitoring.
Publicly Accessible Restrooms	No special measures required.	Deny public access to restrooms.	Deny public access to restrooms.	Deny public access to restrooms.
Interior Windows	No special measures required.	No special measures required	Provide tempered or high-strength glass.	Provide tempered or high-strength glass.

Table F - Security Systems Criteria

Security Criterion	Level I	Level II	Level III	Level IV
CCTV Coverage	No special measures required.	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, and lobbies.	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, and other potential access points.	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, other potential access points, and potential criminal and terrorist pre-operational surveillance locations.
CCTV Monitoring and Recording	No special measures required.	Record CCTV views using time-lapse video recording and digital image storage. At least 1 year storage of images required.	Conduct alarm-activated CCTV monitoring and record using time-lapse video and digital image storage. At least 1 year storage of images required.	Conduct active CCTV monitoring by security officers and record using time-lapse video and digital image storage. At least 1 year storage of images required.
Security Control Center	No special measures required.	Provide an onsite central security control center, staffed 24/7/365.	Provide an onsite central security control center, staffed 24/7/365.	Provide an onsite central security control center, staffed 24/7/365.
CCTV Surveillance Advisory	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.
Intrusion	No special measures	Provide IDS on	Provide IDS on	Provide IDS on

Security Criterion	Level I	Level II	Level III	Level IV
Detection System (IDS) Coverage	required.	perimeter entry and exit doors, and all ground-floor windows.	perimeter entry and exit doors, all windows within 16 feet of the ground or other access point.	perimeter entry and exit doors, all windows within 16 feet of the ground or other access point, and any other openings larger than 96 square inches.
Intrusion Detection System (IDS) Monitoring	If implemented, monitor at a central station with notification and response by armed security officer personnel.	Monitor at an on-site central station with notification and no <15 minute response by on-site armed security officer personnel.	Monitor at an on-site central station with notification and no <15 minute response by on-site armed security officer personnel.	Monitor at an on-site central station with notification and no <10 minute response by on-site armed security officer personnel.
Duress Alarms or Assistance Stations	Implement duress procedures for emergency situations.	Provide duress buttons or call buttons at security officer posts, sensitive public contact areas, in garages, and other areas that are identified as high-risk locations.	Provide duress buttons or call buttons at security officer posts, sensitive public contact areas, in garages, and other areas that are identified as high-risk locations.	Provide duress buttons or call buttons at security officer posts, sensitive public contact areas, in garages, and other areas that are identified as high-risk locations.
Security System Integrity	No special measures required.	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized access.	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized access. Utilize supervised circuits for alarms	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized access. Utilize supervised circuits for alarms.
Security	No special measures	Provide a centralized,	Provide a centralized,	Provide a centralized,

Security Criterion	Level I	Level II	Level III	Level IV
Communications	required.	secure and monitored radio network for security officer personnel.	secure and monitored radio network for security officer personnel.	secure and monitored radio network for security officer personnel.
Building Communication System	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.
Emergency Power for Security Systems	No special measures required.	Provide uninterruptible emergency power to essential electronic security systems for a minimum of 4 hours.	Provide uninterruptible emergency power to essential electronic security systems for a minimum of 4 hours or as long as mission requirements dictate continuous operation of the facility.	Provide uninterruptible emergency power to essential electronic security systems for as long as mission requirements dictate continuous operation of the facility.
Security System Testing	Conduct security system performance testing annually.	Conduct security system performance testing annually.	Conduct security system performance testing annually.	Conduct security system performance testing annually.
Security System Maintenance	Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within five business days.	Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable for service must be replaced or repaired within five business days.	Implement a preventive maintenance program for all security systems. Any critical component becomes inoperable for service must be replaced or repaired within 72 hours. Security system outages due to need	Implement a preventive maintenance program for all security systems. Any critical component becomes inoperable for service must be replaced or repaired within 72 hours. Security system outages due to need

Security Criterion	Level I	Level II	Level III	Level IV
			for service or inoperability due to system upgrades will require increase of security officer patrols.	for service or inoperability due to system upgrades will require appropriate security officer personnel posting at access/entry points.

Table G - Security Operations and Administration Criteria

Security Criterion	Level I	Level II	Level III	Level IV
Designated Official (DO)	The DO is the Center Director and responsible for management oversight of security, safety, and emergency management in the facility.	The DO is the Center Director and responsible for management oversight of security, safety, and emergency management in the facility.	The DO is the Center Director and responsible for management oversight of security, safety, and emergency management in the facility.	The DO is the Center Director and responsible for management oversight of security, safety, and emergency management in the facility.
Security Operations Management	Center Chief of Protective Services has management responsibilities for security officers and other physical security operations.	Center Chief of Protective Services has management responsibilities for security officers and other physical security operations.	Center Chief of Protective Services has management responsibilities for security officers and other physical security operations.	Center Chief of Protective Services has management responsibilities for security officers and other physical security operations.
Security Officer Fixed Post - Exterior	No special measures required.	Provide fixed armed security officer posts on exterior to challenge and identify approaching persons prior to entry into the building 24/7.	Provide fixed armed security officer posts on exterior to challenge and identify approaching persons prior to entry into the building 24/7.	Provide fixed armed security officer posts on exterior to challenge and identify approaching persons prior to entry into the building 24/7.
Security Officer Fixed Posts - Screening Checkpoints	No special measures required.	Post armed security officers at all screening checkpoints.	Post armed security officers at all screening checkpoints.	Post armed security officers at all screening checkpoints.
Security Officer Patrols	No special measures required.	Establish hourly exterior roving armed security officer patrols during normal	Establish hourly interior and exterior roving armed security officer patrols during	Establish hourly interior and exterior roving armed security officer patrols during 24/7.

Security Criterion	Level I	Level II	Level III	Level IV
		business hours.	24/7.	
Security Officer Response	Develop plans for on-site security officer response to incidents.	Develop plans for on-site security officer response to alarms and incidents.	Develop plans for on-site security officer response to alarms and incidents.	Develop plans for on-site security officer response to alarms and incidents.
Facility Security Plan	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.
Occupant Emergency Plan (OEP)	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.
Availability of Emergency Plans and Documents	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.
Protection of Construction	No special measures required.	Limit access to construction	Limit access to construction	Limit access to construction documents to

Security Criterion	Level I	Level II	Level III	Level IV
Information		documents to those persons with an established need-to-know. Mark and handle as CUI.	documents to those persons with an established need-to-know. Mark and handle as CUI.	those persons with an established need-to-know. Mark and handle as CUI.
Security During Construction and Renovation	No special measures required.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.
Mail/Package Handling and Other Deliveries	No special measures required.	Screen all mail and packages using x-ray at a loading dock if present or at an existing screening location if there is no loading dock. Physically inspect items that cannot be passed through screening equipment or when x-ray equipment is not present.		Screen all mail and packages using x-ray at a loading dock if present or at an existing screening location if there is no loading dock. Physically inspect items that cannot be passed through screening equipment or when x-ray equipment is not present.
Security Awareness Training	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.

7.2 Details of Security Measures

a. Effective deployment of countermeasures requires a full understanding of the recommended security measure. Accordingly, the tables below give details of selected security measures identified in Section 7.1 of this NPR. As in that section, criteria are grouped according to site, structure, facility entrances, interior, security systems, and operations and administration. This additional detail is provided to convey the full meaning and scope of those baseline security measures whose title and brief description alone are not sufficient. For those measures for which additional detail is not provided, the baseline description is considered sufficient.

Table H - Site

Security Criterion	Detail
Identification as Federal Facility	Where the interaction with visitors is customer-service oriented, and signage would improve the ability of customers to locate the facility, use of external signage would be appropriate.
Landscaping	Landscaping may be used as a protective measure to obstruct views from outside a facility or as a physical barrier. A balance must be achieved between its usefulness in protection and its potential negative impact on security measures. Apply principles of Crime Prevention Through Environmental Design (CPTED) where appropriate. CPTED is a crime prevention strategy that uses architectural design, landscape planning, security systems and visual surveillance to create a potentially crime-free environment by influencing human behavior. CPTED usually involves the use of four principles: (1) Natural Surveillance (by placing physical features, activities, lighting, and people to preclude blind spots or hiding spots to keep intruders easily observable); (2) Territorial Reinforcement (using buildings, fences, different paving material, changes in street elevation, signs, and other landscaping to express ownership by distinguishing to potential offenders private spaces from public spaces), (3) Natural Access Control (strategic placement of entrances, exits, fencing, landscaping, and lighting to create in potential offenders a perception of risk); and (4)Target Hardening (use of features that prohibit entry or access, such as perimeter boulders/large rocks, streetscape furniture, art ornaments, etc.).
Pedestrian Access to Site	The level of protection afforded by the barriers should be commensurate with the need to limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences or razor/barbed wire. Lower levels of protection, intended to guide pedestrians, can be achieved using shrubbery, decorative fencing, or knee walls.

Security Criterion	Detail
Vehicle Access Points	Reducing the number of vehicle access points, particularly under periods of heightened threat, reduces vulnerability and security costs associated with monitoring and controlling access to the site.
Site Lighting	For minimum lighting levels, refer to the Illuminating Engineering Society (IES) Lighting Handbook. Lighting should be sufficient to illuminate potential areas of concealment, enhance the observation of security officer patrols, and provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility. Site lighting should be coordinated with the CCTV system. Maintained Illumination Level (lux) Horizontal Illumination - Covered parking areas - 10 - Roof and surface parking area - 2.5 - Stairwells, elevator lobbies - 20 - Uniformity ratio (average:minimum) 4:1 - Uniformity ratio (maximum:minimum) 20:1 Vertical Illumination - Covered parking areas-5 - Roof and surface parking area-2.5 - Stairwells, elevator lobbies-10 Consider using motion detection where appropriate.
Restricted Areas	Restricted areas include but are not limited to utility connections, loading docks, emergency power supplies, child-care play yards, hazardous-materials storage, HVAC, and exterior access to critical rooms such as telecom and IT resources. Transparency or opaqueness and height of the fence are a site-specific determination. The level of protection afforded by the barriers should be commensurate with the need to limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences or razor/barbed wire. Lower levels of protection, intended to guide pedestrians, can be achieved using shrubbery, decorative fencing, or knee walls.
Signage - Sensitive Areas	Avoid marking outside locations such as air intakes, fuel supply valves, gas or power distribution locations, evacuation assembly areas, etc.
Control of Parking	Government control of parking, or other formal arrangements with the owner of non-Government parking, is required to ensure the limitation of parking to authorized vehicles. Post "No Parking" signage and arrange for towing of unauthorized vehicles where parking is restricted. For the Level III - High LOP, the setback distance is determined as part of determining the LOP (a combination of hardening and setback to defeat the DBT). All parking within that setback distance must be controlled.

Security Criterion	Detail
Authorized Parking	Utilize a parking pass or other similar system to clearly identify authorized vehicles upon entry and while parked. Passes should be visible, numbered, have an expiration date and issuance should be managed by a single authority. Visitor parking should be located as far from the facility as practical. Assigned employee and Government parking may be used to establish a "buffer zone."
Vehicle Access to Controlled Parking	Design site circulation to prevent high-speed approaches by vehicles, and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.
Vehicle Barriers	Use a vehicle velocity that considers the angle of incidence in conjunction with the distance between the perimeter and the point at which a vehicle likely would be able to start a run at the perimeter. Design site circulation to prevent high speed approaches by vehicles, and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed. Appropriate measures for the barrier system may include walls, fences, trenches, berms, ponds and water basins, boulders, plantings, trees, static barriers, sculptures, and street furniture. Maximum clear spacing between vehicle barriers is 4 feet. Minimum barrier height is 30 inches. Barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, or SD-STD-02.01, Revision A, Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates.
Vehicle Screening	At a minimum, vehicle screening should include a visual inspection of the vehicle exterior, undercarriage, passenger compartment, and trunk. For higher risk facilities, consider explosive trace detection systems or canine support. Provide adequate lighting in screening area to illuminate the vehicle exterior and undercarriage. Provide CCTV coverage of the screening area. Use barrier systems to ensure vehicles cannot pass beyond the screening checkpoint until cleared. Site configuration permitting, vehicle inspection areas should be located beyond the setback distance. The setback distance is determined as part of determining the LOP (a combination of hardening and setback to defeat the DBT). All parking within that setback distance must be controlled.
Pedestrian Access to Controlled Parking Areas	Limit the number of entrances to the extent practicable. Monitoring of parking areas can be accomplished with CCTV, security officer patrols, or visually from fixed security posts. At a minimum, pedestrian barriers around parking areas should be designed to

Security Criterion	Detail
	prevent casual access and increase the visibility of unauthorized access attempts. In higher risk applications, anti-climb fences, etc., may be used to defeat attempts to cross over the barrier. When required, positive access control may be achieved using EPACS or security checkpoints.
Hazardous Materials Storage	Comply with applicable regulations regarding storage and safety requirements. Depending on the nature of the HAZMAT, measures may need to be designed to prevent access to, release of or unauthorized removal of the HAZMAT from the site. Valves and control mechanisms also must be protected from unauthorized access.
Receptacle and Container Placement	All areas of potential concealment should be routinely examined by security officer patrols. Ensure that containers can be removed during periods of heightened alert.

Table I - Structure

Security Criterion	Detail
Windows	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of windows which resist forced entry comparable to the windows and doors of the facility and secure areas. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security officers and law enforcement personnel are notified and respond. Additional solutions may include burglary-resistant bars, wire mesh window systems, etc.
Walls and Non-window Openings	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of windows which resist forced entry comparable to the windows and doors of the facility and secure areas. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security officers and law enforcement personnel are notified and respond. Additional solutions may include burglary-resistant bars, wire mesh window systems, etc. Non-window openings greater than 96 square inches in perimeter walls should be secured with grilles, bars, or IDS.
Protection of Air Intakes	Securing air intakes makes the building ventilation system less accessible and therefore less vulnerable to threats that might introduce contaminates directly into the intakes. When choosing secure locations for intakes in urban areas, take into consideration the vantage points offered to threats from nearby buildings and roofs.
HVAC Control	Written shut-down procedures shall be included as part of the facility's security and occupant emergency plans. A "one-step shut-off" is a mechanism that requires only a single action by an individual (e.g., engineer or security personnel) to initiate the immediate shut down of all air handling equipment in the building. One-step shut-off controls referenced at Level II and III must be immediately accessible to authorized personnel at all times, such as in a security control center, staffed engineering office, or other location staffed at all times the facility is occupied. Special air-filtration systems designed to continue to operate in a contaminated environment to enable mission continuity are acceptable.
Security of Ventilation Equipment and Controls	In order to ensure HVAC system operation cannot be disrupted by someone physically accessing the controls, HVAC equipment should be located in an area with access limited to security and engineering staff.

Security Criterion	Detail
Location of Utilities and Feeders	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Underground service is preferred, and any access points should be controlled. If utility systems cannot be located away from high-risk areas, service feeds, equipment, or equipment rooms should be hardened.
Separation of Emergency and Normal Power Distribution	Emergency power may not be available in small buildings except for a UPS system.
Emergency Generator Protection	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Emergency generators may be required to support the tenant mission, life-safety requirements, or as part of the uninterruptable power supply for security systems. More secure locations include the roof, protected grade level, and protected interior areas. If the emergency generator is installed outdoors at grade, it should be protected by perimeter walls and locked entrances. The generator should not be located in any areas that are prone to flooding. Provisions for securing refueling and shut-off valves in fuel lines within or in close proximity to the building must be addressed.
Protection of Water Supply	Protection of water supply may be necessary when water is an important component of cooling systems. Reference the current DBT established by the ISC, unless Chemical-Biological-Radiological (CBR) threat type is superseded by an agency-specific threat assessment.

Table J - Facility Entrances

Security Criterion	Detail
Badge Identification (ID) System	A photo ID (NASA PIV/Smartcard or other Center specific photo ID) must be worn on the person so that it is visible from the front, waist level or higher. The picture on the ID should be updated regularly. Other applicable regulations may apply (e.g., HSPD-12).
Regulatory Signage	Examples of appropriate signage include but are not limited to: - Prohibiting the unauthorized possession of firearms and dangerous weapons - Consent to search - Local building rules and regulations regarding prohibited items - CCTV surveillance advisory - Federal property/No Trespassing signs Refer to 41 CFR 102-74 for further examples.
Employee Access Control	At a minimum, the security officer must be able to compare the employee's face to the photo on the ID. It is preferable that the security officer physically touch the ID badge as a further measure to detect counterfeiting.
Visitor Access Control	Personnel escorting visitors must maintain a visual line of sight, physical proximity, or other means of control of the visitor(s). The ratio of visitors to escorts shall be established by the CCPS based on operational requirements. Visitors may require vetting prior to granting access to confirm identity and security clearances as needed. Approval for unescorted access will be based on a facility access policy set by the CCPS.
Occupant Screening	Generally, screening is accomplished using visual searches. Established procedures for visual and follow-up screening must be followed, and security officers screening personnel must be appropriately trained.
Visitor Screening	Generally, screening is accomplished using visual searches. Established procedures for visual and follow-up screening must be followed, and security officers screening personnel must be appropriately trained. Exceptions to visitor screening may be implemented to accommodate Law Enforcement Officials, VIP's and other such individuals as determined by CCPS.
Lobby Queuing	Queuing is reduced by increasing throughput, while maintaining the effectives of the security measures. Increasing the number of security officers, the number of screening lanes, and the processing speed of access control systems can all reduce queuing time. In order to prevent incidents in the lobby from impacting the rest of the facility, designing a "sacrificial lobby" or stand-alone visitor screening area outside the main building foot-print is allowed.

Security Criterion	Detail
After Hours Access Control	The building register should document at least the name, purpose, date, time in and out, and a point of contact for visitors. Use of EPACS is recommended.
Limit Building Entry Points	All building entry points must be controlled and/or monitored. Reducing the number of building entry points, particularly under periods of heightened threat, reduces vulnerability and security costs associated with monitoring and controlling access. Buildings designated as NASA Controlled, Limited or Exclusions Areas must be controlled via EPACS.
Entrance Co-location	Separating employee and visitor entrances improves employee throughput and allows for more efficient screening of visitors. Additionally, where the risk of violence perpetrated by a visitor on an employee exists, separating the flow patterns may reduce this risk.
Perimeter Doors & Door Locks	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of doors which resist forced entry comparable to the windows and walls of the facility. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security officers and law enforcement personnel are notified and respond. Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal. Magnetic locks should have at least 1,200 pounds of shear holding power. Electric strikes should meet all specification of UL Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For information on high-security locks, refer to Underwriters Laboratory (UL) Standard 437, Key Locks, American National Standards Institute (ANSI) Standard A156.30-2003, and American National Standard for High Security Cylinders, and ANSI Standard 156.5-2001, American National Standard for Auxiliary Locks and Associated Products.
Control of Keys and Access Media	Access media may include card keys, electronic keys, biometric devices, and NASA PIV Smartcards, etc. All keys and access media should be tracked and inventoried on a regular basis. When an employee no longer requires access, all keys and access media must be recovered or disabled. When keys or access media are reported lost or stolen, they must be deactivated and/or locks should be changed.
Employee Convenience Doors	The use of unguarded/uncontrolled employee convenience doors is discouraged. If used, they should be in locations where they can be monitored, and checked during routine roving security officer patrols. EPACS is recommended for all unguarded entry doors. Such entry doors also should be under CCTV camera coverage, with video recording. Anti-pass back

Security Criterion	Detail
	and anti-tailgating at unguarded doors should be addressed through training and electronic-system programming.
Emergency Exit Doors	Electronic locks on perimeter doors must fail-secure, and electronic locks on interior doors must fail-safe, if such measures do not conflict with applicable fire and safety codes.
Delayed Egress	Delayed egress doors should be used in areas where egress would need to be delayed until security forces can respond and/or CCTV coverage can adequately record the event. Delayed egress should be used for such applications as child-care centers, where children must be prevented from leaving the area unescorted, or from money transaction areas.

Table K - Interior

Security Criterion	Detail
Space Planning	Critical systems and equipment may include security and life-safety systems, power distribution, communications and data, and other mission-critical equipment.
Access to Non-public Areas	The level of protection afforded by the boundaries should be commensurate with the risk to each non-public area. A single facility may have non-public areas protected at various LOPs.
Security of Critical Areas	Critical areas include communications rooms, data centers, operations, and command centers, etc. The following source documents provide Federal physical security requirements for various critical and sensitive areas within facilities. These national requirements are normally augmented by additional agency or departmental specific requirements. SCIFS: Director of National Intelligence, Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities. Non-classified IT Systems: NIST Special Publication 800-53, Revision 2, December 2007, Appendix F-PE. Classified IT Systems: ICD 704, Personnel Security, and Director of Central Intelligence Directive (DCID) 6/3, Protecting SCI information Within Information Technology Systems. National Information Assurance Certification and Accreditation Program (NIACAP). Department of Defense Information Assurance Certification and Accreditation (DIACAP). Open Storage Areas: National Archives and Records Administration's Information Security Oversight Office (ISOO) Directive 1, parts 2001.43 and 2001.52. Additional security measures may be found in the Department of Defense National Industrial Security Program Operating Manual (NISPOM) COMSEC Facilities: NASA Central Officer of Records (COR) COMSEC Standard Operating Procedures (CSOP). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials dated August 1997, as amended by NSTISSC [Memorandum] 003-98 and Committee on National Security Systems (CNSS) [Memorandum] CNSS-079-03, dated 5 August 2003. Special Access Program Facilities: Joint Air Force, Army, Navy (JAFAN 6/9) Manual: Physical Security Standards For Special Access Program Facilities.
Building Systems and Roof Access	Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal. Magnetic locks should have at least 1,200 pounds of shear holding power. Electric strikes should meet all

Security Criterion	Detail
	specification of Underwriters Laboratory (UL) Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For information on high-security locks, refer to UL Standard 437, Key Locks, American National Standards Institute (ANSI) Standard A156.30-2003, American National Standard for High Security Cylinders, and ANSI Standard 156.5-2001, American National Standard for Auxiliary Locks and Associated Products. Where roof access allows entry to critical building or air intakes, CCTV monitoring and recording should be used in conjunction with locking and detection devices.
Publicly Accessible Restrooms	When public access to restrooms is allowed, the level of protection afforded by the boundaries with nonpublic areas should be commensurate with the risk to each nonpublic area. See Access to Nonpublic Areas.
Publicly Accessible Retail and Mixed Use Space	While important to the public nature of buildings, the presence of retail and other mixed uses may present a risk to the building and its occupants, and should be carefully considered on a project-specific basis during the risk-assessment process.
Interior Windows	No special measures required.

Table L - Security Systems

Security Criterion	Detail
CCTV Coverage	The design of the system will vary depending on the objective of the surveillance, environment, facility type, and end-user requirements. Use of a professional for the design and installation is essential to maximize the operational effectiveness of CCTV systems and integration with other physical security equipment. Considerations for CCTV coverage include: - Image quality in all lighting conditions - Lens selection for area versus detail coverage and resolution - Color versus black-and-white images - Fixed cameras dedicated to monitoring specific locations full-time versus pan-tilt-zoom (PTZ) cameras which can be used for active investigation of activity - Blind spots
CCTV Monitoring and Recording	Certain facilities or CCTV views should be actively monitored (including using alarm/IDS integrated CCTV cameras) to facilitate real-time detection and investigation of an incident, and to coordinate an active response to an incident. Other facilities or views may be recorded for forensic purposes only. Security personnel assigned to actively monitor CCTV should be relieved regularly and only be tasked to monitor a limited number of camera views to alleviate fatigue and inattentiveness. Security officials should determine the length of time that personnel can effectively monitor cameras based on the number of views and other activities. An option to minimize fatigue and maximize coverage is the use of sequencing and multiplexing of multiple camera views on the same screen. CCTV recording is intended to develop and maintain a video log of activities which may be referenced if an event is noted after the fact. The minimum length of time for which digital images should be stored is 1 year. Security officials should establish protocols to minimize and control access to the CCTV operating system and stored images. Considerations for CCTV monitoring, recording and storage include: - If the CCTV data is to be transmitted on an IT LAN, determine if the LAN has the capability of providing the minimum level of video resolution, frame rate, and system reliability to satisfy physical security protection needs. - How much and what type of data needs to be retrieved from the system for evidence. CCTV systems may record continuously or only as required to monitor a particular event such as an alarm.

Security Criterion	Detail
	- Develop a chain of custody for evidence retrieval of CCTV images - The need for disaster recovery and remote operational capability, including offsite storage of data - The long-term storage of CCTV images not on operational systems and consideration of offsite storage of data.
Security Control Center	The Security Control Center should incorporate the following (if provided at the facility): - IDS monitoring - CCTV monitoring - Communications equipment for the security officer force - Access control system controls - Fire and other emergency alarm annunciation - HVAC emergency shut-off - Building emergency communications system - Sufficient phone hard lines for incoming and outgoing calls during an incident. These lines may be recorded. - Secure storage of all building plans, security equipment circuit runs, security officer post orders, OEP, COOP, and emergency contacts for security equipment manufacturers. - External emergency notification equipment deemed necessary by the security provider The security control center should be secured as a critical area, and access should be limited to security personnel
CCTV Surveillance Advisory	Signs should be posted at entrances to the site, facility, parking garages, etc., where CCTV coverage exists.
Intrusion Detection System (IDS) Coverage	There are three major groupings of Intrusion Detection Systems (IDS). The following descriptions are provided as benchmarks in considering the appropriate system technologies. All three types are generally used in conjunction with an access control system. 1. Basic Security-in-Depth IDS—Entry Doors: magnetic switch, alarm system keypad, passive infrared sensor (PIR), and an alarm panel (to designated monitoring center). Windows and other openings: glass-break detector, magnetic switches or shock sensors. (Low LOP) 2. Medium Security-in Depth IDS—Entry Doors: Balanced magnetic switch (BMS) or High Security Switch (HSS – UL634 Level 2), PIR, alarm system keypad, alarm system panel (UL1076), with all devices having an individual tamper sensor. Windows (if present) and other openings: glass-break detector, balanced magnetic switches, or shock sensors. IDS control panel fully integrated with other security measures, for example, CCTV cameras, other security

Security Criterion	Detail
	systems (lockdown), sound, heat, and vibration/impact sensors located in critical area(s) or throughout the facility as necessary; also integrated with fire safety system. (SCIFs, open storage areas for collateral classified information, and high consequence lab space, require a high security IDS.) (Medium LOP) 3. High Security-in-Depth IDS—Security Management System: high security IDS system encompassing detection and alarm devices positioned at the site perimeter, restricted areas between the site perimeter and the building, building entrances, and rooms and/or areas within the facility (High LOP). In a facility requiring a High LOP that has no external perimeter, hardening of the first floor may be necessary which may encompass minimizing all entry points, alarming all entry points, enclosing window spaces, and alarming interior rooms and spaces on the first floor with motion detector (volumetric sensors). The technologies used in IDS systems range from relatively basic electrical contact mechanisms (magnetic switch), keypads, and alarm panels connected to a monitoring center to high security devices such as balanced magnetic switches, tamper sensors, motion, heat, sound, or vibration sensors, and other devices that are fully integrated. The specific technologies used should be based on a threat/risk management assessment considering criticality, consequences, and cost. Professional design, engineering, and installation are critical to ensure operational effectiveness of the IDS system itself and its integration with other physical security equipment. UL Listed intrusion detection equipment is strongly recommended. Initial installation should include validation [testing] of the entire system, including monitoring center notification and connected equipment. Periodic testing and maintenance are required to ensure continuous operational effectiveness. Schedule and record results accordingly. Repair/replace malfunctioning equipment as needed based on testing and maintenance results.
Intrusion Detection System (IDS) Monitoring	IDS at certain facilities or protected areas should be actively monitored to facilitate a real-time detection of an incident, and to coordinate an active response to an incident. IDS should be integrated with CCTV systems to the greatest extent possible to facilitate immediate alarm assessment. IDS activity logs are intended to develop and maintain a record of alarm activities which may be referenced if an event is noted after the fact. IDS/alarm activity records should be maintained for a period of not less than 1 year.

Security Criterion	Detail
Duress Alarms or Assistance Stations	Duress alarms should be used at areas such as security officer posts, interview rooms, cash/public transaction areas, or at-risk areas. Duress devices shall be concealed from the public and annunciate for an immediate response. Duress buttons on security officer radios are acceptable for duress buttons at security posts. Procedures on response and telephone contact where the alarm occurred must be established.
Security System Integrity	In addition to controlling physical access, logical access for programming and recordkeeping must be limited to personnel with administrative rights as necessary to maintain and program the system.
Security Communications	For larger or busier security officer forces, it may be necessary to designate a "dispatcher" to control the radio network. Consideration should be given to digitally recording security officer force communications. The radio network should be designed to ensure adequate coverage throughout the facility, and enable a user to contact a communications center regarding tasks, reporting incidents, and requesting assistance.
Building Communication System	The building communication system should be utilized to provide emergency announcements, alerts, and instructions to occupants. On-site communication with security officers, designated response personnel and OEP support employees is essential during an incident. Procedures for standard announcements and drills shall be developed. Standard announcements could be prerecorded into the building communication system for immediate notification by the security provider when warranted. Hearing impaired occupants should be identified and establish alternative procedures to be used in the event of an alert or announcements. Communication may be achieved through public address systems, specially designed phone systems, and computer-based mass delivery.
Emergency Power for Security Systems	Uninterruptable power can be provided through the use of batteries, emergency generators, UPS, or a combination thereof to meet the requirements. More than 4 hours of backup may be required for certain facilities based on mission, such as when the facility is required to maintain 24-hour operations.
Security System Testing	Testing must be based on established, consistent agency-specific protocols, and documented. Components which fail during testing should be serviced in accordance with the Security System Maintenance criteria.
Security System Maintenance	Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing another

Security Criterion	Detail
	temporary measure in instances where the replacement or repair is not achievable within the specified time frame (e.g., a security officer to control access or monitor a critical area normally covered by a camera, or a temporary barrier to replace an inoperable pop-up vehicle barrier). When a security system is inoperable due to system maintenance or upgrade, security officer patrols shall be increased or for critical areas, posted until the security system is operational.

Table M - Operations and Administration

Security Criterion	Detail
Assistant Administrator, Office of Protective Services (AA/OPS)	The AA/OPS is the approval authority for any deviation from minimum perimeter baseline standards or facilities housing NASA Critical Infrastructure (NCI).
Designated Official (DO)	The Center Director serves as the Designated Official (DO) will comply with this NPR. The DO can approve acceptance of the risk for all non-NCI where CCPS acknowledges non-compliance or deviation from required security criteria.
Center Chief Protective Services (CCPS)	The CCPS will ensure compliance with this NPR.
Security Operations Management	In cases where the security organization does not have a presence at the facility or in the region sufficient to meet these requirements, the DO and CCPS will designate an on-site employee to serve in this capacity. If the facility has a security force, the contracting agency will designate (at the request of the DO/CCPS) an on-site employee to serve as a COTR, with the authority to reassign and direct security officer personnel operations during emergencies. The on-site security manager's duties include, but are not limited to: - Contract security force coordination and oversight; - Security equipment testing and maintenance; - Review security assessments and current intelligence information; - Security officer post order development and update; - Ensure implementation of building-specific security policies; - Coordinate with the responsible facility owner (e.g., other Government agency or lessor) the installation, maintenance, testing, repair, and replacement of security equipment; - Maintaining close liaison with the DO, CCPS, and local first responders; and, - The authority to direct security officer force deployment in emergency situations. Security personnel should receive recurring training on current principles, practices, and trends in technology.
Security Officer Fixed Post - Exterior	Require security officers to request the presentation of a NASA issued ID (e.g., NASA PIV Smartcard or valid visitor ID badge) from persons for visual and physical inspection prior to entering the building.
Security Officer Fixed Posts - Screening Checkpoints	Screening checkpoint staffing shall be based on the principle that one security officer only performs one screening task at a time. Consideration must be given to throughput and checkpoint

Security Criterion	Detail
	configuration in making this determination.
Security Officer Patrols	Patrols should be random in nature so as not to establish a predictable pattern that can be circumvented by an adversary. However, the frequency with which a patrol passes any given point on the patrol route should be not more than 1 hour.
Security Officer Response	For facilities that do not have a dedicated security team available for incident response, rovers may be used or posts may temporarily be shut down to provide personnel for a response to an incident. Established procedures and post orders should outline these situations.
Facility Security Plan	The Facility Security Plan provides direction to security personnel on the security management and policies of the building. At a minimum, the Facility Security Plan should: - Identify security related responsibilities; - Identify current and planned security measures; - Define building-specific security policies; - Contain emergency contacts (such as law enforcement, first responders, security organization, and facility manager); - Detail response procedures for emergencies; - Outline approved protocols for access by employees, contractors, and visitors; - Establish changes in security operations due to temporary upgrades in the homeland security advisory system; and, - Outline the security measure testing schedule performed by the security manager at level II and III facilities; and, - Identify security support requirements for OEP. The level of detail to which the plan is written may vary based on the nature of the facility (e.g., Level I facilities may have very abbreviated documents). The plan should be protected as CUI at minimum.
Occupant Emergency Plan (OEP)	The OEP provides direction to the occupants of the building on how to react to emergencies. At a minimum, the OEP should address: - Purpose and circumstances for activation; - Command officials and supporting personnel contact information; - Occupant life-safety options (evacuation, shelter-in-place); - Local law enforcement and first responder response; - Special needs individuals (disabled, deaf, etc.); - Visitors; - Special facilities (e.g., SCIFs, child-care centers); - Assembly and accountability; - Security during and after incident; and, - Training and exercises.

Security Criterion	Detail
	The scope and complexity of the OEP is dependent on the facility's size, population, and mission. The OEP must be reviewed annually and updated. OEPs must also identify unique planning requirements for staff or functions such as evacuating child-care centers.
Availability of Emergency Plans and Documents	The CCPS and other emergency management personnel should have immediate access to the OEP, emergency instructions, building plans, the Facility Security Plan, and contact and communication information. Access to these plans after hours also should be ensured.
Protection of Construction Information	The availability of information on construction, including photography and Web-cam views, must be limited to those with a need-to-know. All efforts should be made to disrupt the planning cycle and increase the chances of discovering a hostile intelligence-gathering operation. The greatest chance of discovery comes when the adversary has to come on or near the site to gather information. If photography or Web-cameras (or similar technology) are used to broadcast construction progress, or construction documents are online, access must be encrypted and password protected.
Security During Construction and Renovation	A Construction Security Plan should describe how NASA's assets, information, equipment, and personnel are protected during the construction process. Construction projects range from small interior space alterations, to building additions, to the construction of a new facility or complex. Required security measures should vary accordingly commensurate with associated threats, vulnerabilities, and consequences. The plan should specify who is responsible for the security of the site during each phase of the project until final completion to include access to the construction site or area within an existing building, and those areas requiring access in order to reach the actual construction area. Security needs may increase or decrease as the project progresses from initial start (demolition or groundbreaking) through substantial completion, that is, when NASA assumes control of the facility and progressive occupancy begins. Critical areas within, or adjacent to, the project may require special, more stringent security measures to protect NASA assets and information. In developing the construction security plan, the Center Protective Services Office should assess all reasonable threats and vulnerabilities to NASA assets, information, equipment, and people. Elements to consider in developing a Construction Security Plan include, but are not limited to, the following: • Perimeter security (site, clear zones, restricted access to areas within a building, etc.)

Security Criterion	Detail
	• Security of construction trailer/construction office • Access control (background checks, clearances, alien status, etc.) • Badging (construction worker ID badges and processing; escort/no escort required; lost badge procedures; access termination procedures) • Vehicular access (construction worker parking; construction material deliveries) • Video surveillance (security officer posts, critical areas, access points within buildings) • Internal security (key control, sensitive areas, internal theft of government or employee property) • Construction worker movement to or through areas that are still occupied or operational • Security of construction plans: (hard copy and electronic) • Physical barriers; construction area warning signs. • Protection of other government (non-NASA) assets • Maintaining security during HAZMAT, law enforcement, fire or medical emergency response Security inspections, such as a Technical Surveillance Countermeasures (TSCM) or explosive detection canine sweep, may be required upon completion of construction work in critical secure areas.
Mail/Package Handling and Other Deliveries	Screening should be accomplished by personnel trained in the ISC Best Practices for Safe Mail Handling and in the operation of the screening equipment. Mail screening may be accomplished by security officers or mailroom staff. For mailroom security measures and mitigation of design events, reference GSA's "Guidelines for Mailroom Construction and Renovation" and the U.S. Postal Inspection Service's "Mail Center Security Guide" Publication 166, September 2002 (at www.usps.com).
Security Awareness Training	Topics may include: - Security policies and procedures; - Workplace violence; - General crime prevention measures; - Suspicious packages; - Reporting security incidents; - Proper reporting and response to fires and other emergencies; and, - Operational security measures. Other training unique to the mission may be applicable and should be requested by the DO/CCPS and provided by the security organization as necessary.

7.3 Undesirable Events (UDEs)

a.To determine if the baseline LOP is sufficient or if customization is needed, the risks to a facility must first be identified and assessed. The table below provides a broad range of undesirable events and definition/description that may impact NASA facilities. A definition of the event is provided to ensure a common understanding of the threat being considered. The definition is a standardized means of categorizing the event and types of activities addressed by the event; it is not intended as the legal definition. Regardless of the level of effort involved in the identification and assessment of risk, the analysis must consider all of these UDEs.

Table N – Undesirable Events

Undesirable Event	Definition/Description
Active Shooter	An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms.
Arson	An attack against a NASA facility by knowingly and willingly setting a fire with the intent to cause damage or destruction to the facility and/or physical injury or loss of life to the occupants.
Assault	Physically assaulting (with or without a weapon) a person or persons inside the facility or on the property.
Breach of Access Control Point – Covert	Use of deceit, coercion, or social engineering to gain access to a facility through a controlled entrance.
Civil Disobedience	Deliberate and planned acts of violence and destruction stemming from organized demonstrations on or near a NASA facility.
Disruption of Building & Security Systems	Physically accessing building or security systems for the purposes of disruption or manipulation of the systems. (Does not include cyber attacks. Prevention of cyber attacks is outside the scope of this document).
Hostile Surveillance	Conducting surveillance of key assets, personnel, security features, operations, or sensitive areas from offsite or outside secure areas for the purposes of collection of information in preparation for an attack.
Release of On-site Hazardous Materials	Unauthorized access to hazardous materials stored onsite with the intent of harming personnel or damaging the facility.
Insider Threat	Individuals with the access and/or inside knowledge of an organization that would allow them to exploit the vulnerabilities of NASA security, systems, services, productions, information, or facilities with the intent to cause harm.
Robbery	Unauthorized removal of Government-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of

	a NASA facility.
Theft	Unauthorized removal of Government-owned or personal property from a facility.
Unauthorized Entry – Forced	Unauthorized access to a facility or controlled area by forced entry.

Undesirable Event	Definition/Description
Unauthorized Entry – Surreptitious	Unauthorized access to a facility or controlled area by stealth
Vandalism	Destruction, damage, or defacing of Government-owned or personal property or assets.
Vehicle Ramming	Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.
Workplace Violence	Violence perpetrated by an authorized occupant or an employee. The assailant can be another employee, authorized tenant, or an authorized visitor.

APPENDIX A. Definitions

Baseline LOP: The degree of security provided by the set of countermeasures identified in this document for each FSL which must be implemented unless a deviation (up or down) is justified by a risk assessment

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Critical Areas: Areas that if damaged and/or compromised could have significant adverse consequences for the agency's mission or the health and safety of individuals within the building or the surrounding community. Also may be referred to as "limited access areas," "restricted areas," or "exclusionary zones." Critical areas do not necessarily have to be within Government-controlled space (e.g., generators located outside Government controlled space).

Customized LOP: The final set of countermeasures developed as the result of the risk based analytical process.

Designated Official (DO): The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials.

Design-Basis Threat (DBT): A profile of the type, composition, and capabilities of an adversary.

Facility Security Level: A categorization based on the analysis of several security related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards
Level of Protection - The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in this NPR are Levels I, II, III and IV.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Risk Acceptance: The explicit or implicit decision not to take an action that would affect all or part of a particular risk

Risk Assessment: The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Risk Assessment Report: The documentation of the risk assessment process to include

the identification of undesirable events, consequences, and vulnerabilities and the recommendation of specific security measures commensurate with the level of risk.

Risk Management: A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and, when necessary, risk acceptance.

Risk Mitigation: The application of strategies and countermeasures to reduce the threat of, vulnerability to, or consequences from an undesirable event.

Setback: The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.

Site: The physical land area controlled by the Government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.

Site Entry: A vehicle or pedestrian access point into, or exit from, the site.

Site Perimeter: The outermost boundary of a site. The site perimeter is often delineated by the property line.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the agency.

Visitor: Any person entering the government facility who does not possess the required identification badge/pass for access or who otherwise does not qualify as an “occupant.”

Vulnerability: A weakness in the design or operation of a facility that an adversary can exploit.

APPENDIX B. Acronyms

ANSI – American National Standards Institute

ASTM – American Society for Testing and Materials

AA – Assistant Adminsitrator

AA&E – Arms, Ammunition, and Explosives

BMS – Balanced Magnetic Switch

CBR – Chemical-Biological-Radiological

CCC – Child Care Center

CCPS – Center Chief of Protective Services

CCTV – Closed Circuit Television

CFR – Code of Federal Regulations

CPTED – Crime Prevention Thgouh Environmental Design

CNSI – Classified National Security Information

COMSEC – Communications Security

COOP – Continuity of Operations

COR – COMSEC Office of Record

COTR – Contracting Officer's Technical Representative

CUI – Controlled Unclassified Information

CSOP – COMSEC Standard Operating Procedures

DBT – Design-Basis Threat

DCID – Director of Central Intelligence Directive

DIACAP – Department of Defense Information Assurance Certificaiton and Accreditation Process

DVD – Digital Video Disk

DSMD – Director, Security Management Division

DO – Designated Official

EPACS – Electronic Physical Access Control System

EO – Executive Order

FSC – Facility Security Coordinator

FSL - Facility Security Level

FSM – Facility Security Manager

FN – Foreign National

GAO – Government Accounting Office

GSA – General Services Administration

HAZMAT – Hazardous Material

HVAC – Heating, Ventilation and Air Conditioning

HSPD – Homeland Security Presidential Directive

HSS – High Security Switch

ICD – Intelligence Community Directive

ID - Identification

IES – Illuminating Engineers Society

IDS – Intrusion Detection System

IPO – Institutional Program Office

ISC – Interagency Security Committee

ISOO – Information Security Oversight Office

IT – Information Technology

ISS – International Space Station

JAFAN – Joint Air Force, Army, Navy Manual

LAN – Local Area Network

LOP – Level of Protection

MHE – Material Handling Equipment

NACI – National Agency Check with Inquiries

NIACAP – National Information Assurance Certificaiton and Accreditation

NISPOM – National Industrial Security Program Operating Manual

NIST – National Institue of Standards and Technology

NPD – NASA Procedural Directive

NPR – NASA Procedural Requirement

NCI – National Critical Infrastructure

NSTISSI - National Security Telecommunications and Information Systems Security Instruction

NSN – National Stock Number

OEP – Occupant Emergency Plan

OI – Office of Inspector General

OPS – Office of Protectives Services

PIR – Passive Infrared

PIV – Personal Identity Verification

PDD – Presidential Decision Directive

POL – Petroleum, Oils, Lubricants

RVI – Random Vehicle Inspection

SCIF – Sensitive Compartmented Information Facility

SF – Standard Form

SOP – Standard Operating Procedure

TV – Television

TSCM – Technical Surveillance Countermeasures

UAV – Unmanned Aerial Vehicle

UDE – Undesirable Event

UL – Underwriters Laboratory

U.S. – United States

USC – United States Code

USPS – United States Post Office

UV – Ultraviolet

VIP – Very Important Personnel

VCR – Video Cassette Recorder

APPENDIX C. Verification Matrices

a. Center Directors and Center Chiefs of Protective Services (CCPS), or their designees determine and document compliance by applying a verification approach that is tailored to meet the needs of the Center. The Office of Protective Services (OPS) conducts functional reviews of the Centers and conducts spot-checks and inspections to review Center compliance and implementation.

b. To determine the OPS compliance with the requirements contained in this NPR, internal and external auditors responsible for verifying Headquarters requirements and processes shall evaluate performance against the requirements contained within this NPR.

JPL NPR 1660.1B, Counterintelligence/Counterterrorism Procedural Requirements

These documents apply to NASA Headquarters and NASA Centers, including all Component Facilities, and to the Jet Propulsion Laboratory to the extent specified in its contract.

NASA Counterintelligence (CI) / Counterterrorism (CT)

NASA Federal and contract employees, grantees, or other entities as provided in the governing agreement or instrument and who are located at any NASA facility shall cooperate fully with NASA CI/CT Special Agents (CISA) to the extent permitted by law during the conduct of CI/CT investigations and activities. (NPD 1660.1B, Para 5.B)

NASA Federal and contract employees shall protect NASA classified and sensitive unclassified information in accordance with Federal and NASA regulations. Accordingly, NASA Federal and contract employees who observe or become aware of information of actual or suspected loss or compromise of NASA classified or sensitive unclassified information shall immediately report such information to a NASA CISA. (NPR 1660.1B, Para 1.2.7.)

NASA Federal and contract employees who observe or become aware of unusual or suspicious contact or overtures by a foreign national to acquire NASA classified or sensitive unclassified information outside normal channels shall immediately report such information to a NASA CISA. (NPR 1660.1B, Para 1.2.7)

NASA Federal and contract employees who observe or become aware of information about suspected or actual international or domestic terrorist activities shall report such information immediately to a NASA CISA or NASA Security Officer. (NPD 1660.1B, Para 5.d and NPR 1660.1B, Para 1.2.3.A & 1.2.7)

NASA Federal and contract employees shall receive a foreign travel CI/CT threat briefing prior to official travel to designated country or high-threat location. Upon return, the employee shall contact a NASA CISA to receive a post travel debrief. For non-official travel to a designated country or high-threat location, employees are strongly encouraged to contact a NASA CISA to receive a foreign travel threat briefing prior to travel. (NPD 1660.1B, Para 2.4 and NPR 1660.1B, Para 1.2.8)

NASA Federal and contract employees shall receive a CI/CT threat briefing when hosting individuals from a designated country or high-threat location. (NPD 1660.1B, Para 5.C.4 and NPR 1660.1B, Para 1.2.3.A)

NASA Procedural Requirements

JPL NM 1600-95

COMPLIANCE IS MANDATORY

NASA Identity and Credential Management

Responsible Office: Office of Protective Services

Table of Contents

Preface
P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Introduction
1.1 Overview
1.2 Identity, Credential, and Access Management (ICAM) Governance
1.3 Scope
1.4 Waivers and Exceptions

Chapter 2. Roles and Responsibilities
2.1 Overview
2.2 Agency Roles and Responsibilities
2.3 Center Roles and Responsibilities
2.4 Separation of Duties for the PIV Role
2.5 Training
2.6 Privacy

Chapter 3. Enrollment and Credential Issuance
3.1 Overview
3.2 Chain of Trust
3.3 NASA Credential Types
3.4 Applicant Types
3.5 Onsite Enrollment and Issuance Procedures for NASA PIV Credentials

Chapter 4. Foreign Nationals
4.1 Overview
4.2 NASA Foreign National Access Policy and Related Requirements
4.3 Processing Onsite Visit Requests
4.4 Foreign National Request and Sponsor
4.5 Requirements and Risk Review
4.6 Authorization
4.7 Implementation
4.8 Variations Based on Type of Onsite Visit Request
4.9 Variations Based on Visitor Characteristics
4.10 Identity Vetting Requirements Based on Length of U.S. Residence
4.11 Identity Vetting Requirements and Credential Type for Visits, Temporary Employees, and Permanent Employees
4.12 Processing Information Technology (IT) Remote Only Requests
4.13 Escort Requirements

Chapter 5. Characteristics of NASA Badges
5.1 NASA Credential Types
5.2 NASA PIV Credential Data
5.3 The Universal Uniform Personal Identification Code (UUPIC)

Chapter 6. PIV Credential Management Lifecycle
6.1 PIV Credential Inventory
6.2 PIV Credential Storage and Handling
6.3 Final Adjudication and Subsequent Investigation
6.4 PIV Credential Usage: Display, Protection, and Proper Usage
6.5 PIV Credential Renewal
6.6 PIV Credential Re-issuance
6.7 PIV Credential PIN Reset
6.8 PIV Credential Revocation
6.9 Lost and Stolen Credentials
6.10 Forgotten Credentials
6.11 PIV Credential Suspension
6.12 PIV Credential Return
6.13 PIV Credential Termination
6.14 PIV Credential Destruction

Appendix A – Definitions
Appendix B – Acronyms
Appendix C – NASA Photo Identification Badge Standards
Appendix D – Subscriber Agreement

Preface

P.1 PURPOSE

a. This NASA Directive establishes Agency-wide identity and credential management policy and establishes high-level implementation requirements as set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended.

b. This NASA directive prescribes personnel responsibilities and procedural requirements for the creation, usage, and management of identities and the creation and issuance of identity credentials to assist NASA Centers and component facilities in executing the NASA security program to protect people, property, and information.

P.2 APPLICABILITY

a. This NASA directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NASA directive is applicable to all other personnel completing work through Space Act Agreements or Memorandums of Agreement/ Understanding, those assigned or detailed under the Intergovernmental Personnel Act, partners, cooperative agreements, and visitors.

P.3 AUTHORITY

The National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. § 2473(c)(1)

P.4 APPLICABLE DOCUMENTS

a. 5 Code of Federal Regulations Sections 731.202 and 731.501

b. E-Gov Act of 2002, Public Law 107-347, 44 U.S.C. Ch 36

c. Executive Order 10450 of April 17, 1953 (as amended)

d. Executive Order 12968 of August 2, 1995

e. Federal Acquisition Regulation Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel

f. Federal Information Processing Standards Publication 201 (FIPS 201)

g. Homeland Security Presidential Directive 12 (HSPD-12)

h. NASA Procedural Requirements (NPR) 1600.1, Security Program Procedural Requirement
i. NPR 1382.1, NASA Privacy Procedural Requirements

j. NPR 2810.1, Security of Information Technology

k. NASA Grant Information Circular (GIC) 06-02, September 22, 2006

l. NIST Special Publication (SP) 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

m. NIST SP 800-104, A Scheme for PIV Visual Card Topography

n. Office of Management and Budget (OMB) Memo M-05-24, of August 5, 2005, "Implementation of Homeland Security Presidential Directive (HSPD) 12 -Policy for a Common Identification Standard for Federal Employees and Contractors"

o. Privacy Act of 1974, U.S. Public Law 93-579, 1974.

p. X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, v2.5 16 OCT 2006

P.6 CANCELLATION

a. NPR 1371.2, Processing Requests for Access to NASA Installations or Facilities by Foreign Nationals or U.S. Citizens Who are Reps of Foreign Entities.

b. NASA Memorandum (NM) 1600-46, Security Identification System Requirements.

c. NM 1600-50, Photo Identification Color-Coding Requirements.

d. NM 1600-52, Personal Identity Verification Policy and Procedures.

Dr. Woodrow Whitlow, Jr.
Associate Administrator for Mission Support Directorate

CHAPTER 1. Introduction

1.1 Reserved

1.2 Identity, Credential, and Access Management (ICAM) Governance

1.3 Scope

1.3.1 The policies and procedures identified within this document define the approved processes for NASA to manage personal identities and the issuance to those identities of NASA Personal Identity Verification (PIV) credentials. This NPR also establishes the policy for the management of other types of NASA credentials – visitor badges and temporary badges. Non-PIV logical access tokens are not covered in this document. The policies and procedures for vetting an identity are covered in NM 1600-96 NASA Personnel Security. Usage of this vetted and bound identity for physical access is covered by NPR 1600.1 and logical access by NPR 2810.1 Security of Information Technology. The policies and procedures necessary to properly manage identity, credential, and access management (ICAM) services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration are covered in NPR 2841.1 Identity, Credential, and Access Management Services.

CHAPTER 2. Roles and Responsibilities

2.1 Overview

2.1.1 All NASA employees and contractor employees as well as NASA tenants and contractors for NASA tenants will be required to comply with this Directive. Commercial or private entities and their contractors (all tiers) and employees needing physical or logical access per Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA), Commercial Space Launch Act (CSLA) agreements also must comply with this directive. The Assistant Administrator, Office of Protective Services (OPS), is the system owner of all systems used to manage identities and to issue NASA PIV credentials. The Assistant Administrator, Office of Protective Services also has overall responsibility for ensuring uniformity of credential issuance policies and procedures throughout the Agency. All NASA organizational components shall adhere to the policies and procedures herein and promulgate implementing regulations, as required, consistent with the policies and procedures set forth herein. Center Directors, through their Center Office of Protective Services (OPS), supported by the Center Office of the Chief Information Officer (OCIO), Center Human Resources Office (HRO), Procurement Office, and other offices as necessary, shall ensure that local operating procedures and execution conform to the policies and procedures herein. The following roles and responsibilities are established to conform to the guidelines prescribed in NIST Special Publication 800-79-1 "Guidelines for the Accreditation of Personal Identity Verification Card Issuers."

2.2 Reserved

2.3 Center Roles and Responsibilities

2.3.1 The Center PIV Issuing Facility (PIF) Manager - The Center PIF Manager shall be a federal civil servant employee serving as the Center Chief of Security (CCS), Chief of the Protected Services Office (PSO), or equivalent role designation at a Center or a designee of the chief. The PIF Manager supports the PCI AIMO at the Center level. The PIF Manager oversees the identity management and credential management program implementation at the Center and documents the operations and procedures of the Center's identity management and credential management programs. The PIF Manager or designee validates the individuals at the Center who perform the roles of PIV requester and PIV sponsor. The PIF Manager or designee monitors training status of all persons fulfilling PIV identity management and credential management roles at the Center. The PIF Manager identifies and designates individuals to fill the roles of PIV authorizer, PIV Enrollment Official, and PIV Issuance Official. The PIF Manager is responsible for ensuring that all personnel, services, facilities, and/or equipment necessary to carry out the policies in this document at the Center are procured, updated, and provided reliably. The PIF Manager is responsible for ensuring that Credentials are produced and issued in accordance with the requirements in this document. The PIF

Manager or designee reviews I-9 document discrepancies and provides determinations for the acceptance of the documents.

2.3.2 PIV Applicant - Per FIPS 201-1, the PIV Applicant is the individual to whom a PIV credential needs to be issued. The PIV applicant shall be a prospective or current NASA employee (e.g., either a civil servant or a federal contractor), requiring access to NASA facilities and/or IT resources. The PIV applicant is responsible for providing demographic data for the PIV request, for being photographed and providing biometrics during enrollment and providing valid identity documents during enrollment and issuance. The PIV applicant signs for acceptance of the PIV credential and acknowledgement of related responsibilities for proper handling and use of the PIV credential once issued, as defined in Appendix C: Subscriber Agreement. The PIV applicant shall not perform any role in the creation of their identity and issuance of their credential with the exception of the role of requester for the purpose of renewal and reissuance.

2.3.3 PIV Requestor - The role of PIV requestor is not defined in FIPS 201-1. The PIV requestor is the individual who submits the necessary information on behalf of the PIV Applicant to initiate the process of requesting a PIV credential. The PIV requester shall be an individual from one of the following categories depending on the applicant affiliation:

a. Manager or authorized administrator of a specific NASA program or contract;

b. NASA Human Resources (HR) for prospective or current NASA employees;

c. NASA grant provider for grantees; or

d. International Visits Coordinator (IVC) for foreign nationals.

2.3.3.2 The PIV requester creates the initial request for a PIV applicant to receive a NASA federal credential.

2.3.4 PIV Sponsor - The PIV Sponsor is defined in FIPS 201-1 as the individual who substantiates the need for a PIV credential to be issued to the PIV Applicant, and provides sponsorship to the PIV Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant. The PIV sponsor shall be a NASA civil servant employee or a California Technical Institute Jet Propulsion Laboratory employee who establishes and endorses the need for a relationship between the applicant and NASA. The PIV sponsor designates and approves the Position Risk Determination (PRD). The PIV sponsor modifies, as necessary, incorrect or missing information in the credential issuance request. The PIV sponsor is an individual from the identified entity for the following applicant affiliation:

a. HR specialist for NASA civil servant employees;

b. Contracting Officer's Technical Representatives (COTR) or other federal civil service technical personnel responsible for work requirements for contractors;

c. Grants technical official for grantees;

d. Authorizing official or designee for Economy Act, Space Act, CSLA or CSCA agreements, or

e. The NASA civil servant program or project manager who requires the foreign national to access NASA facilities or IT systems.

2.3.5 PIV Enrollment Official - The PIV Enrollment Official covers a portion of the duties that are described in FIPS 201-1 for the PIV Registrar. The PIV Enrollment Official is the entity responsible for identity proofing of the PIV Applicant and ensuring the successful collection of the information necessary to confirm employer sponsorship, bind the applicant to their biometric, and validate the identity source documentation. The role of PIV enrollment official shall be performed by personnel from the Center Security Office. The PIV enrollment official collects, establishes, and verifies identity information of an applicant. The PIV enrollment official captures the biometrics and photograph of the applicant. The PIV enrollment official checks I-9 identity source documents for authenticity, captures copies and/or scans of the I-9 documents, compares the name and demographic data in the PIV credential request and the I-9 documents, and determines whether any discrepancies exist on an applicant’s I-9.

2.3.6 PIV Authorizer - The PIV Authorizer covers the portions of the PIV Registrar duties described in FIPS 201-1 that are not done by the PIV Enrollment Official. The PIV Authorizer provides the final approval for the issuance of the PIV credential to the Applicant. The PIV authorizer shall be a Federal employee. The PIV authorizer shall hold no other role in the identity management or credential issuance process for a given identity. The PIV authorizer shall hold no role other than applicant in the issuance of their credential. The PIV authorizer must be trained in adjudication by an accredited provider of adjudication training. The PIV authorizer reviews the PIV credential request, the PIV sponsor's endorsement, and confirms that I-9 validation and biometrics capture has occurred. The PIV authorizer coordinates checks for existing background investigations. The PIV authorizer coordinates requests for background investigations as necessary. The PIV authorizer coordinates background investigation submissions through the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigation Processing (e-QIP), as required. The PIV authorizer adjudicates the results of the fingerprint check and adjudicates background investigation results. The PIV authorizer records results of the fingerprint check and background investigation results and approves or denies NASA PIV credential issuance. The authorizer records the final result of

adjudicated investigations, and when the adjudicated investigations are favorable, authorizes continued use of an issued PIV credential as required in NM 1600-96 NASA Personnel Security.

2.3.7 PIV Investigation Reviewer - The PIV Investigation Reviewer is an optional role within NASA that is not described in FIPS 201-1. The PIV Investigation Reviewer may be a civil servant or a designated contractor. The PIV investigation reviewer shall NOT be allowed to authorize production or issuance of a NASA PIV credential. The PIV Investigation Reviewer assists the PIV authorizer with:

a. reviewing the PIV credential request, the PIV sponsor's endorsement, and confirming that I-9 document validation occurred and that biometrics capture has occurred;

b. coordinating checks for existing background investigation;

c. coordinating requests for background investigations as necessary;

d. coordinating background investigation submissions through the OPM e-QIP, as required;

e. reviewing the results of the fingerprint check and background investigation as they are received;

f. recording results of the fingerprint check;

g. updating PIV applicant information when necessary; and

h. rejecting a PIV applicant’s application when necessary.

2.3.8 PIV Issuance Official - The PIV Issuance Official is defined in FIPS 201-1 as the PIV Issuer. The PIV Issuer is the entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuance Official is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials. The role of PIV issuance official shall be performed by personnel authorized by the Center Chief of Security. The PIV issuance official issues NASA PIV credentials to approved PIV applicants. The PIV issuance official responsible for submitting the order for the PIV credential to be encoded and printed with the appropriate identity information. The PIV issuance official verifies the applicant's identity through visual and biometric verification prior to issuing the NASA PIV credential. The PIV issuance official ensures the applicant has selected a Personal Identification Number (PIN). The PIV issuance official secures, receives, accounts for, and handles un-issued NASA PIV credential stock and NASA PIV credentials that are no longer authorized for use due to termination of

employment, badge expiration, contract or grant expiration, or expiration of need for the badge by a foreign national.

2.4 Separation of Duties for the PIV Role

2.4.1 Per the requirements specified in FIPS 201-1, the roles of PIV Applicant, PIV Sponsor, PIV Enrollment Official, and Issuer are mutually exclusive for each individual PIV credential. No individual shall hold more than one of these roles in the identity proofing and registration process for a single PIV credential. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

2.4.2 Individuals and entities assigned to the PIV Enrollment Official, PIV Authorizer, PIV Investigation Reviewer, PIV Issuance Official, and the PIV Digital Signatory roles shall meet the applicable requirements established by the appropriate accreditation process.

2.5 Training

2.5.1 Overview training is required for each role identified in this document to ensure a general and uniform understanding of the NASA policies and procedures for identity management. Training is required for each role of the following roles in the PIV issuance process: PIV Enrollment Officer, PIV Authorizer, PIV Investigation Reviewer, and PIV Issuance Official. Re-certification is required each year to ensure training is up-to-date and conducted with the most recent system updates. Training records are maintained by the SATERN computer based training system or subsequent/succeeding system(s). End-user training is provided on an as-required basis to Agency personnel. Technical and user training are available through computer based training or on-site "desk-side coaching" sessions on an as-needed basis. Day-to-day operations' training is provided to system operators and administrators to ensure that they have a thorough understanding of the systems and related components being managed.

2.6 Privacy

2.6.1 NASA shall ensure that applicant information and systems which facilitate identity management processes are managed consistent with:

a. NPD 1382.17, NASA Privacy Policy

b. NPR 1382.1, NASA Privacy Procedural Requirements

c. Homeland Security Presidential Directive 12 (HSPD-12)

d. OMB memorandum 05-24

e. Privacy Act of 1974, U.S. Public Law 93-579

f. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36)

2.6.2 As prescribed by the Office of the Chief Information Officer, NASA shall conduct and maintain a Privacy Impact Assessment (PIA) of the identity management program. NASA shall conduct and maintain PIAs for all systems which are used in the identity management processes and include Personally Identifiable Information

(PII) and Information in Identifiable Form (IIF) of the applicant. The NASA System of Records Notice (SORN) shall be updated and maintained to reflect the disclosure of information to other Federal agencies.

2.6.3 Only individuals with a legitimate need to access the systems in which an applicant's IIF is stored and maintained shall be allowed to access those systems. It is the responsibility of each Center to limit who has legitimate access to those identity management systems they maintain. NASA shall ensure privacy of applicant information is sustained through all steps of identity management including enrollment and issuance. PIV credential issuance facilities shall provide an electromagnetically opaque sleeve that assists in protecting against unauthorized contactless access to information stored in the PIV credential.

2.6.4 The Privacy Act Statement shall be posted in every enrollment and issuance location, on the applicable NASA website, and provided in pre-enrollment packages to the applicant. The Privacy Act Statement covers:

a. use of collected PII;

b. protections provided to ensure the security of PII; and

c. Effects of partial disclosure and non-disclosure of information by the applicant.

2.6.5 The Subscriber Agreement shall be posted in every enrollment and issuance location, on the applicable NASA website, and provided in any pre-enrollment packages to the applicant. The Subscriber Agreement covers:

a. authorized uses of the PIV credential;

b. authorized uses of the PKI certificates and services provided with the PIV credential;

c. notification requirements for the applicant; and

d. requirements to return the PIV credential at the end of use.

2.6.6 The following documentation shall be made available, at the request of the applicant:

a. complaint procedures;

b. appeals procedures for those denied a PIV credential or whose PIV credential is revoked; and

c. sanctions for employees violating NASA privacy policies.

2.6.7 All notifications provided during identity management processes shall be conducted in a secure manner, ensuring applicant information is secure at all times. Centers shall establish

procedures for notifying applicants when their PII is lost, damaged, becomes corrupt, or stolen.

2.6.8 NASA shall normally discipline any individuals violating the privacy requirements established in this chapter in compliance with NASA guidelines established in NPR 1382.1 NASA Privacy Procedural Requirements.

2.6.9 NASA shall archive and safeguard all stored data pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules. Identity files are maintained for a minimum of two (2) years after an individual's relationship with the Agency has ended. NASA may, at its discretion, increase but not reduce the time that identity source documents have to be maintained. The data to be maintained in electronic or hard copy includes:

a. completed and signed PIV credential request;

b. information related to the applicant's identity source documents;

c. results of the applicant's background check;

d. copies of the applicant's photograph; and

e. any additional documents used in the enrollment and issuance process.

3.1 Reserved

3.2 Chain of Trust

3.2.1 A chain of trust is followed which simultaneously captures the biometrics, photograph, identity source documents, and background investigation of the applicant, and can be tied to the identity of that applicant at any point in the identity management process.

3.2.2 The credential is released to the applicant only after completion of the chain of trust by verifying that the biometric information contained on the credential matches the applicant.

3.3 NASA Credential Types

3.3.1 NASA uses both PIV credentials and non-PIV credentials. Access is granted via NASA PIV Credentials. NASA PIV Credentials allow physical only, logical only, and both physical and logical access to resources at NASA. Each NASA credential is linked to an established identity and must go through the appropriate issuance steps as outlined in this chapter. See NPR 2810.1, Security of Information Technology for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. NASA visitor badges are NASA non-PIV badges which allow only physical access to NASA Centers. For short-term visitors, Centers are authorized to issue Center-specific badges (i.e. NASA non-PIV badges) for physical access to that Center based on a risk-based determination documented as part of the permanent record. Requirements for the characteristics of these credentials, including printing elements and technology capabilities are detailed in Chapter 5, Characteristics of NASA Badges.

3.3.2 NASA PIV credentials shall be issued to all persons who have been deemed as needing access to NASA Centers, Facilities, and IT systems and resources for a period exceeding 179 days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners, as well as non-NASA tenants in NASA facilities. NASA PIV credentials shall be issued to both U.S. citizens and foreign nationals. NASA PIV credentials shall be issued following the complete identity-proofing, registration, and issuance processes defined in this document for the management of identities of all new and current employees, contractors, and affiliates including foreign nationals. NASA PIV credentials shall be issued only after completion of a FBI fingerprint check and submission of a background investigation which must be a National Agency Check with inquires (NACI) background investigation at a minimum. NASA PIV credentials shall have an expiration date set for a period not to exceed 5 years from the Card Production Request (CPR) generation date. NASA PIV credentials shall not be issued to individuals holding a federal PIV credential issued by another federal entity or to individuals holding a PIV-I credential issued by an organization whose PIV-I credentials conform to the federal PIV-I standard. Exceptions to this policy may be made only when the exception has been formally documented and approved via the process described in section 1.4 of this document. The exception request must specifically explain why a non-NASA credential is not usable in the NASA ICAM services.

3.3.3 Any person (i.e., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals such as volunteers, guest researchers, interns, grantees, etc.) who will be affiliated with NASA and its Centers or Facilities for a period of 179 days or less shall be issued a NASA non-PIV badge (i.e., a NASA temporary badge). The 179-day period begins the first day of affiliation and ends 179 calendar days later regardless of the work schedule. If an individual's affiliation extends past 179 days in a 365-day period, the individual must be issued a NASA PIV credential if the individual is a NASA employee (either a civil servant or a federal contractor employee). All other individuals (volunteers, guest researchers, interns, grantees, etc.) may be exempted from the 179-day limit on use of a NASA non-PIV badge consistent with risk-based assessments by CCS/CPS. Issuance of NASA non-PIV badges requires at minimum a favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4 of section 3.5, On-Site Enrollment and Issuance Procedures. Escort requirements for individuals with a NASA non-PIV badge shall be based on risk-determination by the Center Chief of Security.

3.3.4 NASA visitor badges may be issued to individuals requiring access to a NASA Center for a period not to exceed 29 days in any single visit and not more that a cumulative total of 29 days in a 365-day period. Individuals needing access beyond 29 days must be issued a NASA Non-PIV Temporary badge. Issuance of NASA visitor badges requires completion of steps 1-3 of section 3.5, Enrollment and Issuance, and shall include capture of the visitor's photograph section 3.5.4, Step 4: Enrollment Process. Visitors requiring access to a NASA Center for more than 5 days shall undergo a minimum of a National Crime Information Center name query prior to receiving a visitor badge. Escort requirements for individuals with visitor badges shall be based on risk-determination by the Center Chief of Security.

3.3.5 NASA Center-specific badges may be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials, NASA non-PIV badges, and NASA visitor badges. All NASA Center-specific badge Templates shall have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA Center-specific badges shall be issued upon completion of a favorable adjudication of a National Crime Information Center (NCIC) name query. Issuance of these badges shall be based on a risk-based access determination by the Center Chief of Security. NASA Center-specific badges may be issued to individuals who hold a PIV credential issued by another federal government agency or department if their current non-NASA PIV credential does not work at the NASA Center. This may include contractors from another NASA Center in the event that electronic verification of a need to be on the NASA Center is not available at a point of entry. Issuance of NASA Center-specific badges requires completion of steps 1-3 of section 3.5, On-Site Enrollment and Issuance Procedures, verification of a favorably adjudicated investigation, and capture of the individual's photograph, section 3.5.4, Step 4: Enrollment Process.

3.3.6 Logical access credentials and their usage are addressed by NPR 2810.1, Security of Information Technology and include but are not limited to username and password, RSA tokens, digital certificates.

3.4 Applicant Types

3.4.1 NASA employees are Federal civil servants employed and paid by NASA. NASA Employees also includes individuals employed and paid by another entity but working for NASA under an Intergovernmental Personnel Act (IPA) agreement. NASA Employees include all Non-Appropriated Funds Instrumentality (NAFI) Employees. These employees shall be issued a Civil Servant badge with the affiliation of NAFI.

3.4.2 NASA contractors are individuals working under contract with the responsibility to perform activities for NASA.

3.4.3 NASA grantees are individuals who are working under grant and performing activities for and/or at NASA Centers and Facilities.

3.4.4 Detailees are either Federal employees from other-Federal Agencies, or U. S. military personnel, or non-Federal employees working at NASA through an Intergovernmental Personnel Act (IPA) assignment. Any badges issued to a Detailee shall be designated with an affiliation of "NASA" and shall appear as a federal employee badge. The Center PIF Manager shall coordinate with the Center Human Resources Office (HRO) to validate investigative and suitability results for detailees from other-agency partners. Government employees from other departments and agencies who do not have a PIV credential issued by their Agency or Department, and require identity verification and access at NASA, may be issued a NASA PIV credential or NASA temporary badge by NASA.

3.4.5 International Partners are individuals, working for agencies or organizations of foreign governments, foreign education institutions, foreign companies, or international organizations, engaged in a program of international cooperation in work done pursuant to a Space Act Agreement as defined by NPD 1050.1H, Authority To Enter Into Space Act Agreements. A signed international agreement must first be in effect for international partners to receive a foreign national NASA PIV credential.

3.4.6 Tenants are individuals who require physical access to a NASA facility but do not work directly for NASA. There may or may not be a "Formal" agreement associated with a tenant (example: Credit Union). The tenant may require logical access to certain NASA applications. A tenant may work for another government agency as either a civil servant or contractor and may have a PIV badge from this other agency. Tenants include those entities and their contractors and employees under Economy Act, Space Act, Commercial Space Competitiveness Act (CSCA) or Commercial Space Launch Act (CSLA) agreements are those individuals needing physical or logical access based on the above authorities. The tenant may work for a company that is leasing space on a NASA facility but does not work on a NASA-related project.

3.4.7 Transients are individuals (i.e., construction workers, club members, childcare drop off/pickup, delivery drivers, retirees, Center transits, and others approved by Center Chiefs of Protective Services/Security) who requires intermittent access for 180 days or more. Transients shall be issued Center-specific badge.

3.5 On-Site Enrollment and Issuance Procedures for NASA Credentials

3.5.1 Step 1: Credential Request - A requester completes a credential request within IdMAX for an applicant. The requester submits the request to the sponsor via IdMAX. The information submitted includes the following:

a. Name of the applicant;

b. Date of Birth of the applicant;

c. Position of the applicant;

d. Contact information for the applicant;

e. Name of the requester;

f. Organization of the requester; and

g. Contact information for the requester.

3.5.2 Step 2: Sponsorship - The sponsor validates the receipt of the request from the requester. The sponsor reviews the data in the Request. The sponsor reviews the Position Risk Determination. The sponsor approves or denies the request, establishing the need for a relationship between the applicant and NASA, and the applicant's need for a PIV credential

3.5.3 Step 3: Check for Background Investigation - The authorizer or Investigation Reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review the Office of Personnel Management (OPM) and other federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

a. If the applicant has an investigation on file or in progress that meets the investigative and reciprocity requirements, the authorizer submits the request to the Enrollment Official and the applicant proceeds to enrollment, section 3.5.4, Step 4: Enrollment Process, for capture of enrollment data with flat fingerprints.

b. If no investigation is on file or in progress, the authorizer coordinates initiation of an invitation in the OPM e-QIP for the applicant to complete the appropriate background investigation form and authorizes the Enrollment Official to obtain the applicant's flat and rolled fingerprints, I-9 documents, and photograph.

3.5.4 Step 4: Enrollment Process - The Enrollment Official validates the receipt of the request from the authorizer. The sponsor advises the applicant that they must appear in-person before the Enrollment Official and present two forms of identity source documents in original form. The applicant appears in-person before the authorized Enrollment Official and presents two forms of identity source documents in original form per Form I-9, one of which must be a

Federal or state issued picture identification. The Enrollment Official inspects the source document for authenticity and validates the source document through visual or electronic scrutiny and, when necessary, with the authority or entity which issued it.

a. Enrollment fingerprints - The applicant's fingerprints are captured. If the applicant currently has a favorable background investigation on file or in progress, only flat fingerprints are required to be captured. If no background investigation is on file or in progress, both flat and rolled fingerprints are required to be captured. In cases where there is difficulty in collecting fingerprints due to damage, injury or deformity, NASA shall perform authentication using asymmetric cryptography for authentication. The facial image collected from the applicant during enrollment can also be used for authenticating badge recipients covered under Section 508 of the Rehabilitation Act.

b. Enrollment Photograph - The applicant's photograph is captured which must include the entire face, from natural hairline to the chin, and may not be obscured by dark glasses, coverings, etc. The facial expression shall be neutral (non-smiling) with a closed mouth. Eye patches that do not obscure an excessive portion of the face need not be removed. Individuals with temporary eye patches should be issued a temporary badge until such time as the patch is no longer necessary and an un-obscured full-facial photograph can be captured. Waivers for religious reasons may be obtained by written application to the AA for Protective Services who may refer the matter for a recommendation to a NASA Headquarters Access Appeals Panel.

c. Enrollment I-9 Documentation - The Enrollment Official obtains and maintains a legible photocopy or scan copy of the original I-9 documentation. Any document that appears invalid (e.g., absence of security hologram, or other known security features, on a State issued driver's license; security features on a birth certificate or passport; smeared ink, etc.) is to be rejected by the Enrollment Official and reported to the proper authority for review. Photocopies of rejected documents are to be made and retained for a period not to exceed one year, or until any appeal process is completed. I-9 documents that do not pass electronic examination, if available, are rejected and another approved I-9 document must be obtained and subjected to electronic scrutiny. In the event the applicant is required to provide documentation to resolve discrepancies or omissions in data collected, the Enrollment Official shall review the information with the applicant as necessary. The information submitted by the applicant shall be used to update the applicant identity record.

d. Enrollment Subscriber Agreement - The Enrollment Official provides the applicant with the Subscriber Agreement, Appendix D, Subscriber Agreement, and obtains an electronic signature of the applicant attesting to their reading and acceptance of the Subscriber Agreement.

3.5.5 Step 5: Adjudication Process - If no investigation is on file or in progress, the fingerprints captured during enrollment are submitted to OPM with a request for a background investigation. The authorizer receives the results of the fingerprint check. If the fingerprint check comes back with a status of unclassifiable, the Center may use the results of a NCIC to process the PIV credential request. The authorizer makes a determination based upon receipt of the fingerprint check results, or evidence of an acceptable existing background investigation (as found in section 3.5.3, Step 3: Check for Background Investigation), if the applicant is eligible to receive a PIV credential If the adjudication of the available background investigation is favorable, the

authorizer submits a PIV credential issuance request to authorize the creation and issuance of a PIV credential In instances where a badge is to be issued, the authorizer notifies the sponsor and requester that the badge issuance has been authorized. Final adjudication of the record is performed in compliance with NASA personnel security policies.

3.5.6 Step 6: Badge Production Process - The Issuance Official validates the receipt of the issuance request from the authorizer. The Issuance Official submits a request for badge printing if the badge is to be printed remotely at a commercial facility or a shared service provider. The necessary information is included in a batch card creation request. The initialized and printed badges are returned to NASA and forwarded to the appropriate Issuance Officials where the credentials shall be held in a secure location. If the badge is to be produced locally, the Issuance Official prints the identity information onto the card and compares the photo to the identity database. The badge shall be encoded with the identity and biometric data of the applicant. The encoded badge shall be tested. The applicant shall be notified when the badge has been successfully encoded.

3.5.7 Step 7: Issuance Process - The applicant appears before the Issuance Official, who establishes whether the badge was printed in a batch job, previously printed on-site, or is to be printed on-site: If printed in a batch job or previously printed on-site, the Issuance Official obtains the card stock from storage. If the badge is to be printed on-site, the Issuance Official obtains a blank badge from storage, verifies the identity of the applicant against the database, and prints the badge. The Issuance Official checks the printed badge to verify the identity of the applicant, conducts a biometric match and encodes the badge with an applicant entered PIN number. Upon completion of the badge printing and encoding, the badge is officially released to the applicant. An approved electronically shielded badge holder shall be offered to the applicant in order to protect the badge and the privacy of information on the badge.

CHAPTER 4. Foreign Nationals

4.1 Overview

This NPR shall be the authoritative source for all identity management requirements specific to foreign nationals at NASA including, but not limited to, visit coordination, access approval, escort procedures, fingerprint checks and background investigations for permanent, temporary, and visitor access. A foreign national is any person who is not a United States citizen. Lawful permanent residents (LPR) are not United States citizens, however they are entitled by law to most of the same rights and privileges (and are held to the same accountability for such) as U.S. Citizens. Therefore, LPRs shall have identity proofing and vetting accomplished in the same manner as U.S. Citizens.

4.1.1 Foreign nationals shall complete the following steps prior to being issued a NASA PIV credential:

a. Obtain visit approval for the visit or assignment;

b. Sponsorship for the foreign national shall be determined. If a foreign national is not under a contract where a COTR has been officially designated, the foreign national shall provide information directly to their visit/assignment host, and the host shall fulfill the duties of the sponsor as required herein; and

c. Pre-visit identity vetting shall be conducted.

4.1.2 This Chapter outlines the requirements that NASA personnel shall follow in granting access by foreign nationals to NASA physical or information technology resources for any purpose other than a tour of facilities that is or would normally be conducted for the general public The sub-sections outline the processes, procedures and authorizations necessary to successfully obtain required access permissions in a timely manner. These requirements apply to foreign national civil servants, contractors, researchers, international partners as defined via International Space Act Agreements (ISAA), as well as high-level protocol visitors (HLPV), the news media, NASA sponsored J-1 Visas and visitors. Also included are the requirements for the processing of persons who have multiple citizenships and persons who are U.S. citizens working for foreign entities.

4.1.3 Questions regarding the receipt and processing of access requests for foreign nationals or NASA contractor or grantee foreign national employees or visitors, and the conduct of approved visits and other access shall be directed to the NASA Center or Component Facility International Visit Coordinator (IVC). In the event that the criteria for processing a specific foreign national cannot be accommodated within one of the scenarios documented here, an exception request can be submitted to the NASA Office of Protective Services for review and approval (see section 1.4 of this document). Suggestions for process improvements are welcome and should be addressed to the NASA Office of Protective Services, Headquarters Office, Washington, DC 20546.

4.2 NASA Foreign National Access Policy and Related Requirements

4.2.1 NASA partners extensively with its foreign aeronautical, scientific, and technical counterparts in support of broad Agency objectives and program goals. Frequently, this working relationship results in the need for foreign national access to physical and information technology resources. Visits also facilitate acquisition of information about foreign programs of interest to NASA, and provide other benefits to the U.S. Government. All visits and other approved access will be conducted in conformance with Agency and national policies and regulations, including U.S. national security, nonproliferation and foreign policies, and export control laws and regulations.

4.2.2 Visits and other access for the purpose of implementing a mutually agreed program or project must be conducted in accordance with the terms of the NASA/foreign partner program or project agreement, particularly the provisions in the agreement dealing with responsibilities of the parties and the transfer of data and goods. Discussion or other release of information by NASA personnel to a foreign national during a visit or other approved access that does not pertain to an agreed program or project must be limited to information which has been approved for release to the general public, i.e., unclassified, non-sensitive, and non-export-controlled.
Visits, assignments or IT access requests for foreign nationals from non-designated areas are coordinated and implemented at the Center through the IVC. Visits, assignments or IT access requests for foreign nationals from designated areas (see Office of International and Interagency Relations web page at http://oiir.hq.nasa.gov/nasaecp) are coordinated initially through the Center Export Control and the Center IVC, then shall be forwarded to NASA Headquarters External Relations, Export Control and Program Points-of-Contact (as necessary) for review and final approval. Only after final approval shall a foreign national be provided access to NASA physical or information technology assets.

4.3 Processing On-Site Visit Requests

4.3.1 SA Center or Component Facility IVC will directly receive and review all requests from, or on behalf of, foreign nationals for access to its buildings, installations, facilities or IT resources for any purpose. All foreign national access requests other than for public tour shall undergo an identity vetting process based on visit type, foreign national residency, and country affiliation. The Center IVC shall approve the requests for foreign nationals from non-designated countries. Requests for foreign nationals from designated countries shall be forwarded and approved by Headquarters Office of External Relations for review and approval before final approval by the Center IVC.

4.3.2 If the visit is for the purpose of gathering information or conducting discussions in technological areas that NASA considers sensitive (e.g., for proprietary, national security, or export control reasons), then the visit should be disapproved in the absence of a specific NASA programmatic interest. Requests

should be approved only to the extent the foreign national understands that discussions and information provided by the NASA representatives will be confined to information that has been previously approved for release to the general public. All identity proofing and vetting for foreign nationals from non-designated countries shall be performed at the Center. The requirement to forward all IT access requests to Headquarters is rescinded. This eliminates steps (thus time) in the process and does not create new processes for the Centers. All current Center review processes shall continue as they do now at each Center's discretion.

4.3.3 Only NASA civil servants or NASA contractors holding active PIV credentials shall be allowed to escort foreign nationals.

4.3.4 Centers shall accept the identity vetting of their peer Centers as a baseline requirement. Additional identity vetting may be required should access requirements change (e.g., if the foreign national needs privileged access or the IT Security Plan warrants a higher-level investigation).

4.3.5 A person with multiple citizenships, all foreign, and one is from a Designated country, shall be processed as from a Designated country.

4.3.6 NASA Center personnel will apply the credentialing processes and standards as provided in the OPM Memorandum of July 31, 2008, Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 to non-U.S. nationals who work as employees or contractor employees including those who require long-term logical or physical access to NASA facilities. For individuals who are non-U.S. nationals in the United States or a U.S. territory for 3 years or more a background investigation (i.e. NACI or equivalent) must be initiated after employment authorization is appropriately verified through e-Verify (or immigration status is appropriately verified for those individuals not working for NASA through the USCIS Systematic Alien Verification for Entitlements (SAVE) system).

a. For foreign nationals in the U.S. or a U.S. territory for less than three years, NASA Center personnel will delay the background investigation until the individual has been in the U.S. or a U.S. territory for three years. In such cases, an alternative facility access identity credential may be issued as appropriate based on a risk determination. Before an alternative identity credential may be issued, the individual's employment authorization must be verified and an FBI fingerprint based criminal history check must be completed. Center personnel will request an FBI Investigations Files (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against SAVE. Some of these database checks may be requested directly from OPM or through automated tools such as NCIC and Visual Compliance

b. Centers shall perform additional database checks to determine if there are changes to the foreign national's identity status. These status checks may be performed separately or through an automated tool,

(1) Visual Compliance Unverified List

(2) Entities List

(3) Denied Persons List

(4) Debarred Parties List
(5) Specially Designated Nationals

(6) Terrorist database

4.3.7 Foreign national non-PIV credentials shall be issued for a maximum period of three years, date of visa/passport expiration, date of I-94/W expiration, or assignment end date, whichever comes first. Foreign nationals on visa waivers may have credentials issued for a period of three years, date of visa waiver expiration, date of I-94/W expiration, or assignment end date, whichever comes first. Foreign nationals on visa waivers will return their credential to the Center Security Office after each visit. Foreign nationals on visa waivers shall present their current passport/visa to the Center Security Office to retrieve their credential at the beginning of each visit. When a foreign national with a visa waiver needs to stay in the U.S. beyond the 90 days, they are required to provide the visa information to the Center IVC.

4.3.8 For foreign nationals in the U.S. greater than three years to receive a PIV credential, they MUST complete the SF-85/NACI or the SF-85P Public Trust (via e-QIP if the person has an SSN) or a paper copy of the background investigation can be mailed to OPM if the foreign national does not have an SSN.

4.3.9 Foreign nationals with PIV credentials will be allowed to access all Center perimeters without additional identity proofing or vetting. Additional access (physical or IT) shall be determined by the physical or IT asset owner and coordinated through the Center's International Visits Coordinator prior to the foreign national's arrival at the receiving Center. For Centers who use Physical Access Control Plans, they must be valid and accurate. Technology Transfer Control Plans (TTCP), as required by Export Control, must be updated as necessary. Physical access beyond the perimeter (escorted or not) is at the discretion of the Center Security Office. If required, the Security Office will issue a Center credential for access purposes.

4.3.10 IT Remote Access ONLY will be enabled by the IVC after approval in IdMAX. There is no Federal requirement for Identity vetting for foreign national Remote IT Only Access. NASA collects basic information that allows us to approximate level of assurance for user ID/password and/or RSA token access to IT assets. When the capability is available to perform in-person identity verification

through trusted agents, Remote IT ONLY access users will undergo the identity verification process. The worker's sponsor in coordination with the IT system owner shall determine whether identity vetting is warranted based on the security requirements of the system documented in the IT System Security Plan. If identity vetting is required, the investigation should be conducted and recorded. If fingerprints are captured, assure the following:

a. Where fingerprints are captured at a location other than the Center Security Office, the transmission of those fingerprints to the Center Security Office must be from a valid law enforcement agency or other accredited fingerprint provider.

b. To ensure a chain of trust, the fingerprint cards shall be delivered to the Center Security Office by the entity that took the fingerprints.

c. Any foreign national having access to NASA data must provide a written certification that they fully understand and will adhere to NASA rules and regulations regarding the integrity and confidentiality of NASA data being accessed. This certification may be in the form of completed NASA IT Security training or a signed document signaling understanding of IT access requirements as outlined in NPR 2810.1. Either of these activities will satisfy the completion of NASA IT Security Training requirement prior to activation of IT access. Recertification must be performed annually.

4.4 Foreign National Request and Sponsor

4.4.1 The requester for a foreign national shall be a currently employed NASA civil servant or contractor. The sponsor shall be a NASA civil servant or a Jet Propulsion Laboratory (JPL) California Institute of Technology (Caltech) employee who is a U.S. citizen. The sponsor shall perform a risk assessment based on the status of the foreign national and the assets that the foreign national is to access. This information is necessary to determine the level of investigation or escort requirements that may be necessary while the foreign national is at a NASA facility.

4.4.2 To expeditiously process the request, the sponsor shall assure that the following information is provided to the IVC:

(a) Full legal name

(b) Date of birth

(c) Place of birth

(d) Residence (including country)

(e) Citizenship(s)

(f) Passport and visa information (including visa waiver)

(g) Social security number (if one is available)

(h) Foreign national number (if no SSN is available)

(i) Contact information

(j) Sponsor name

(k) Physical access requirements

(l) Information technology access requirements (on-site and/or remote)

(m) Export control data access requirements (including license requirements)

(n) NASA affiliation (civil servant, contractor, partner, etc.)

(o) Work description (includes purpose, program, authority or other information that allows approvers to make an informed decision. The more information provided, the quicker the request can be processed.)

4.5 Requirements and Risk Review

4.5.1 The IVC shall be a currently employed NASA civil servant or contractor. The IVC shall review the foreign national request and perform the following:

(a) Confirm sponsorship.

(b) Review with the Project Office and sponsor the access requirements, work description, dates of visit, assignment or length of IT access request, and sponsor's risk assessment. Review and approve Technology Transfer Control Plan (TTCP) which is described in NPR 2190.1 NASA Export Control Program.

(c) Review with the Center Security Office broader security issues, including counterintelligence, counterterrorism, threats against national security, and pertinent data about country of origin (designated and high threat countries). Determine appropriate level of investigation relative to physical and information technology access requirements. Determine circumstances whereby escort only status shall be applied. Review and approve TTCP, if accessing NASA physical resources.

(d) The Center Security Office shall begin the background investigation based on visit type, foreign national residency, and country affiliation and commensurate with risk levels outlined in the TTCP.

(e) The Counterintelligence/Counterterrorism Office shall perform their background investigation (as needed) and report results back to the Center Security Office.

(f) With the Export Control Office, review export control issues to ensure information being exchanged does not violate export control laws, and make risk-based determination on access protocols. Review and approve TTCP, if accessing NASA information technology resources.

(g) With the Information Technology Security Manager (ITSM), review information technology access requirements (on-site and remote), and make risk-based determination on access protocols. Review and approve TTCP, if accessing NASA information technology resources.

(h) With the Public Affairs Office (if the individual is a member of the press or a public affairs member with a foreign space agency), review access requirements and protocols.

(i) With Headquarters External Relations (if the individual is part of the NASA Exchange Visitor Program), obtain endorsement from the appropriate Enterprise/Functional Office at NASA Headquarters. Review and approve TTCP for physical and information technology access.

(j) Confirm all Center authorizations have been received.

4.6 Authorization

4.6.1 The IVC shall coordinate and provide final approval for identity vetting, physical access, and information technology access for foreign nationals from non-designated countries. In circumstances where the IVC is not a civil servant with adjudicator authority, the Center Security Office's PIV authorizer shall provide the final approval.

4.6.2 Centers or Programs may specify restrictions regarding physical or information technology (IT) access privileges or escort requirements that are more restrictive than those documented in this NID.

4.6.3 If a foreign national will be accessing multiple Centers, it will be incumbent on the foreign national's sponsor and Center IVC to collaborate with affected Centers to determine which access and escort restrictions apply at which Center.

4.6.4 If a foreign national will be accessing an information technology resource from multiple locations (including remote), it will be incumbent on the foreign national's sponsor and system owner to determine how that access will be provisioned at multiple locations.

4.6.5 The IVC shall coordinate input for identity vetting, physical access, and information technology access for foreign nationals from designated countries. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP, the IVC shall forward all information to the Headquarters Export Control Office, External Relations Desk Officer and (as required by the Program), the Headquarters Program Point-of-Contact for review and approval. The Headquarters Export Control Office, External Relations Desk will then forward the approval back to the IVC who will issue the final approval. In circumstances where the IVC is not a civil servant with adjudicator authority, the Center Security Office's PIV authorizer shall provide the final approval.

4.7 Implementation

4.7.1 Once all approvals have been received, the IVC shall report back to the foreign national's sponsor the terms and conditions of the on-site assignment. The sponsor shall assure implementation of the foreign national's access credentials. The sponsor shall assure that the foreign national's access requirements as documented in the TTCP are adhered to throughout the foreign national's on-site assignment.

4.7.2 If a foreign national is denied access (all or in part), the IVC shall provide the sponsor with the Appeals process.

4.7.3 If a foreign national application has been outstanding for longer than 30 days from initial request, the IVC shall follow-up with Center or Headquarters personnel to determine the cause(s) for the delay. Applications outstanding for longer than 30 days from initial request shall be escalated to the Agency Identity Management Official (AIMO) for resolution.

4.8 Variations Based on Type of Onsite Visit Request

4.8.1 If a foreign national is working for NASA at an overseas location, to the extent practicable, all aspects of "Processing On-Site Visit Requests" shall be performed. In instances where a NACI cannot be rendered, a determination shall be made between the Program Manager and the Chief for Center Security performing the investigation as to the level of investigation required. The foreign national will be given a physical access credential commensurate with the level of investigation performed and access requirements. Non-PIV credentials shall expire at the end of the program/project or contract term. Investigation status information shall be updated annually. Access to information technology resources will be administered with a non-PIV credential.

4.8.2 If a foreign national is working for NASA under an International Space Act Agreement (ISAA) and requires periodic access to NASA facilities, the foreign national shall be processed in accordance with procedures for “Foreign National Works at Overseas NASA Location.”

4.8.3 If a foreign national is coming to NASA periodically as an accredited news media representative, the IVC shall coordinate with the Center Public Affairs Office to obtain requisite information. Once the IVC has determined that agreement has been reached on requirements, the IVC shall coordinate with the Chief for Center Security as to the level of investigation required. The foreign national will be given a physical access credential commensurate with the level of investigation performed and access requirements. Only non-PIV credentials shall be issued. Investigation status information shall be updated annually. Access to information technology resources will be administered with a non-PIV credential.

4.8.4 If a foreign national is coming to NASA for a High-Level Protocol Visit (HLPV), the IVC shall coordinate with the Center Protocol Office to obtain requisite information. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP (if necessary), the IVC shall forward all information to the Headquarters External Relations Desk Officer and Export Control (if TTCP was created) for review and approval.

4.8.5 Under the provisions of 22 CFR Part 62, and as approved by the Department of State, NASA is authorized to conduct an exchange visitor program and can authorize foreign nationals to be assigned to NASA installations on J-1 exchange visitor visas. NASA has authority to sponsor two exchange visitor categories: Research Scholars and Government Visitors. The regulations regarding these categories and the exchange visitor program in general can be found at 22 CFR 62.1 through 62.90.

4.8.6 If a foreign national is coming to NASA as part of the NASA Exchange Visitor Program (J-1 Visa), the IVC shall coordinate with the Center sponsor to obtain requisite information and to assure that the foreign national is part of an existing International Space Act Agreement (ISAA) partnership. Once the IVC has determined that agreement has been reached on requirements, including completion of the TTCP (if necessary), the IVC shall forward all information to the Headquarters External Relations Desk Officer and Export Control (if TTCP was created) for review and approval.

4.8.7 No NASA funding is provided to the foreign national under the NASA Visitor Exchange Program. All funding must come from the foreign sponsor or from personal funds, and NASA must assess if the funds being made available are sufficient to sustain the individual for the period of the assignment. NASA provides office space and supplies, and, if necessary and approved pursuant to NPR 2810.1, computer and network access.

4.9 Variations Based on Visitor Characteristics

4.9.1 If a foreign national has dual citizenship, the IVC shall determine if one of the countries of citizenship is the United States (U.S.). If one country of citizenship is the U.S., the identity vetting process shall follow that for a U.S. citizen. The physical access credential provided the individual will be one for U.S. citizen (PIV or Proximity). Physical access restrictions shall be determined and agreed to by the Center Security Office and the sponsor. If the foreign national has dual citizenship for two foreign countries, the IVC shall determine the countries of citizenship. If both countries are non-designated, the foreign national identity shall be vetted as non-designated. If any one country is designated, the foreign national identity shall be vetted as designated.

4.9.2 U.S. citizens go through the same identity vetting process regardless of their employer (U.S. or foreign). All U.S. citizens are bound by the same Federal laws. If a U.S. citizen is found to have committed espionage (i.e., giving/selling data to a foreign entity), they will be prosecuted as a U.S. citizen. The minimum identity vetting process for a full-time civil servant or contractor working at a NASA facility is the National Agency Check with written Inquiries (NACI).

4.9.3 Physical access permissions are granted by the Center Security Office. IT access permissions are granted by IT system owners. A higher level of risk is associated with having access to either physical or IT resources, and whether export controlled data is involved. All conditions contribute to whether access should be granted and whether a higher level identity vetting requirement is necessary (e.g., access to restricted areas, mission essential infrastructure, and sensitive or classified information).

4.9.4 Lawful permanent residents (LPR) shall undergo the same identity vetting as U.S. citizens. LPR identity records will be maintained in IdMAX versus the Foreign National Management System (FNMS). The credential provided to LPRs shall be the blue stripe LPR credential. This credential shall conform to the color coding requirements for Zone 15 described in NIST Special Publication 800-104. The letters “LPR” shall be displayed superimposed on the NASA logo in the lower right hand corner of the front of the credential. In the event an LPR chooses not to complete the SF 85/85P required for issuance of a NASA PIV credential, then the LPR shall be issued an LPR proximity credential only following the requirements described in section 3.4.6.

4.10 Identity Vetting Requirements Based on Length of U.S. Residence

4.10.1 Foreign nationals who have been resident in the U.S. for less than three years shall undergo the following identity vetting process:

(a) A Visual Compliance database check that reveals no violations or derogatory information

(b) Reciprocity of vetting performed by Customs and Border Patrol officials at the Port of Entry FBI fingerprint check

4.10.2 The foreign national proximity credential (foreign national Blue) shall be issued. The term of issue will be the length of assignment or time in which the foreign national is resident in the U.S. for three years whichever is shorter.

4.10.3 Foreign nationals who have been resident in the U.S. for three years or greater shall be asked to complete the SF 85/85P so that an appropriate OPM investigation may be conducted. Foreign nationals are eligible for issuance of a NASA PIV credential upon favorable adjudication of a NACI investigation or higher. In the event a foreign national chooses not to complete the SF 85/85P required for full identity vetting, the Center Security Office shall require a minimum annual revalidation of the Visual Compliance database search along with an NCIC check. The foreign national blue credential shall be issued based on the results of the identity vetting revalidation. The term of issue will be the length of assignment.

4.11 Identity Vetting Requirements and Credential Type for Visits, Temporary Employees, and Permanent Employees

4.11.1 For foreign national visits of 29 days or less, the following is required:

a. A Visual Compliance database check that reveals no violations or derogatory information;

b. Reciprocity of vetting performed by Customs and Border Patrol at the port of entry; and

c. FBI finger print check (foreign national must be escorted until favorable finger print results are returned). Foreign nationals may then be issued a Center-specific temporary foreign national visitor credential.

4.11.2 For foreign national temporary employees whose assignments will last 30 to 179 days, the same procedures as described in section 4.11.1 apply. A non-PIV foreign national credential may be issued for this assignment category.

4.11.3 For foreign national Permanent Employees whose assignments will last 180 days or more, the following conditions are applicable:

a. If foreign national has resided in the U.S. for 36 months or greater, may complete SF 85/85P to initiate an OPM investigation and upon completion and favorable adjudication may be issued a NASA PIV credential.
b. If foreign national has resided in the U.S. for less than 36 months, must undergo identity vetting described in section 4.10.1 and may be issued a non-PIV foreign national credential.

4.12 Processing Information Technology (IT) Remote Only Requests

4.12.1 In accordance with the Federal Information Systems Management Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, and NPR 2810.1, NASA has established security requirements and procedures to assure an adequate level of protection for NASA Information Technology (IT) systems that includes the appropriate screening of individuals having access to NASA IT systems. The level of reliability checks and/or investigations is dependent on the sensitivity of the information to be handle and the risk of magnitude of loss or harm that could be caused by the individual.

4.12.2 Foreign national access to "limited privileged" IT systems shall be allowed only if the foreign national is involved in a program member under an International Space Act Agreement (ISAA). The sponsor shall verify that an ISAA is in place. The sponsor has accountability for assuring the security of IT system data being accessed by the foreign national.

4.12.3 IT Remote Access ONLY will be enabled by the Requestor's sponsor. There is no Federal requirement for Identity vetting. NASA collects basic information that allows an approximation of IT access assurance of user ID/password and/or RSA token access. When the capability is available to perform in-person identity verification through trusted agents, Remote IT ONLY access users will undergo the identity verification process. The worker's sponsor in coordination with the IT system owner shall determine whether identity vetting is warranted based on the security requirements of the system documented in the IT System Security Plan. If identity vetting is required, the investigation should be conducted and recorded. If fingerprints are captured, assure the following:

4.12.4 Where fingerprints are captured at a location other than the Center Security Office, the transmission of those fingerprints to the Center Security Office must be from a valid law enforcement agency or other accredited fingerprint provider. To ensure a chain of trust, the fingerprint cards shall be delivered to the Center Security Office by the entity that took the fingerprints.

4.12.5 Any foreign national having access to NASA data must provide a written certification that they fully understand and will adhere to NASA rules and regulations regarding the integrity and confidentiality of NASA data being accessed. This certification may be in the form of completed NASA IT Security training or a signed document signaling understanding of IT access requirements as outlined in NPR 2810.1. Either of these activities will satisfy the completion of NASA IT Security Training requirement prior to activation of IT access. Recertification must be performed annually.

4.13 Escort Requirements

4.13.1 Identity vetting requirements established here do not preclude each Center Security Office from enacting their requirements regarding access to the Center, buildings, or other secured areas. Access requirements for foreign nationals are outlined in the TTCP.

4.13.2 It is incumbent on the IVC to work with the Center Security Office to determine escort requirements while the foreign national is located at the Center and to assure the foreign national sponsor understands and agrees to abide by those requirements.

CHAPTER 5. Characteristics of NASA Badges

5.1 NASA Credential Types

5.1.1 NASA PIV Credentials - The information on a NASA PIV credential exists in both visual printed and electronic forms. The NASA PIV credential shall be equipped with technologies that allow for physical access through a proximity antennae and logical access through an imbedded chip.

a. NASA PIV credentials contain the following security and distinguishable features on the front of the card:

(1) holographic overlay; and

(2) Smart chip.

b. NASA PIV credentials have the following printed vertically on the front of the badge:

(1) the photograph of the applicant in the top left corner;

(2) the legal name of the applicant, printed below the applicant photograph;

(3) two badge expiration dates; one located in the upper right corner (MMM YYYY format), and the second to the right of the applicant photograph, below the Agency identifier, and over the Agency logo (YYYYMMMDD format);

(4) the NASA Agency identifier logo;

(5) the affiliation of the applicant, to the right of the applicant photograph and over the Agency logo;

(6) the NASA Agency identifier, to the right of the applicant photograph, below the affiliation, and over the Agency logo;

(7) the unique badge identification number, below the NASA Agency identifier and the affiliation color band;

(8) solid color band across the middle of the badge, over the full name with the color determined by the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type; and

c. NASA PIV credentials have the following printed horizontally on the back of the badge:

(1) return address;

(2) applicant height;

(3) applicant eye color;

(4) applicant hair color; and

(5) bar code.

5.1.2 NASA Temporary Badge - Temporary badges may be equipped with technologies that allow for physical access through a proximity antennae and/or logical access through an imbedded chip. Temporary badges shall not resemble the NASA PIV credential.

a. Temporary badges have the following printed vertically on the badge:

(1) the silhouette of a vertical space shuttle on the right side of the badge, located above the solid affiliation color area;

(2) the photograph of the applicant in the top left corner;

(3) the legal name of the applicant, printed below the applicant photograph;

(4) the NASA Agency identifier, to the right of the applicant photograph;

(5) the designation of the issuing Center, below the applicant name;

(6) the unique badge identification number, below the NASA Agency identifier;

(7) the badge expiration date that is 180 days or less from the date of Center/Facility affiliation, below the badge identification number;

(8) solid colored lower section based on the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type; and

(9) OPS mailing information on the bottom front of the badge.

b. Temporary badges have the following printed horizontally on the back of the card:

(1) return address;

(2) applicant height;

(3) applicant eye color; and

(4) applicant hair color.

5.1.3 NASA Visitor Badges - Centers may prescribe the topology for visitor badges as long as they meet the following criteria:

a. the photograph of the applicant;

b. the legal name of the applicant;

c. the full name of the issuing Center; and

d. the full badge expiration date that is 29 days or less from the date of Center/Facility affiliation.

5.1.4 NASA Center-specific badges - Center-specific badges shall not contain technologies that allow for physical (beyond recognition by Center security) or logical access. Center-specific badges shall contain the following printed information:

a. the photograph of the applicant;

b. the legal name of the applicant;

c. the name of the issuing Center (Center name may be common abbreviation, e.g., ARC, DFRC, et alia, as appropriate).

5.1.5 Visual Color Coding for Employee Type - NASA PIV and temporary badges use colored markings on the badge to determine the affiliation of the badge holder. NASA PIV credentials use a color band through the name of the applicant and temporary badges use a colored lower section below the photograph and including the name. Unless otherwise indicated, the color being used is for both NASA PIV and temporary badges as described in Table 5.1.5:

Table 5.1.5

Employee Type	Color Coding
Federal Employee	A plain white color band
Contractor Employee	Contractors shall have a green color band. On the right side of the band is a "G" inside a white circle to assist individuals with visual impairment in recognizing the green color.
Contractors at the NASA Jet Propulsion Laboratory (JPL)	Contractors at the NASA Jet Propulsion Laboratory (JPL) who are United States (U.S.) citizens shall be recognized by the addition of a solid silver color below the green contractor color band.
Interagency Personnel Agreement (IPA) Employee	A plain white color band. The lower right corner on the front of the badge the label "IPA" shall appear in black letters.
Foreign Nationals	Foreign National badge characteristics take precedence over all other affiliation characteristics. Foreign National badges have a light blue color band. On the right side of the band is a "B" inside a white circle to assist individuals with visual impairment in recognizing the light blue color. Foreign National badges have a light blue color border around the applicant photo.
International Partners	International Partners shall have a flag of the applicant's country of citizenship in the lower right corner of the badge in addition to the light blue Foreign National color band and border.
Emergency Response Officials	Emergency Response Officials shall be recognized by a Red stripe containing the words "Emergency Response Official" on the bottom of the badge in Zone 12 per the requirements of NIST Special Publication 800-104. The back of an Emergency Response Official (ERO) badge contains text stating their position as ERO and access permissions after verification of the badge holder's identity.

5.1.6 Emergency Response Officials (ERO) Badges - Emergency Response Office badges may be issued only to the following persons:

a. EROs to include individuals who are:

(1) Continuity of Operations (COOP) and Continuity of Governance (COG) personnel associated with continuity of operations at a NASA Center or an alternate operating site during emergency/crisis situations. This includes only those persons who are members of the Emergency Relocation Group (ERG) and their respective support staff and Emergency Operation Center (EOC) personnel who are appropriately certified and trained.

(2) Disaster response personnel for each facility who possess National Incident Management System (NIMS) training or professional certifications.

b. Personnel to be deployed to support the NASA National Response Framework (NRF) Emergency Support Function (ESF) Annexes. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

c. NASA Special Agents, NASA Security Police or Security Officers who have graduated from NFLET and members of the NASA Inspector General (IG) staff who are sworn law enforcement officers.

d. Center Protective Services and Security Staff who provide support, or other security functions for emergency/contingency operations as deemed necessary by the Center Chief of Protective Services/Center Chief of Security so long as they possess the above mentioned NIMS training or professional certifications

e. Center Directors, Deputy Center Directors, and Directors of Center Operations and their deputies.

5.1.7 Personnel who will be fulfilling support duties will be issued NASA PIV credential, without the ERO designation, to facilitate verification of identity and ease movement through the various checkpoints. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

5.1.8 Table 5.1.8 details the color coding for temporary badges:

Table 5.1.8

Employee Type	Color Coding
Contractor	Temporary contractors shall be recognized by a dark blue lower section. Temporary contractors at JPL who are U.S. citizens shall be recognized by a silver lower section with red lettering for the "JPL" Center designation.
Foreign Nationals	Temporary Foreign Nationals shall be recognized by an orange lower section.
Detailees	Temporary Detailees shall be recognized by a green lower section.
Interns and Grantees	Interns and grantees shall be recognized by a temporary badge with a purple lower section.

5.1.9 Badges for Press Corps – The press corps shall be recognized by the word "PRESS" printed vertically down the right side of the temporary badge. U.S. press corps shall be further recognized by a brown lower section. Foreign national press shall contain all characteristics from the foreign national color coding as detailed in Table 5.1.5.

5.2. NASA PIV Credential Data

5.2.1 Data printed on a NASA PIV credential consists of:

a. Name (Last Name, First name and middle initial);

b. Photo;

c. Affiliation (Civil Servant, Detailee, Contractor, Grantee, or Foreign National, etc.);

d. Badge Expiration Date;

e. Badge Number consisting of a three (3) digit Center code plus six unique digits and printed as a number on the front, and a 3x9 bar code on the back;

f. Height, Eye and Hair Color;

g. Agency Card Serial Number; preprinted and used for tracking card stock; and

h. Issuer Identification consisting of a six character department code, the agency code for NASA, and a five-digit issuing facility number.

5.2.2 The digital data stored on the NASA PIV credential supports physical and/or logical access use, encryption and signing capability, and provides security and authentication protection for the PIV credential and PIV credential holder.

a. Card Holder Unique Identifier (CHUID) - The CHUID is used by access control applications, and is the only data that is accessible through both the contact and contactless interfaces. Applications can read this data without any action from the badge holder. The CHUID is composed of:

(1) Federal Agency Smart Credential Number (FASC-N) composed of:

(2) NASA Agency Code;

(3) System code identifying the original issuing Center

(4) A credential number; and

(5) PIV credential holder's UUPIC.

(6) Expiration Date

b. Digital Certificates

(1) PKI X.509 certificates are used for authentication of the PIV credential, and digital signing, encryption and authentication of the PIV credential holder.

(2) Credentials used for logical access have a certificate for PIV credential authentication. Additional certificates are loaded based on the duties and needs of the PIV credential holder.

c. Biometrics (typically fingerprints of the right and left index fingers) are stored as minutiae templates that represent a specific biometric, but cannot be reverse-engineered to re-create an image of that biometric.

d. Digital Representation of Printed information - Certain items printed on the front and back of the card are stored on the chip as a security and authentication measure including name, affiliation, organization, badge expiration date, agency card serial number, and issuer identification.

e. Photograph - The facial image used in creating the photo printed on the front of the badge is stored in the badge. A facial image is required, and obscuring headwear may not be worn for the photograph.

f. The Personal Identification Number (PIN) is used to secure and protect the electronic data stored on the PIV credential. The PIN is used by the PIV credential holder to allow applications to access data, and as part of the authentication process. It is stored in a secure section of the smart card, separate from the rest of the PIV credential digital data. All PIV credential data, with the exception of the CHUID, require the PIV credential holder to enter their PIN before an application can either access or use the data. The PIN is a minimum of a six digit number selected by the PIV credential holder and written to the PIV credential during finalization. It is not stored in the identity management system and should not be written down or otherwise recorded by the PIV credential holder. The PIV credential is automatically locked after no more than 15 consecutive tries of entering an invalid PIN. Section 6.7, PIV Credential PIN Reset details requirements for resetting a PIN.

5.3. The Universal Uniform Personal Identification Code (UUPIC)

5.3.1 UUPIC System Management - The UUPIC system shall be owned by OPS, working in concert with the OCIO, to ensure proper functioning, assignment, use, and protection of the UUPIC system. OPS is responsible for administrative identity management in the UUPIC system. The UUPIC system shall be treated as a high confidentiality, integrity, and reliability system. Access to the UUPIC system shall be controlled by two-factor authentication, firewalls, and encryption techniques. The UUPIC may not be used as a login identifier or user account name for any information systems, databases, web sites, et al. The UUPIC system may not be used for identification purposes outside those needed for positive identification of individuals within information systems without the concurrence of the Agency Identity

Management Official, with the exception of account initiation in the identity management system. System owners requiring access to the UUPIC system must submit a signed Service Level Agreement (SLA) and/or Memorandum of Understanding (MOU) to OPS.

5.3.2 Approval to Access the UUPIC System - The system owner requiring access to the UUPIC system must submit a signed SLA/MOU to the ICAM Logical Access Management team detailing the purpose for accessing the UUPIC system. The ICAM Logical Access Management team will work with the system owner to ensure proper documentation, and authority to access the UUPIC system. The ICAM Logical Access Management team will make a recommendation to approve or disapprove UUPIC system access to the Agency Identity Management Official. In the event of a denial for UUPIC access, the requesting system owner may appeal by sending a letter, along with the SLA/MOU, to OPS and OCIO. OPS and OCIO will respond with a final decision within 60-days of receipt of the appeal.

5.3.3 UUPIC Characteristics - UUPICs will only be issued through the population of seed data (name, Social Security Number or Foreign National visitor number for foreign nationals without a Social Security Number, and date of birth) into the UUPIC database. This information is required for all NASA civilians, contractors, partners, and virtual IT system users. Any request for a UUPIC will be initiated via an approved work flow method. The UUPIC database will auto-populate the IdMAX, IDMS and EPACS upon returning a UUPIC number. The reliable assignment of the UUPIC to persons uses at least two unique attributes, in addition to name attributes, from the documents as specified in the Department of Justice Form I-9, Employment Verification Data. The Agency directory is used as the UUPIC repository for general access to the UUPIC number. UUPIC numbers will be issued in random sequence, consistent with NASA policy and meet the following requirements:

(a) Is a nine-digit numerical code without any significance as to the characteristics of the individual;

(b) Is displayed as a set of 3 x 3 x 3 numbers, for example: 123 456 789; and

(c) Cannot be reverse engineered based on other data contained in the UUPIC application.

5.3.4 UUPIC Usage - The UUPIC will serve as a replacement for the Social Security Number by providing a unique identifier that can serve as a data point across NASA information systems. Therefore, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, web site, et al. With the exception of account initiation in the Identity Management System, use of the UUPIC for any identification purposes outside those needed for positive identification of individuals across and only within information systems is prohibited without the consent of the Agency Identity Management Official. The UUPIC may never be posted on any

Internet accessible web site. Any deviation from this policy must be coordinated with OPS through OCIO in advance. Requests for a UUPIC must be initiated via the approved workflow method. The UUPIC database will auto-populate the appropriate identity management systems upon returning a UUPIC number. UUPIC numbers are stored internally along with the first, middle and last names, and other information necessary to uniquely associate the UUPIC with a person.

CHAPTER 6. PIV Credential Management Lifecycle

6.1 PIV Credential Inventory

6.1.1 Ownership. A PIV credential is not personal property. It is the property of the U.S. Government. All personnel are responsible for appropriately safeguarding issued credentials, immediately reporting the loss or false use of a PIV credential, challenging uncredentialed personnel, notifying the proper authority of a name change, properly displaying a PIV credential when on Center, and surrendering a PIV credential upon resignation, retirement, or the direction of the issuing authority.

6.1.2 Reciprocity. PIV credentials issued by other Departments and Agencies shall be accepted for the purpose of establishing the identity of the individual.

6.1.3 Misuse. Forging, falsifying, or allowing misuse of a PIV credential or other forms of NASA identification in order to gain unauthorized access to NASA physical and logical resources is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than 1 year, or both, and may further result in termination of employment and access to NASA resources.

6.1.4 Production. Printing or finalizing of credentials shall only be performed by approved personalization service providers and shall be shipped directly to a Center by the service provider.

6.1.4 Stock protection. Unprinted or unfinalized PIV credentials shall be shipped directly to a Center by the PIV credential manufacturer. The PIV credential Issuing Facility Manager or other appropriate authority shall designate a point of contact who is responsible for receipt of, signing for, and inventory and storage of PIV credential stock. PIV credential stock shall be accessible only by authorized personnel and maintained in a secure manner, pursuant to Section 6.2, PIV Credential Storage and Handling. PIV credential stock shall be monitored through the use of a log which includes, at a minimum, the date of check in, the date of check out, and the name of the person(s) performing the PIV credential stock check-ins or check-outs.

6.2 PIV Credential Storage and Handling

6.2.1 Credentials are stored using the following minimum requirements:

a. Properly identified and treated as “controlled material” for inventory;

b. Segregated from classified materials, firearms, ammunition, or currency; and stored in secure area protected by guard(s), key lock(s), and/or card reader(s).

6.2.2 Credentials which are lost, stolen, or unaccounted while in storage shall be reported immediately to the PIV credential Issuing Facility Manager and in a timeframe not to exceed 24 hours after discovery. PIV credential details, including PIV credential identification numbers and status, will be reported to the NEACC within 24 hours of discovery in order to update the card management system. The PIV credential Issuing Facility Manager shall forward a report outlining all pertinent facts to the OPS Security Management Division Director no later than 2 days after receiving reports of the lost, stolen, or unaccounted for credentials.

6.2.3 A defective PIV credential shall be identified, reported, and delivered to the Core Technical Team. The Issuance Official shall record the defective PIV credential identification number and the defective status in the PIV credential storage log. A new PIV credential shall be created following Sections 3.4.4 of this document.

6.2.4 All PIV credential encoding failures shall be reported to the Core Technical Team within five days of discovery and include the identification number, failure description, and any other pertinent information.

6.2.4.1 PIV credential encoding failures include:

a. Rejection by a card reader or machine;

b. Error message(s) during encoding of the PIV credentials; and

c. PIV credential is not recognized by physical or logical access control systems (PACS or LACS).

6.2.4.2 If the PIV credential becomes defective as a result of the encoding failure, refer to Section 6.2.3 of this NID.

6.3 Final Adjudication and Subsequent Investigation

6.3.1 Final adjudication may occur at any time in the process. Final adjudication should be conducted within 20 days of receipt of the background investigation. Final adjudication may occur after the issuance process has completed and an applicant has received a PIV credential following favorable fingerprint check results. Upon receipt of the background investigation, the authorizer shall adjudicate the results of the background investigation to determine if the results of the investigation are favorable or unfavorable. This adjudication shall be documented and performed in accordance with OPM policy.

6.3.2 When background investigation results are favorable, the authorizer shall update the applicant's record to reflect favorable adjudication of the background investigation; and the background investigation indicator in the PIV credential data model shall be set to indicate background investigation completion. When background investigation results are unfavorable, the authorizer shall update the applicant's record to reflect unfavorable determination of the background investigation result. The authorizer shall revoke all physical and logical access rights associated with the PIV credential. The PIV credential shall be immediately confiscated. The requester and sponsor shall be notified of the denial decision.

6.3.3 The PIV credential holder shall be provided the opportunity to appeal, pursuant to NM 1600-96 NASA Personnel Security. If the PIV credential holder does not appeal or appeal is denied, the confiscated PIV credential shall be terminated.

6.4 PIV Credential Usage: Display, Protection and Proper Usage

6.4.1 NASA shall provide an electromagnetically opaque badge holder selected from an approved products list in order to physically protect the badge and electronically protect the information contained in the badge. Other holders found on the approved products list may be purchased by a Center at their discretion. Such holders are the responsibility of the purchasing Center to ensure that they are electromagnetically opaque. The badge must be properly displayed and worn at all times while the bearer is on a NASA Center or Component Facility. They shall be worn above the waist on the outermost garment; and with the side with the photograph visible. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, decals, etc.) on a PIV credential (or any alteration or modification thereof) is not allowed.

6.4.2 PIV credentials shall be accepted at all Centers for access to public areas and IT resources at that Center. Access to non-public areas at each Center shall be handled on an as-needed basis in compliance with the policies established by that Center for access to facilities and/or IT resources. Silver JPL contractor PIV credentials shall be accepted at all NASA Centers. Contractor PIV credentials from another Center may be accepted following a risk-based decision at the visited Center. Tenant credentials and foreign national PIV credentials will only be accepted at the Center from which they were issued. Foreign national PIV credentials from other Centers must be accompanied by an approved visit request.

6.4.3 NASA temporary badges shall only be used for access to the Center or facility from which it was issued. NASA temporary badges may be used for access to secure NASA computer systems and networks. Policies for temporary access to NASA IT resources are addressed by NPR 2810.1.

6.4.4 The visitor badge shall only be valid for the term issued, pursuant to section 3.4.6, NASA Visitor Badges. The visitor badge shall be returned at the end of the visit and individuals issued a visitor badge shall be escorted by NASA PIV or NASA temporary badge holders based on risk-determination at the Center.

6.4.5 A Center Chief of Security may establish Center-specific temporary badges for the following purposes:

a. Providing access for relatives or next of kin requiring access to wellness facilities (child care, health care, etc.);

b. To provide visual verification in the absence of electronic verification for PIV credentials issued by other federal agency and department; and

c. Recognition of retirees and other individuals previously affiliated with NASA (such as ex-astronauts) who no longer require access for official NASA business.

6.4.6 PIV credential usage requirements related to logical access are established in the NASA Subscriber Agreement, provided to and signed by the applicant for:

a. Authorized uses of the PIV credential; and

b. Authorized uses of the PKI Certificates and Services provided with the PIV credential.

c. Additional usage requirements for logical access credentials are established in NPR 2810.1, Security of Information Technology.

6.4.7 The background investigations associated with the issuance of the Common Access Card (CAC) by DOD have been determined by OPM to be equivalent to the background investigation requirements for issuing a PIV credential. The DOD Transition CAC (tCAC) satisfies HSPD-12 as a PIV compatible credential and shall therefore be accepted as an appropriate identity credential for DOD personnel working on NASA facilities. The tCAC does not identify that the individual is authorized to access NASA facilities. Centers shall continue to issue a NASA Center-specific badge that reflects the individual's authorization to access the Center. This differentiates the DOD employee working at a Center from the one at home on leave. PIV credentials issued by other Federal Government Agencies shall be accepted for the purpose of identity verification at a Center. Access shall be granted to the facility using a NASA Center-specific badge or the PIV credential with a card reader to establish granted access rights.

6.5 PIV Credential Renewal

6.5.1 Credential renewal shall occur prior to PIV credential expiration and facilitate replacement of the PIV credential without the need to repeat the full registration process. PIV credential holders may apply for a renewal starting six weeks prior to the expiration date on their PIV credential. The PIV credential holder shall coordinate with the sponsor, who ensures personnel records are accurate and current before the issuance of a new PIV credential. The old and/or expired PIV credential is to be collected and destroyed at the time of renewal pursuant to section 6.14, PIV Credential Destruction. If warranted, the authorizer shall approve the renewal and coordinate the request for a new background investigation to be performed.

6.6 PIV Credential Re-issuance

6.6.1 The old PIV credential shall be revoked, pursuant to Section 6.8, PIV Credential Revocation for the following conditions and the applicant shall undergo the entire registration and issuance process. PIV credential re-issuance shall occur when the PIV credential:

a. has reached its expiration date;

b. has been compromised;

c. is lost, stolen, or damaged; or

d. requires a change in printed information (name change, etc.) or employee status.

6.6.2 NASA PIV credentials shall not be re-issued for individual transferring from one Center to another.

6.6.3 PIV credential holders that have officially changed their name must submit a request for a reissuance of their PIV credential. The PIV credential hold shall be required to reenroll and provide

approved I-9 documentation that reflects the name change prior to enrollment occurring and issuance of the new PIV credential.

6.7 PIV Credential PIN Reset

6.7.1 Credentials that are disabled or locked-out due to a maximum of 15 consecutive invalid PIN entry attempts shall have their PIN reset. It is the responsibility of the PIV credential holder to arrange for a PIN reset to occur. Biometric verification of the applicant's biometrics to the biometrics stored on the card shall occur prior to the PIV credential being returned to the applicant. PIN reset does not require the reissuance of a PIV credential.

6.8 PIV Credential Revocation

6.8.1 Credentials shall be revoked under the following conditions:

a. exit on duty;

b. change in need for access;

c. termination of employment

d. unfavorable fingerprint check or background investigation determinations; or

e. death of the PIV credential holder.

6.7.2 Revocation of a PIV credential shall result in the following:

a. the PIV credential holder's relationship shall be set to "inactive";

b. the PIV credential shall be returned and terminated; and

c. notification shall be provided to the sponsor of the PIV credential revocation.

6.9 Lost and Stolen Credentials

6.9.1 Lost and stolen credentials shall be reported to the PIV credential Issuing Facility Manager within 24 hours of discovery of the loss/theft. The PIV credential holder shall, within five business days of reporting the loss/theft, appear in person at the badging office and provide their Social Security Number (SSN) or Foreign National Management System Identification number (FNMSID) to verify loss/theft of the PIV credential and be issued a new PIV credential. The lost/stolen PIV credential shall be revoked and/or disabled, cancelling all certificates and access privileges of that card. The identity of the PIV credential holder itself will remain active, as only the card is disabled. The PIV credential holder shall be required to undergo a PIV credential re-issuance, Section 6.6 PIV Credential Re-issuance. Until the new PIV credential is created, the PIV credential holder shall obtain a visitor or temporary PIV credential and NPR 2810.1, Security of Information Technology for logical access credentials.

6.9.2 It is the responsibility of NASA Centers to establish policy for the handling of multiple lost and stolen Credentials. Centers may adopt one of the below methods for managing PIV credential holders who report their PIV credential as lost or stolen on multiple occasions. The following list is not comprehensive and additional methods may be chosen by the Center:

a. Allow for the replacement of two (2) Credentials after which the PIV credential holder must undergo awareness training for each subsequent lost PIV credential prior to receiving the PIV credential; or

b. Implement a lost/stolen PIV credential form which requires signature of the PIV credential holder's manager, sponsor or other appropriate individual(s).

6.10 Forgotten Credentials

6.10.1 It is the responsibility of NASA Centers to establish policy for the handling of forgotten credentials. Centers may adopt any number of the below methods for managing PIV credential holders who forget their PIV credential. The following list is not comprehensive and additional methods may be chosen by the Center:

a. Require the PIV credential holder to retrieve the PIV credential;

b. Allow issuance of a visitor PIV credential to the PIV credential holder with verification of identity through an I-9 document such as a driver's license; or

c. Suspend the forgotten PIV credential until the PIV credential holder appears in the badging office with the forgotten PIV credential for it to be activated.

6.11 PIV Credential Suspension

6.11.1 Credentials shall be set to "suspended," temporarily disabled, when the PIV credential has been misplaced and the PIV credential holder knows the current location of the PIV credential. Lost or stolen credentials shall be handled pursuant to section 6.9, Lost and Stolen Credentials. The PIV credential holder shall appear at the badging office, no later than 24 hours after discovery of the misplacement, and file a report stating the PIV credential has been misplaced and the location of the PIV credential is known. Until the PIV credential is recovered or declared lost or stolen, the PIV credential holder shall obtain a visitor or temporary PIV credential. PIV credential holders shall report to the badging office within five business days of the original report to update the PIV credential status as being recovered, lost, or stolen. Lost and stolen credentials shall adhere to section 6.9, Lost and Stolen Credentials. Credentials that are found shall be set to "active" upon report of the PIV credential being found and visual confirmation of the PIV credential. Any temporary or visitor badge issued shall be returned.

6.12 PIV Credential Return

6.12.1 Credentials are to be returned to NASA once an individual's affiliation with NASA has ended. Credentials should be returned to the issuing authority no later than the last day of

association with NASA. The issuing authority shall be responsible for recording receipt of the PIV credential that are returned and properly storing the PIV credential until destruction. Credentials are not allowed to be kept as souvenirs. The responsibility of PIV credential return oversight shall be:
a. HR for NASA Civil Servant;

b. Contract Program Manager for Contractors;

c. Grant administrator for grantees; or

d. IVC for Foreign nationals.

6.13 PIV Credential Termination

6.13.1 Credentials returned to the badging office that do not meet any of the requirements previously established in this chapter and are to be terminated shall have all data, certificates, and access privileges invalidated, revoked, and/or disabled. Credentials that are to be terminated shall have their status set to “terminated” and a reason shall be supplied for the termination. Deactivation of a PIV credential and associated identity shall be completed within 18 hours of notification of the need for PIV credential termination. Terminated Credentials shall be destroyed following the requirements in section 6.14, PIV Credential Destruction.

6.14 PIV Credential Destruction

6.14.1 Credentials meeting the following criteria shall be destroyed:

a. expired credentials;

b. credentials discovered or located after being declared lost or stolen;

c. credentials that are damaged; and

d. terminated credentials.

6.14.2 Credentials shall be thoroughly destroyed using heavy duty cross cut shredders that are capable of smart card destruction, deposit into a burn bag for burning, or more rigorous methods.

APPENDIX A: DEFINITIONS

A.1 Access. The ability to obtain and use information and related information processing services; and/or enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances.

A.2 Access Control. The process of granting or denying specific access requests.

A.3 Accreditation. Formal declaration by a Designated Approving Authority (DAA) that an information technology system is approved to operate in a particular security mode for the purpose of processing CNSI, using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

A.4 Adjudication. A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources, is in the best interest of national security or efficiency of the Government.

A.5 **Asset.** A system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

A.6 Authorized holder. Anyone who satisfies the conditions for access to classified information in accordance with section 4.1 (a) in Exec. Order No. 13,526.

A.7 Authentication. (1) The validation and confirmation of a person's claim of identity. (2) The validation and identification of a computer network node, transmission, or message. (3) The process of establishing confidence of authenticity. (4) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to facilities and information systems.

A.8 Authorization. The privilege granted to a subject (e.g., individual, program or process) by a designated official to do something, such as access information based on the individual's need to know.

A.9 Center Chief of Security (CCS) - The senior Center security official who is responsible for management of the Center security program.

A.10 **Certification** - Used under two separate contexts in this NID:
a. A formal process used by the Certifying Official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

b. A formal process implemented at the CCS level to ensure a room, vault, or security container meets minimum structural and physical security attributes necessary to ensure adequate protection of CNSI. Certified Tempest Technical Authority (CTTA) - Designated official responsible for performing Tempest countermeasures cost and security analyses prior to the implementation of Tempest countermeasures.

A.11 **Component Facilities** - NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, NASA IV&V).

A.12 **Contractor** - For the purpose of this NID, any non-NASA entity or individual working on a NASA installation or accessing NASA information technology.

A.13 Credential. A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials are presented to access control systems in order to gain access to assets.

A.14 Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

A.15 **Escort** - The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, authorized topics of discussion, etc.

A.16 **Exception** - The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

A. 17 Executive Order (EO) - Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

A.18 **Foreign National** - A synonym for "Foreign Person" (see definite of Foreign Person below).

A.19 **Foreign Person** - Any person who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or any person who is not a protected individual as defined by 8 U.S.C. 1324b(a)(3). This also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the United States, as well as any international organizations, any foreign governments and any agency or subdivision of foreign governments (e.g., diplomatic missions).

A.20 **Grant Recipient** - Organization (Universities, nonprofits, etc.) or individual that has received official designation and funding to perform specific research on behalf of NASA.

A.21 I-9 document – one of the documents listed on the OMB Form I-9, Employment Eligibility Verification

A.22 Identity. The set of attributes that uniquely identify an individual for the purpose of gaining logical and physical access to protected resources and identification in electronic transactions.

A.23 Identity Proofing. The process for providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority (RA) when attempting to establish an identity or issue a credential.

A.24 Identity Verification. The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the credential or system and associated with the identity being claimed

A.25 Identity Vetting. A review of information about a person for possible approval or acceptance. In this document, a vetted person has been reviewed to determine eligibility for access to NASA physical and/or logical assets.

A.26 **International Partners** - Foreign nationals who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

A.27 **Lawful Permanent Resident (LPR)** - Replaces the term “Permanent Resident Alien (PRA)” - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information. (NOTE: LPR’s are not prohibited from accessing export controlled commodities but must still have a work related “need-to-know” and are still considered foreign nationals under immigration laws.
A.28 Logical Access. Access to information records, data, information technology systems and applications.

A.29 **NASA-Controlled Facility** - NASA Centers and individual facilities where access is controlled by issuance and mandatory use of photo-identification badges, armed security force personnel, and electronic access control systems to ensure only authorized personnel are admitted.

A.30 **NASA PHOTO-ID** - refers to the NASA photo-ID that has any number of imbedded and external technology capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded “smart card” chip.

A.31 **NASA National Agency Check** - Conducted electronically by NASA Security Offices of the files of the Federal Bureau of Investigation (including fingerprint files), Office of Defense Central Index of Investigations (DCII), the Office of Personnel Management, or other Government agencies, as appropriate. The files of the Bureau of Immigration and Customs Enforcement (BICE), the Central Intelligence Agency, and the U.S. State Department shall be reviewed, as available, when the individual is a resident alien or naturalized citizen of the United States.

A.32 **National Agency Check (NAC)** - The NAC is a search of the following four indices:

a. U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.

b. Federal Bureau of Investigation (FBI) Identification Division (FBIF) contains a fingerprint index and name file.

c. FBI Records Management Division (FBIN) contains files and records of all other investigations (e.g., background, criminal, loyalty, intelligence); and

d. Defense Clearance and Investigations Index (DCII) contains investigations, including criminal investigations, conducted on civilian and military personnel in the Department of Defense. (Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)

A.33 **National Agency Check and Inquiries (NACI)** - The NACI is a NAC that also includes written inquiries sent to employers, educational sources, law enforcement agencies, and references. The NACI is the minimum acceptable investigation for access to government facilities.

A.34 **Non-designated Country** - Country with which the United States has favorable diplomatic relations.

A.35 **Permanent Resident Alien (PRA)** - A non-U.S. citizen, legally permitted to reside and work within the United States and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the Federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information. (NOTE: PRA's are not prohibited from accessing export controlled commodities but must still have a work related "need-to-know" and are still considered Foreign nationals under immigration laws.)

A.36 **Protected Persons** - A non-U.S. citizen allowed into the country under "refugee," "displaced person," "religious," or "political" persecution status.

A.37 **Revocation.** The removal of an individual's eligibility to access physical or logical assets based upon an adjudication that continued access poses a risk to the Agency.

A.38 **Risk Acceptance** - An official acknowledgement by a management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate the risk.

A.39 **Risk Assessment** - A formal process whereby a project, program, or event is evaluated to determine the types and level of risk associated with its implementation.

Risk Management - A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

A.40 Smartcard. Credential issued with an individual's unique vetted identity information encoded and physically printed on the exterior and with embedded integrated circuits which can process data

A.41 Transient. A person (i.e., construction worker, club member, childcare frop off/pickup, delivery driver, retiree, Center transit, and others approved by Center Chiefs of Protective Serivces/Security) who requires intermittent access for 180 days or more.

A.41 **U.S. Person (non-U.S. Citizen)** - For the purpose of implementing protection and accountability under the ITAR; A person who is a lawful permanent resident (LPR) as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United , States. It also includes any governmental (federal, state, or local) entity. It does not include any foreign person as defined in this chapter.

A.42 **Visitor** - Any person who needs physical access to a NASA facility for less than 30 days.

A.43 **Waiver** - The approved continuance of a condition authorized by the AA for Protective Services that varies from a requirement and implements risk management on the designated vulnerability.

APPENDIX B: ACRONYMS

AA – Associate Administrator

AIMO – Agency Identity Management Official

BPL – Business Process Lead

C&A - Certification and Accreditation

CA – Certification Authority

CAC - Common Access Card

CBP – Customs and Border Patrol

CCS – Center Chief of Security

CHUID – Cardholder Unique Identifier

CIA - Central Intelligence Agency

CNSI – Classified National Security Information

CPR – Card Production Request

COG – Continuity of Governance

COOP – Continuity of Operations

COTR - Contracting Officer's Technical Representative

CSCA - Commercial Space Competitiveness Act

CSLA - Commercial Space Launch Act

CTTA – Certified Tempest Technical Authority

DAA – Designated Accreditation Authority

DCII - Defense Clearance and Investigations Index

DOD – Department of Defense

EOC – Emergency Operations Center

EPACS – Enterprise Physical Access Control System

e-QIP – Electronic Questionnaire for Investigation Processing

ERG – Emergency Relocation Group

ERO – Emergency Response Official

ESF – Emergency Support Function

FASC-N – Federal Agency Smart Credential Number

FBI – Federal Bureau of Investigation

FBIN – Federal Bureau of Investigation Records Management Division

FICAM – Federal Identity, Credential, and Access Management

FIPS – Federal Information Processing Standards

FISMA – Federal Information Systems Management Act

FNMS - Foreign National Management System

FNMSID – Foreign National Management System Identification Number

GAO - Government Accountability Office

GIC - Grant Information Circular

HLPV - High level protocol visitors

HR - Human Resources

HRO – Human Resources Office

HSPD – Homeland Security Presidential Directive

ICAM – Identity, Credential, and Access Management

ICE – Immigration and Customs Enforcement

ID – Identification

IdMAX – Identity Management and Account Exchange

IDMS – Identity Management System

IG - Inspector General

IIF - Information in Identifiable Form

IPA - Intergovernmental Personnel Act

ISAA – International Space Act Agreement

IT - Information Technology

ITAR – International Traffic in Arms Regulations

ITSM – Information Technology Security Manager

IV&V - Independent Verification & Validation

IVC – International Visit Coordinator

JPL – Jet Propulsion Laboratory

LACS - Logical Access Control System

LAM - Logical Access Management

LPR – Lawful Permanent Resident

MEI - Mission Essential Infrastructure

MOU – Memorandum of Understanding

NAC – National Agency Check

NAFA – Non-Appropriated Funds Activity

NEACC – NASA Enterprise Applications Competency Center

NFLET – National Federal Law Enforcement Training

NCIC - National Crime Information Center

NID -NASA Interim Directive

NIMS – National Incident Management System

NIST - National Institutes of Standards and Technology

NM – NASA Memorandum

NPD – NASA Policy Directive

NPR - NASA Procedural Requirement

NRF – National Response Framework

OCIO - Office of the Chief Information Officer

OMB – Office of Management and Budget

OPM - Office of Personnel Management

OPS - Office of Protective Services

PACS – Physical Access Control System

PCI – Personal Card Issuer

PDR – Position Risk Determination

PKI - Public Key Infrastructure

PIA - Privacy Impact Assessment

PIF - PIV Issuing Facility

PII - Personally Identifiable Information

PIN – Personal Identification Number

PIV – Personal Identity Verification

PIV-I – PIV Interoperable

POC – Point of Contact

PSO – Protective Services Office

RSA – Remote Secure Access

SAO - Senior Authorizing Official

SATERN - System for Administration, Training and Educational Resources

SAVE - Systematic Alien Verification for Entitlements

SII – Security/Suitability Investigations Index

SLA – Service Level Agreement

SORN – System of Records Notice

SP - Special Publication

SSN - Social Security Number

TCAC - Transition Common Access Card

TTCP – Technology Transfer Control Plan

USCIS – United States Citizen and Immigration Service

UUPIC – Universal Unique Personal Identification Code

APPENDIX C: NASA PHOTO IDENTIFICATION BADGE STANDARDS

Table C-1

1. LETTERING	**COLOR-FONT**	**POINT**
a. Badge No: ######	Black-Helvetica	6pt. Upper & lower case. Left Justified.
b. First/MI/Last Name	Black-Helvetica	12 pt. Upper & lower case. Lower left justified.
c. Center Numerical Designation	Black-Helvetica	18 pt. Lower left.
d. PO Box	Black-Helvetica	6 pt. Upper & lower case. Bottom centered.

2. NASA PHOTO-ID STANDARDFEATURES	**CHARACTERISTIC**	**SIZE**
a. Photograph	COLOR	(2.9cm x 3.9cm) 7 x 9 picas.
b. Card Stock	Standard	(5.5cm x 8.6cm) 13 x 20.3 picas.
c. Strap Slot (authorized for Center-specific photo-ID only.	Precut & Centered	(1.4cm x .3cm) 3.5 x 7 picas.
d. Logo	Silhouette of Space Shuttle	
e. Reliability Color for all Photo-ID	White	

3. COLOR CODING	**CARD COLOR**
a. Civil Service	GOLD
b. Consultant/Contractor	BLUE
c. Military/Other Agency (Detailee)	GREEN
d. Interns/CO-Ops, Summer Students	VIOLET
e. U.S. National Press	BROWN
f. Foreign National (Non-Designated/Press)	ORANGE
g. Foreign National (Designated)	RED
h. Jet Propulsion Laboratory	SILVER

4. CENTER	CENTER ALPHA DESIGNATOR
a. Ames Research	ARC
b. Dryden Flight Research Center	DFRC
c. Glenn Research Center	GRC
d. Goddard Space Flight Center	GSFC
e. NASA Headquarters	HQS
f. Jet Propulsion Laboratory	JPL
g. Johnson Space Center	JSC
h. Kennedy Space Center	KSC
i. Langley Research Center	LARC
j. Marshall Space Flight Center	MSFC
k. Stennis Space Center	SSC

PART 2.

Privacy Act Notice

General - Pursuant to Public Law 93-579, Privacy Act of 1974, as amended (5 U.S.C. 552a), the following information is being provided to persons who are asked to provide information in order to obtain a NASA Personal Identity Verification (PIV) Card.

Authority - This information is collected under the authority of the National Aeronautics and Space Act (Section 304a), 42 U.S.C. 2455, and Executive Order 9397.

Purposes and Uses - The primary use of collecting the information requested by this form is to facilitate the issuance of a NASA PIV Card. Social Security numbers are requested to keep NASA records accurate because other employees may have the same birth date. When collected, this information shall be maintained in NASA Privacy Act Systems of Records (10SECR). Generally, the information contained in this category of records is used within NASA for determining suitability for Federal employment and access to classified information (security clearances), as well as access to security areas, NASA Centers, and other matters connected with security programs and operations.

In addition to the internal uses of such information, it shall also be disclosed to Federal, State, local, or foreign agencies in connection with official business, including law enforcement, intelligence activities, determinations concerning access to classified information, and matters concerning immigration. Information connected with a law enforcement or administrative inquiry or investigation shall be disclosed to NASA contractors, subcontractors, or grantees. Disclosure shall also be made to the White House or Congressional offices in the course of

certain inquiries. Additionally, in the event of a courts or formal administrative proceeding, information shall be disclosed in the course of presenting evidence or during pretrial discovery. NASA shall disclose information to the Department of Justice or other agencies in connection with such a proceeding.

Effect of Non-Disclosures - Providing this information is voluntary. However, if the form is not completed, a NASA PIV Card shall not be obtained. This shall result in various undesired actions such as disqualification for employment or access

APPENDIX D: SUBSCRIBER AGREEMENT

NASA Public Key Infrastructure (PKI) Subscriber Agreement (HSPD 12 Compliant badge) (version 1.0, August 2007):

YOU MUST READ THIS NASA PKI SUBSCRIBER AGREEMENT BEFORE REQUESTING, ACCEPTING, OR USING A NASA HSPD 12 COMPLIANT BADGE. BY SUBMITTING A REQUEST FOR A NASA HSPD 12 COMPLIANT BADGE, YOU ACKNOWLEDGE YOUR ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

By submitting a request for a NASA HSPD 12-compliant badge you agree to use the badge and any related NASA PKI Certificate and Services only in accordance with this Subscriber Agreement, including:

a. make true representation at all times regarding information in your HSPD 12 compliant badge request, related Public Key Certificate request, and other identification and authentication information related to a NASA PKI Certificate;

b. use your badge exclusively for authorized NASA business such as to gain access to NASA facilities and/or systems; - take reasonable precautions to protect your badge from loss, disclosure, modification, or unauthorized use;

c. inform NASA within 24 hours of the loss of your badge; - inform NASA within 48 hours of a change to any information included in your HSPD 12 compliant badge request and related Public Key Certificate application;

d. return the badge to NASA upon expiration, demand by NASA, or when you no longer require the badge, for reasons including job transfer, extended leave, resignation or termination of employment. NASA HSPD 12 compliant badge contains a NASA Public Key Certificate suitable for providing authentication.

Failure to abide by NASA certificate policies and practices may constitute grounds for revocation of certificate privileges, and may result in administrative action and/or criminal prosecution under the computer fraud and abuse act (18 U.S.C Sec. 1030(c)). NASA reserves the right to refuse to issue a NASA Public Key Certificate. Additional information regarding NASA Public Key Certificates is available at http://nasaca.nasa.gov/docs.html**.**

This agreement shall be governed by and construed in accordance with United States federal law. NASA badges and Public Key Certificates are deemed government supplied equipment, and as such, all users are bound by U.S. federal law governing the use of government provided equipment.
If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, all other provisions shall remain in force. Further

information, including HSPD-12 badge applicant rights and responsibilities, is available on the Agency web site at http://hspd12.nasa.gov**.**

Account Access:

The following statement describes your responsibility for using the badge for logical access to NASA computer assets: Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/ these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution. (NPR 2810.1A, 11.3.3.2)

Statement:

I hereby certify that the information provided by me is true and correct to be best of my knowledge and belief. I certify that I am the individual described in the NASA badge request. I agree to maintain control of the badge at all times once my fingerprint activates it and upon receipt and to abide by the agreements above. Once issued to me I will immediately notify the Center Protective Services Office (Security) if I discover that it is not under my control due to misplacement, loss or other cause.

CONTRACT APPENDIX 1

NASA and Caltech Understanding Concerning the NASA Jet Propulsion Laboratory

This **Contract** appendix provides the historical context of the NASA/JPL relationship. This appendix is a non-binding statement with no contractual implications, and does not augment, supplement or clarify requirements set forth in the **Contract**. Any statements contained in this appendix, including the advantages that NASA currently sees through its relationship with Caltech operating JPL as a university managed FFRDC, do not commit NASA to continuing the relationship. This appendix explains Caltech's and NASA's view on the issues covered herein, but does not commit NASA to any of the precepts set forth in the language. All statements or agreements outside of the **Contract** (including, but not limited to past Memoranda of Understanding) are void.

Background

The foundations for the Jet Propulsion Laboratory ("JPL") were laid in the late 1930's by Professor Theodore von Karman and his graduate students of the Guggenheim Aeronautical Laboratory of the California Institute of Technology ("Caltech"). Their pioneering experiments with rocket engines initially were funded by private Caltech sources, but with the onset of World War II, objectives and sponsorships became entirely military. By 1944, a permanent organization had evolved, and Caltech formally established the "Jet Propulsion Laboratory." In the years that followed, JPL pioneered a series of advanced rocket vehicles, mostly for the Army Ordnance Corps, including Corporal and Sergeant. Finally, JPL developed Explorer I, the United States' first Earth-orbiting satellite.

On December 3, 1958, President Eisenhower transferred the responsibilities for JPL from the Army to the newly created National Aeronautics and Space Administration ("NASA"), together with the Government owned property used by JPL. A contract for research, development and related activities was entered into between NASA and Caltech. That work continues today under Contract NNN12AA01C.

NASA / CALTECH RELATIONSHIP FOR OPERATION OF THE JET PROPULSION LABORATORY

JPL has a dual character: it is a NASA-owned facility in Pasadena, California, as well as an operating division of Caltech staffed with regular Caltech employees. Caltech has operated JPL as a NASA Federally Funded Research and Development Center (FFRDC) since 1959 to meet certain Government research and development needs which could not be met as effectively by existing Government resources or normal contractor relationships. Contractors operating FFRDCs are allowed access beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive and proprietary data, and to Government employees and facilities. As a part of this special relationship, it is also required that JPL be operated in the public interest with objectivity and independence, be free from

organizational conflicts of interest, and have full disclosure of its affairs to NASA. The JPL facility and the employees with their knowledge, shared experiences and traditions of excellence, are together a major national capability. Caltech and NASA each recognize a shared interest in assuring the proper use and maintenance of that national capability, not only for NASA programs but also for other programs of national interest which require the unique capabilities of JPL.

On its part, Caltech is fully committed as set forth in the Contract, as its principal mission at JPL, to carrying out NASA programs, projects and tasks assigned to JPL. In doing so, Caltech recognizes that JPL is a full member of the NASA team and, as such, must recognize and appropriately comply with those applicable laws, regulations, directives and established procedures, as are necessary to the orderly carrying out of NASA's programs and other activities. Caltech also recognizes that in addition to his responsibilities as the head of an operating division of Caltech, the Director of JPL has responsibilities to NASA similar to those of the NASA Center Directors.

It is recognized by Caltech and NASA that JPL through its connection with Caltech represents a unique educational and research resource of significance to the university community generally, and that JPL, in turn, needs close and continuing interaction with broad segments of the university community in order to carry out its mission for NASA. Accordingly, NASA encourages a high degree of interaction between the Caltech Campus and JPL at all levels, and between JPL and the university community. For its part, Caltech recognizes that it must act not only in its own interest but in the interests of the entire university community in carrying out its JPL activities**,** however; Caltech is still ultimately responsible to NASA for carrying out NASA programs. Caltech has a need and an obligation to facilitate the involvement of the ablest available scientists, engineers, and students from the entire university community in NASA and other Government-sponsored research and development at JPL. Caltech regards its undertaking at JPL not only as a contract, but also as a public trust.

In order to expand further the interaction between the university community and JPL, part-time participation of JPL employees in research supervision and in teaching on the Caltech Campus and with other universities is specifically encouraged by Caltech and NASA, as is the part-time work at JPL by faculty members of the Caltech Campus and other universities. Further, Caltech will make its best effort to promote additional postdoctoral research opportunities at JPL, consistent with JPL's programmatic obligations. Additionally, the part-time utilization of faculty and students at JPL will continue to be encouraged by Caltech. It is understood that these activities should not interfere with the support of NASA programs, and that NASA has the right to review JPL work in these areas for reasonableness and appropriateness.

In line with its responsibility for JPL, Caltech recognizes the continuing need for the management of an advanced technology laboratory such as JPL to have oversight and direction (that is consistent with NASA oversight and direction) from broadly experienced industrial, university, and professional leaders on scientific, technological, programmatic and general management matters. In recognition of this need, the Caltech Board of Trustees has established a JPL Committee of the Board. The Board of Trustees of Caltech will continue to ensure that the Committee is composed of persons with relevant experience and recognized achievements in industry, universities and governmental areas. The Committee will hold regularly scheduled meetings to provide oversight and direction to Caltech/JPL on operating policy and

procedures, relationships with NASA, other Federal agencies, industry, universities and the scientific community.

NASA and Caltech believe that in order to achieve the unique benefits available through the close association of JPL with Caltech, on the one hand, and to meet the JPL responsibility for major programmatic objectives, on the other hand, JPL as an institution must encompass a full spectrum of activities from basic research all the way through to the conduct and management of space flight missions. Further, JPL must be a technical "doing" organization with the fraction of total effort performed in-house highest at the research end of the spectrum of activities. To ensure a synergistic relationship with the U.S. advanced technology industry, JPL will utilize industrial capabilities to the fullest extent reasonable—consistent with the necessity that its technical management be based upon current in-depth technical understanding and first-hand implementation expertise. The necessary balance between maximum utilization of industry, on the one hand, and maintenance and development of credible technical and management skills at JPL, on the other, will be considered by NASA in program implementation decisions. Although NASA can make no commitment to the future balance of JPL directed versus competed programs, NASA's general goal is to carry out at least one key challenging flight mission in an in-house implementation mode, and other flight systems in various system contract implementation modes appropriate to the distribution of technological inheritance within the industry and at JPL.

JPL, in developing and disseminating advanced technology, has contributed significantly to the growth and capability of U.S. advanced technology industry. Caltech and NASA are committed to the continuation of that process. Caltech, for its part, will make its best effort to interface appropriately with the private sector to facilitate and encourage the dissemination, further development and broad commercial utilization of new technology arising from JPL efforts. JPL will participate in NASA's Technology Utilization Program to apply aerospace technology from throughout NASA to non-aerospace applications. NASA, for its part, will make its best effort to facilitate the administrative processes involved in fostering the utilization of technology by U.S. industry developed by JPL. NASA's program to provide potential domestic users early access to NASA-developed technology having significant early commercial potential prior to general publication or export of the technology will be implemented at JPL by an early screening of NASA-sponsored work having such early commercial potential and JPL will consult with NASA on the dissemination of technical data resulting from such work.

NASA and Caltech recognize the importance of JPL to the Nation and believe that judicious efforts by JPL to identify and seek potential, appropriate work which is sponsored by agencies other than NASA, but which benefit NASA programs and makes use of JPL's special competencies or falls within their purpose or mission is encouraged. NASA and Caltech believe that the facilities at JPL should be at a level of quality and functional capability as is necessary to maintain JPL in the forefront of space research and development. A review of facility requirements will be conducted by JPL annually and NASA will take the results of those reviews into consideration in the annual budgetary cycles.

NASA recognizes the special character of JPL within the NASA family and the desirability of maximizing the benefits which this university-related, FFRDC can bring to NASA. In carrying out its mission JPL will adopt programmatic management policies and practices compatible with those elsewhere in the Agency and will strive to achieve the highest levels of performance,

safety, and cost effectiveness. While recognizing the importance of its interface with NASA, the Laboratory will conduct its business, administrative, and personnel affairs in a manner consistent with its role as an operating division of Caltech, and it will seek to adopt the best business practices available. NASA will consider JPL's FFRDC status as a university managed FFRDC and other factors to ensure that Government policies to be applied to JPL are appropriate.