

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE		PAGE 1 OF 1 PAGES	
2. AMENDMENT/MODIFICATION NO. P00007		3. EFFECTIVE DATE 08/05/2020		4. REQUISITION/PURCHASE REQ. NO.		5. PROJECT NO. (If applicable)	
6. ISSUED BY CODE NASA Management Office Jet Propulsion Laboratory 4800 Oak Grove Drive M/S 180-802 Pasadena CA 91109				7. ADMINISTERED BY (If other than Item 6) CODE			
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code) CALIFORNIA INSTITUTE OF TECHNOLOGY 1200 E CALIFORNIA BLVD PASADENA CA 91125-0001				(X)			
				9A. AMENDMENT OF SOLICITATION NO.			
				9B. DATED (SEE ITEM 11)			
				10A. MODIFICATION OF CONTRACT/ORDER NO. 80NM0018D0004			
CODE 80707 FACILITY CODE				10B. DATED (SEE ITEM 13) 06/29/2018			

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Continuation Sheet If Applicable

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.

IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
<input type="checkbox"/>	
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: 52.243-2, Changes—Cost Reimbursement (AUG 1987) (Alt III, V) (APR 1984)
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copies to issuing office.	

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to update the table within B-5 Lump Sum Amount and Attachment A with new OCIO Implementation Plans:

(1) In the table within B-5, Allowable Costs, paragraph (c)(2), add the following FY 2020 data:

NEGOTIATED LUMP SUM AMOUNT	MOD #
(b) (4)	7

(2) Attachment A within the OCIO Section, the following four (4) Implementation Plans have been added:

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Gayk Dzhordzhalyan Contracting Officer	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA GAYK DZHORDZHALYAN <small>Digitally signed by GAYK DZHORDZHALYAN Date: 2020.08.05 10:52:04 -07'00'</small> (Signature of Contracting Officer)	16C. DATE SIGNED

CONTINUATION SHEETREFERENCE NO. OF DOCUMENT BEING CONTINUED
80NM0018D0004P00006

Page 2 of 2

NAME OF OFFEROR OR CONTRACTOR CALIFORNIA INSTITUTE OF TECHNOLOGY

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	NPD 2810.1/ NPR 2810.1 NASA Information Security Policy IP NPR 2841.1 Identity, Credential, and Access Management (ICAM) IP Software License Management IP 21st Century Integrated Digital Experience Act (IDEA) IP All other Terms and Conditions remain unchanged. End of Modification.				

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT				1. CONTRACT ID CODE		PAGE 1 OF 2 PAGES	
2. AMENDMENT/MODIFICATION NO. P00007		3. EFFECTIVE DATE		4. REQUISITION/PURCHASE REQ. NO.		5. PROJECT NO. (If applicable)	
6. ISSUED BY CODE		7. ADMINISTERED BY (If other than Item 6) CODE					
NASA Management Office Jet Propulsion Laboratory 4800 Oak Grove Drive M/S 180-802 Pasadena CA 91109							
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code) CALIFORNIA INSTITUTE OF TECHNOLOGY 1200 E CALIFORNIA BLVD PASADENA CA 91125-0001				(X)			
				9A. AMENDMENT OF SOLICITATION NO.			
				9B. DATED (SEE ITEM 11)			
				10A. MODIFICATION OF CONTRACT/ORDER NO. 80NM0018D0004			
				10B. DATED (SEE ITEM 13) 06/29/2018			
CODE 80707		FACILITY CODE					

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Continuation Sheet If Applicable

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.

IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
<input type="checkbox"/>	
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: 52.243-2, Changes—Cost Reimbursement (AUG 1987) (Alt III, V) (APR 1984)
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copies to issuing office.	

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to update the table within B-5 Lump Sum Amount and Attachment A with new OCIO Implementation Plans:

(1) In the table within B-5, Allowable Costs, paragraph (c)(2), add the following FY 2020 data:

NEGOTIATED LUMP SUM AMOUNT	MOD #
(b) (4)	7

(2) Attachment A within the OCIO Section, the following four (4) Implementation Plans have been added:

15A. NAME AND TITLE OF SIGNER (Type or print) Katrina Christian, Manager Office of Contracts Management		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Gayk Dzhordzhalyan Contracting Officer	
15B. CONTRACTOR/OFFEROR E-SIGNED by Katrina Christian on 2020-08-04 19:42:27 GMT (Signature of person authorized to sign)	15C. DATE SIGNED 2020-08-04 19:42:27 UTC	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED

Previous edition unusable

CONTINUATION SHEETREFERENCE NO. OF DOCUMENT BEING CONTINUED
80NM0018D0004P00006

Page 2 of 2

NAME OF OFFEROR OR CONTRACTOR CALIFORNIA INSTITUTE OF TECHNOLOGY

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	NPD 2810.1/ NPR 2810.1 NASA Information Security Policy IP NPR 2841.1 Identity, Credential, and Access Management (ICAM) IP Software License Management IP 21st Century Integrated Digital Experience Act (IDEA) IP All other Terms and Conditions remain unchanged. End of Modification.				

Office of the Chief Information Officer

Information Security Implementation Plan

Directive Information

NPRs and NPDs

1. NPR 2810, Security of Information Technology
2. NPD 2810, NASA Information Security Policy
3. Applicable cybersecurity requirements pursuant to Prime Contract 80NMO18D0004 Sections I-7 and H-43. The Contractor considers Cybersecurity requirements identified by the link in I-7 to be lower-tiered documents.

NFS

1. 1852.239-74 Information Technology System Supply Chain Risk Assessment (NASA Procurement Class Deviation (15-03C)(SEP 2018)

NASA Responsible Office

Office of the Chief Information Officer

Declaration

Consistent with the Article in the Contract entitled “Non-Applicability of Lower-Tier Documents” and except as provided below, the Contractor fulfills the sections of the documents listed above that apply to the Contractor personnel, except for inherently governmental functions, as defined in FAR Subpart 7.5 and this Contract.

Scope

The Contractor will protect all Contractor and NASA information and information systems, both classified and unclassified, as defined in federal and NASA requirements. If the Contractor is unable to meet those requirements for a particular system, a Risk Based Decision (RBD) will be submitted in RISCS for Authorizing Official (AO) decision.

All information systems containing NASA data will be entered into RISCS. For the purpose of this Plan, NASA data is any data (as defined in the FAR Rights in Data clause of the Prime Contract) or the content of Government records, as defined in clause H-16, that is processed, managed, accessed or stored on an IT system(s) in the performance of the Prime Contract. Until NASA grants an Authority to Operate (ATO) for a System Security Plan, the use of data in RISCS will be limited to support the ATO process for the corresponding Plan. After the ATO is granted, the approved Plan’s RISCS data may be used for other purposes. For new requirements to NASA's required Authority to Operate policy and processes, parties agree to follow the process

outlined in section G-13 (c) of Prime Contract 80NM0018D0004, entitled New or Updated Government Policies.

This plan is organized into chapters, each of which addresses new cybersecurity components which are not captured by responding to required controls in NASA and federal policy and requirements. Each chapter starts with a high-level summary of the requirements and includes a description of the practices that the Contractor employs to meet the specified requirement. The description of current practices is followed by the Contractor assessment of the degree to which the Contractor meets the requirements as well as gaps. The Contractor will discuss mitigating steps with the responsible Authorizing Official for requested approval. NASA will conduct audits to validate the contract requirements are met.

1.0 Assessment & Authorization

The Contractor understands that NASA's Assessment and Authorization (A&A) process is the Agency's implementation of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), and that NASA adheres to the processes defined by the NIST RMF.

The Contractor and NASA mutually agree that the process and supporting technology for the A&A process are open to streamlining, with the ultimate goal of having a single point for compliance and related security assessments that streamlines data ingestion, supports robust analytics, and is integrated into the flight project life-cycle where applicable.

The Contractor has a long-term goal of adopting and streamlining the full A&A process, which will require a change management strategy. A separate plan and schedule will need to be drafted in the future to meet the full A&A process for all plans. The Contractor will also have resource needs in order to support and maintain a full A&A process.

1.1 Adoption of the A&A Process

In order to support NASA's understanding of risk posture, the Contractor will adopt the A&A process, and begin the migration of existing plans and introduction of new plans into the NASA RISCS system.

The Contractor has been following the Certification and Accreditation (C&A) process which does not align to the A&A process currently being utilized by NASA. In support of the transition to the NASA A&A process, the Contractor will launch a project dedicated to the implementation of A&A at JPL.

1.1.1 Contractor Action	<p>The Contractor to launch a project dedicated to the implementation of A&A at JPL. This will include the development of processes and procedures necessary in response to the A&A process requirements.</p> <p>Clear communication and change management is critical in order to ensure the process is successfully implemented.</p>
--------------------------------	--

	The Contractor understands that we need to still move forward with plan entry in parallel with this project but request that NASA partner with the Contractor during lessons learned and other collaborative initiatives.
1.1.2 Joint Action	The Contractor and NASA to collaborate on the Risk Management Framework including but not limited to, consistency in the independent assessment, engagement from the AODR, and a shared definition of risk categorization across all stakeholders to help prioritize POAMs.

2.0 Security Plan Visibility & Creation

There are three distinct categories of system security plans at JPL.

1. Flight Projects systems: This category includes all non-subscribed flight project system security plans.
2. Subscribed systems: This category is comprised of one system security plan which is a service delivered and managed by the Service Contractor that includes patch management, hardware, core applications, CDM Suite including BigFix Client, and periodic hardware refreshment. The hardware is procured, owned and managed by the JPL outsourced desktop contractor.
3. Institutional Infrastructure and Support Security Plans: This category includes JPL procured and government owned system security plans that are managed at the system owner level for procurement, patch management, CDM requirements and hardware refresh lifecycle. These systems reside primarily within the JPL line organizations.

The strategy and schedule for migration and creation of these three categories of system security plans are to be broken out in two separate, but parallel work efforts.

As it is the same set of resources working to enter all the plans into RISCS and work through the A&A lifecycle, the Contractor recommends a holistic plan prioritization, data entry and ATO work effort approach.

2.0.1 NASA Action	<ul style="list-style-type: none"> • NASA confirmed that an employee of the Contractor can act as an Authorizing Official Designated Representative. The Contractor will work with the identified AO to nominate a Contractor AODR, with the AO reserving final decision-making authority. • NASA will provide the Security Control Assessor for each plan.
------------------------------	---

2.1 Approach and Schedule for NASA's A&A Process

2.1.1 Flight Project Systems Plan Prioritization

For Flight Project Security Plans with an SMD Authorizing Official, plan prioritization will be provided by NASA's Science Mission Directorate in accordance with the guidance issued in the June 23, 2020 letter from NMO subject: Guidance for Authorization To Operate (ATO) Documentation for SMD Systems (included as Appendix B).

All systems with a PDR after June 23, 2020 are required to enter all required documentation into the RISCS system.

1. All development systems in Phase D or later may use a combination of Hard Copy and RISCS entry for issuance of an ATO with a plan to finalize the RISCS transition by June 2022.
2. All development systems not covered by either of the above may have a mixture of Hard Copy and RISCS documentation for evaluation prior to launch. A plan must be developed for transition of all information into the RISCS system with a completion date no later than six-months after launch.
3. All operational systems shall develop a plan to transition documentation into the RISCS system by June 2023 or as coordinated with SMD.
4. NASA SMD will work with JPL to identify the project priorities within the above guidelines for completing and submitting

For Flight Project Security Plans with an Authorizing Official outside of SMD, plan prioritization will be coordinated with the Authorizing Official.

2.1.1.1 Joint Action	The Contractor and NASA SMD to collaborate and finalize the list of in scope existing and near-future Flight Project Plans to help realize a schedule and communicate the upcoming changes to the flight project plan owners.
-----------------------------	---

2.1.2 Institutional Infrastructure and Support Security Plans

As part of the adoption of the A&A process, the Contractor will re-evaluate the system security boundaries of their Institutional Infrastructure and Support Security plans and refactor new plans based on this evaluation. The Contractor will begin the task of refactoring and restructuring the plans and related assets. After a plan has been re-scoped and related assets assigned to the plan, the Contractor will update the BigFix client on those assets to reflect the new plan number in RISCS.

As there are approximately 120 Infrastructure Security Plans in place at this time, this work effort will require a strategic analysis to understand the scope of work that needs to be performed.

2.1.2.1 Contractor Action	For Institutional Infrastructure and Support Security plans the Contractor will provide a refactor and migration strategy that will include the following information:
----------------------------------	--

	<ol style="list-style-type: none"> 1. Assessment for level of effort to refactor and restructure these ~120 plans with accurate security boundaries with the expectation of reduction in the number of plans. 2. Prioritize the following system boundaries - infrastructure/lab support; Microsoft 365; ICAM; VPN; SOC; LAN/WAN; Data Center/AWS; Splunk; Active Directory; Security Perimeter Devices 3. Estimated start dates for RISCs entry for priority areas defined above, with the long-term target of a plan prepared for the full ATO lifecycle <p>Delivery of Assessment Findings and Strategy: August 6, 2020</p>
--	---

2.1.3 Subscribed System Security Plan

The Contractor developed a system security plan (SSP) for ITSD Subscribed Systems in RISCs with plan number NN-9999-JPL-4748. This plan includes ~12,000 devices some of which are managed by the Service Contractor that includes patch management, hardware, core applications, CDM Suite including BigFix Client, and periodic hardware refreshment. For the devices managed by the Service Contractor, the hardware is procured and owned by the JPL outsourced desktop contractor and is provided to JPL as a service.

A subset of the devices in plan number NN-9999-JPL-4748 are managed by system plan owners. As each Flight Project system plan and Institutional Infrastructure and Support Security plan is entered/updated in RISCs, the devices assigned to NN-9999-JPL-4748 will be evaluated to determine if any devices under the Contractor's Subscribed system security plan should be moved to the corresponding SSP being entered/updated.

2.1.4 Holistic Schedule

The effort to ensure plan information in RISCs is to give NASA visibility into the Contractor's system security boundaries. To prepare a plan for the full ATO lifecycle requires not only a large amount of data to be gathered and entered on the Contractor's side, but for NASA to perform a full assessment of the controls and full lifecycle partnership from the beginning of the plan creation.

Therefore, the combined schedule to migrate all plans into RISCs needs to include a partner on NASA's side to collaborate with the plan owner and JPL A&A Team.

2.1.4.1 Joint Action	<p>NASA and the Contractor to assess the plans identified in 2.1.1 Flight Project Plans and 2.1.2 Institutional Infrastructure and Support Security plans and prioritize a holistic schedule. If NASA wishes to expedite any specific plans, the Contractor may need additional resources in order to prioritize against an agreed upon schedule.</p>
-----------------------------	---

3.0 Check In & Lessons Learned

3.0.1 Joint Actions	<p>An initial Lessons Learned was held on July 8, 2020. This meeting demonstrated value by disclosing a need for all parties to identify agreed upon risk metrics, terminology and future business process.</p> <p>The Contractor recommends at least an additional two Lessons Learned check ins for August and September in order to assess plan quality, receive feedback, and drive towards consistency with the A&A process lifecycle.</p> <p>Lessons Learned check ins should include representatives from all impacted stakeholders. At minimum the Lessons Learned meetings will include representatives from NASA's Office of the Chief Information Officer, Science Mission Directorate, and Human Exploration and Operations Mission Directorate, and the Contractor's Information and Technology Solutions Directorate, Engineering and Science Directorate, and Interplanetary Network Directorate.</p> <p>The Contractor is looking to ensure feedback provided is then incorporated into future plan creation in order to streamline the process and would like a standardized approach for the entire lifecycle.</p> <p>Future discussion items include, but are not limited to:</p> <ul style="list-style-type: none"> • Evaluate plans entered into system <ul style="list-style-type: none"> ○ Parties will reassess data entry and NASA expectations ○ Parties will reassess refactoring plans • NASA and the Contractor to continue to evaluate Lessons learned from A&A Process Implementation of small Unmanned Aerial Systems (sUAS), Deep Space Network, Mars 2020, NISAR and SWOT. The lessons learned will be used to refine approach for future cycles. <p>Estimated Completion by: September 30, 2020</p>
--------------------------------------	---

4.0 Technical Support & Training for RISCS

In order to support this process internally, the Contractor will be interacting frequently with the NASA RISCS system. The NASA RISCS system already has RMF training mandatory for NASA Authorizing Officials and an optional "RISCS AO and AODR" training.

The Contractor will need to ensure that there is a formal pathway for support on the NASA RISCS system and training for those that need to perform additional RMF roles.

4.0.1 Contractor Action	Upon AO's approval of a JPL AODR, the JPL AODR will complete training in SATERN.
--------------------------------	--

5.0 Resource Augmentation to Facilitate Work Effort

As transitioning to the NASA A&A process is resource intensive, the Contractor will need to obtain additional resources in order to assist internal organizations with their completion of the NASA A&A process. After exploring all internal solutions, the Contractor will inform NASA, through NMO, of resource constraints in achieving the deadline. The estimates below are based on the number of plans, the timeline provided by NASA, and the heavy lift needed to migrate between authorization processes between the Contractor and NASA.

5.0.1 Contractor Action	<p>The Contractor will acquire the following roles in order to facilitate requested deadline:</p> <p>The Contractor has estimated the need to hire the following positions</p> <ul style="list-style-type: none"> • Information Systems Security Officers • Information System Security Engineers • Project Managers • Technical Writers • The Contractor will create job descriptions, hire resources, and once staffed up, begin the process of meeting with the prioritized system owners to facilitate the implementation of the NASA A&A process • Funding for matrixed resources on projects that no longer have any budget <p>Estimated Start by: April 15, 2020 – In progress</p>
5.0.2 NASA Action	If NASA wishes to expedite any specific plans, the Contractor may need additional funding or resources to prioritize against an agreed upon schedule.

6.0 Security Configuration Baseline and Management

The Contractor locally manages all IT services and does not participate in the Agency's IT services contract. Therefore, the Contractor has historically derived their security baseline configuration standards through our Prime Contract from NPRs, NPDs, and NIST Security Standards. Each security requirement is accompanied by an Audit Procedure based on 800-53A to ensure compliance with JPL Cybersecurity Requirements.

Although the Contractor has a core build managed by its asset management partner (ManTech), we are reviewing the NASA Agency Security Configuration Standards (ASCS) baseline as provided via the Cybersecurity Standards Engineering Team (CSET) site.

6.0.1 Contractor Action	<ul style="list-style-type: none"> • The Contractor will document the delta between the NASA configuration baselines for operating systems provided in CSET with the existing JPL baselines and communicate to NASA where adopting the NASA configuration baseline would severely impact critical operations. • The Contractor will provide an assessment of the delta between its existing recommended baseline on applications used by both NASA and the Contractor when resources are available. • This assessment will include impact and risk, and a strategy by the Contractor that discusses how and where the baseline can be aligned. For areas that require additional discussion or a deviation from the baseline, the Contractor will provide more details for approval by the NASA SAISO. <p>Estimated Completion by: September 30, 2021</p>
--------------------------------	--

7.0 Incident Response and Operating Level Agreements for the Security Operation Center (SOC)

The Contractor has negotiated an Operating Level Agreements (OLA) between JPL and the Associate Chief Information Officer (CIO) for Cybersecurity & Privacy Division (included as Appendix A). This agreement covers the provision and support of the NASA Security Operations Center (SOC). The OLA describes the services and metrics required to meet security operations requirements between the JPL SOC and the NASA SOC. Should the scope of the OLA not encompass all related Information Security areas, this plan will be updated, to reflect the plan of executing those areas, unless already identified in the Contractor's Annual Performance Evaluation Management Plan.

8.0 Identity, Credential and Access Management

Consistent with the Decision Memo, *Identity, Credential and Access Management (ICAM)*, dated December 20, 2019, NASA has directed the Contractor to continue to work on the ICAM effort for an additional 18-24 months. The ICAM Implementation Plan deals with a subset of ICAM requirements that have been approved by NASA.

Please reference the ICAM Implementation Plan for specifics concerning the Contractor's ICAM implementation.

9.0 Network Access Control (NAC) Tools - Pulse Secure

JPL uses PulseSecure NAC tools (Pulse Profiler and Pulse Policy Secure) to accomplish network discovery of devices.

This tool was approved for CDM use in place of Forescout, which was the tool prescribed by Booz Allen for CDM implementation. This waiver was granted for several reasons:

- JPL already deployed the PulseSecure NAC tools and had already made a significant investment
- PulseSecure NAC was better able to deploy into JPL's complex and wide-spread network
- PulseSecure NAC has strong connections to the PulseSecure VPN product JPL uses, enabling greater functionality

As part of this waiver, JPL agreed to report data in an automated fashion to the centralized CDM environment in the format that would be expected by all other centers. This data began successfully reporting in February 2020.

The data that is provided is a real-time feed of all devices that connect to any JPL managed networks, including profiles of the devices and their functions.

10.0 Supply Chain Risk Management

Background

NASA FAR Supplement (NFS) Clause 1852.239-74, Information Technology System Supply Chain Risk Assessment was updated on Contract in January 2020 from the (Apr 2016)(Deviation) to the (Sep 2018)(Deviation) via Modification Number 5. The clause requires that the NASA HQ OCIO IT Security Division review the Contractor's supply chain for the risk of cyber-espionage or sabotage before the Contractor acquires any high-impact or moderate- impact IT systems. In the updated version of the clause, "Information Technology (IT) System" has been redefined and the exceptions have been deleted. Modification Number 5 includes a requirement for the Contractor to implement 1852.239-74 (Sept 2018)(Deviation) through a formal Implementation Plan. This chapter of the Plan discusses how the Contractor will implement the updated clause.

The NASA CIO issued the Draft Agency Information and Communications Technology Supply Chain Risk Management Service Handbook (hereafter referred to as the Handbook) which describes the processes and procedures NASA is implementing as it pertains to the Supply Chain Risk Management (SCRM) service it provides to Agency Centers and suppliers, to ensure its alignment with federal requirements. The Handbook sets forth roles and responsibilities that will allow for practical application of the Policy and includes:

- SCRM roles and responsibilities, delegating responsibility to individuals across the agency,
- SCRM procedures creating a set of assessment considerations, and
- Request for Investigation (RFI) processes

The Handbook calls out roles and responsibilities for each participant in the SCRM process. As discussed below, the Contractor plans to implement SCRM in phases. During Phase 1 of its Implementation Plan, the Contractor will map the roles, responsibilities and functions defined in the Handbook to their counterparts at the Contractor. The Contractor will follow/participate in the functions called out in the Handbook for review and/or risk analysis of all covered articles (CA).

The Contractor notes that certain NASA processes, particularly with regard to workflow systems, are not utilizing NASA's RFI process. The Contractor will ensure the RFI workflow process can be integrated into the Contractor's processes and systems consistent with acquiring CA that is approved by the NASA CISO and CIO prior to placement of orders.

The Contractor's Implementation Strategy assumes that all items listed on the NASA Assessed and Cleared List (ACL), which will be updated by NASA regularly, are authorized for the Contractor to acquire. The Contractor's Implementation Strategy further assumes that for items not found on the ACL that NASA will maintain a review and approval process that is consistent with Handbook processes and the Contractor flight project formulation and implementation schedules.

As discussed in each Phase, as part of our partnership, the Contractor will actively participate in the NASA SCRM Working Group to develop best practices and procedures for implementation in each organizations' infrastructures, and to share processes and procedures developed at JPL. To the largest extent practicable, the Contractor will use NASA's Working Group solutions to identify and perform necessary screening. In parallel, the Contractor will integrate SCRM management and compliance oversight into the Contractor's local command media, including its deployment processes, to ensure all relevant information is communicated appropriately throughout the Lab.

Implementation Strategy

The Contractor's Implementation Strategy will be accomplished through three (3) distinct implementation phases.

The Contractor will continue to actively participate in NASA's SCRM Working Group to share processes and procedures developed at JPL and to bring back Center best practices during all phases and beyond as part of our partnership. To the largest extent practicable, the Contractor will use NASA's Working Group solutions to identify and perform necessary screening.

10.1 Phase 1: Commercial off-the-shelf (COTS) CA

As part of Phase 1, the Contractor will provide a detailed implementation plan for the overall initiative.

In Phase 1, the Contractor will focus on Commercial off-the-shelf covered articles. The scope of Phase 1 does not include COTS CA that are for use by flight projects. The COTS CA used by flight projects will be included in Phases 2 and 3.

During Phase 1 the Contractor will actively participate in NASA's SCRM Working Group to share processes and procedures developed at JPL and to bring back Center best practices. To the largest extent practicable, the Contractor will use NASA's Working Group solutions to identify and perform necessary screening. At the end of Phase 1 the Contractor will have processes and procedures in place to screen COTS CA prior to order placement.

10.1.1

Detailed implementation plan:

Contractor Action	<ul style="list-style-type: none"> • The Contractor to provide a detailed implementation plan schedule for submittal to NASA. <p>Estimated Completion by: Not more than four (4) months after this IP is accepted by NASA, the Contractor will provide a detailed schedule for implementation of this Plan</p> <p>Phase 1: COTS Work Effort:</p> <ul style="list-style-type: none"> ○ Map Agency functions to the Contractor equivalents ○ Analyze acquisition history for COTS CA volume and type ○ Develop methods and tools to identify CA on P-Card and Purchase Orders and capture essential information to perform required screening ○ Work with NASA on RFI workflow processes ○ Educate suppliers and Laboratory personnel ○ Implement screening on COTS CA <p>Estimated Completion by: November 30, 2020</p>
--------------------------	---

10.2 Phase 2: Quality Critical Items (QCI)

Phase 2 will concentrate on expanding the tools and processes developed in Phase 1 to encompass Quality Critical Items (QCI). QCI items are used on flight projects and are defined as items requiring heightened Mission Assurance surveillance and handling to protect against counterfeit parts. QCI are managed in accordance with NASA Policy Directive (NPD) 8730.2, NASA Parts Policy, which includes robust requirements to evaluate parts to ensure authenticity prior to use on flight projects. The Contractor will build-out existing QCI processes to incorporate Phase 1 defined activities to screen and vet for cyber risk.

10.2.1 Contractor Action	<ul style="list-style-type: none"> • Phase 2 may include a Pilot Program under which the Contractor will test these processes on a flight project. • At the end of Phase 2 the Contractor will have the processes and procedures in place to screen QCI CA prior to order placement. <p>Estimated Completion by: August 1, 2021</p>
10.2.2. Joint Action	<ul style="list-style-type: none"> • NASA will support the development of Contractor's processes to screen QCI CA, as part of the ongoing participation in the NASA SCRM Working Group. NASA support may include sharing best practices, and joint communication to Missions. NASA SCRM Working Group includes SMD and OCIO representative.

10.3 Phase 3: Tool Expansion

Phase 3 will concentrate on expanding the tools and processes developed in Phase 2 to encompass the remaining CA the Contractor acquires, including flight project hardware and software.

10.3.1 Contractor Action	<ul style="list-style-type: none"> • Phase 3 may include a Pilot Program under which the Contractor will test these processes on a flight project. • At the end of Phase 3 the Contractor will have the processes and procedures in place to screen CA prior to order placement in compliance with the NASA FAR Supplement. <p>Estimated Completion by: March 30, 2022</p>
---------------------------------	--

If, during any Phase of this Plan the Contractor determines an alternate approach is warranted, the Contractor will propose a revision to this Plan for NASA concurrence.

10.4 Implementation Schedule

The Contractor estimates each Phase of this plan will require approximately 8 (eight) months to complete, with the Phases overlapping to support the planned outcomes. Therefore, the Contractor plans approximately twenty-four (24) months to implement this Plan. As discussed above, the Contractor will provide a detailed schedule to NASA during Phase 1 to accomplish this Plan.

Detailed SCRM Implementation schedule	11/30/2020
Phase 1 - COTS	11/30/2020
Phase 2 - Quality Critical Items	8/1/2021
Phase 3 - Expansion of Phase 2 to remaining CA JPL	3/30/2022

Appendix A: Operating Level Agreement



National Aeronautics and
Space Administration



OPERATING LEVEL AGREEMENT (OLA)

NASA JET PROPULSION LABORATORY
AND
THE ASSOCIATE CHIEF INFORMATION OFFICER (CIO)
FOR
THE CYBERSECURITY & PRIVACY DIVISION (CSPD)

SECURITY OPERATIONS CENTER (SOC)
AND
INCIDENT MANAGEMENT

July 10, 2020

Table of Contents

1.0	Description of the Service.....	3
1.2	Location of the Services	5
2.0	Service Hours	5
3.0	Operational Targets and Metrics.....	7
3.1	General Service Targets	7
3.2	Operational Availability	8
3.3	Service Continuity	8
4.0	Incident Management and Service Request.....	9
5.0	Periodic Reviews	11
6.0	Configuration Management	11
7.0	Service Level Management and Escalation	12
8.0	Monitoring and Reporting.....	12
9.0	Cost	13
10.0	Security and Governance	13
	Appendix A - Acronyms	14
	Appendix B - Definitions.....	15
	Appendix C – JPL SOC Log Integration	16
	Appendix D – Response Times.....	17

1.0 Description of the Service

The NASA SOC functions as the only authorized single agency-wide cybersecurity operational entity whose mission is to provide proactive prevention, detection, and response to computer security incidents targeting NASA's unclassified networks and systems. These unclassified NASA networks and systems include but are not limited to the corporate, mission and operational technology domains across NASA's vast spectrum. The NASA SOC will operate 24/7/365 and function as the nerve center for all cybersecurity incident monitoring, reporting, detection, prevention, response, mitigation, and cyber threat analysis for the Agency. The NASA SOC will provide the Agency with real-time, continuous cybersecurity monitoring and triage; uninterrupted event detection; incident analysis, coordination and response; situational awareness; and cybersecurity countermeasure implementation capabilities for maintaining a secure cyber and information assurance posture.

The NASA SOC provides three key core cybersecurity services to the NASA enterprise which includes Monitoring, Detection and Prevention, Incident Containment and Mitigation, and Reporting and Communications. Monitoring, Detection and Prevention provides proactive and timely identification, response, and resolution of issues arising from events that indicate a compromise or that could potentially compromise a NASA information systems. Incident Containment and Mitigation (IC&M) focuses on the isolation of anomalies which threaten NASA networks to reduce the severity or attack surface from a realized event in order to return systems or networks to normal operations. By providing NASA Center IR Teams with Policies and Governance IR, NASA SOC sets the expectations for enterprise wide IC&M. Reporting and Communications provides information used in reporting the Agency's incident response posture to the Centers, ranging from incident trends to specific incident data.

The NASA SOC provides these services through distributed enterprise systems. The distributed enterprise services and systems include a triage service to report IT security incidents, an Incident Management System (IMS) and a Security Information and Event Management System (SIEM). At each NASA Center and facility, the NASA SOC provides systems for IT security detection and monitoring with Intrusion Detection Systems (IDS) and Packet Capture (PCAP) infrastructure. The Office of Cybersecurity Services (OCSS) provides Log Aggregation systems for the collection of log information from Center and the Office of the Chief Information Officer (OCIO) security systems such as firewalls and anti-virus. NASA SOC and Center access to the data from these log aggregation systems is available to the Center's incident response teams.

The NASA SOC partners with the Communications Program (CP) to provide Intrusion Prevention Service (IPS) and sinkhole service capabilities. The sinkhole services provide re-routing and data collection for malicious network traffic, based on domain name service (DNS) and the Internet Protocol (IP). The NASA SOC also partners with the End User Services Program (EUSP), in order to protect against malicious attacks with email as the vector through email blocks or email extraction. The EUSP will leverage a secure email gateway (SEG), in order to support email blocks, based on malicious file attachments, file extensions or Uniform Resource Locators (URL).

The NASA SOC also reviews reports of potential threats and vulnerabilities and attempts to determine which of those threats and vulnerabilities are relevant to the NASA enterprise. The

NASA SOC Cyber Threat Analysis (CTA) team then distributes related information to the NASA cyber security community to enable various parties to act upon that information. NASA needs both proactive and reactive capabilities in addressing computer security at the Agency level. The NASA SOC Cyber Threat Hunt (CTH) team composed of Computer Forensics, Incident Analysis, and Detection functions within the SOC provides cyber security analytical capability and forensics for NASA. This service provides the Agency with fly-away, on-site hunt and detection responses to intrusions; provides indications and warnings of potential threats, incidents, and attacks; as well as analytics in response to incidences suspected or in progress.

The JPL Information Technology (IT) Directorate, also known as the Information and Technology Solutions Directorate (ITSD), provides a suite of IT capabilities and services in support of JPL institutional, mission, and business system computing services to enable the success of NASA missions carried out by JPL. Primary to fulfilling the ITSD's Charter and achieving its goals and objectives is the use of the capabilities of the JPL SOC to protect against, monitor and detect, respond to, mitigate the impact of, and restore services that are impacted by verified network-borne threats (voice or data). At JPL, the ITSD is also responsible for management and oversight of the IT Security incident response function at JPL.

The JPL Cybersecurity Operations Center (JPL SOC) is chartered to deliver the following services and capabilities, which constitute the foundation of this OLA and enable the partnership between the JPL SOC and the NASA SOC.

- A. Risk Identification and assessment
- B. Intrusion detection
- C. Threat prevention and mitigation
- D. Event investigation
- E. Incident triage and reporting
- F. Monitoring, Detection and Prevention
- G. Incident Containment and Mitigation
- H. Reporting and Communications
- I. Intelligence sharing
- J. Incident lessons learned

For the NASA Management Office (NMO), the JPL SOC will support the NMO by providing Incident Response functions including data that may include but not limited to raw data (PCAP when available), IDS signature trigger, probable root cause, agency and center trends and other data that may be captured through SOC systems.

1.1 OLA Scope

This agreement is made between JPL and the Associate Chief Information Officer (CIO) for Cybersecurity & Privacy Division and covers the provision and support of the NASA Security Operations Center (SOC). This OLA will describe the services and metrics required to meet security operations requirements between the JPL SOC and the NASA SOC.

1.2 Location of the Services

NASA Security Operations Center Distributed Operations Sites:

- A. The NASA SOC operates from multiple distributed operation sites ensuring NASA's corporate, mission, and operational security business continuity and security operations assurance.
- B. Distributed operations sites provide a single synchronized and collaborative entity for security operation services to the corporate, mission and operational technology domains across NASA's vast spectrum.
- C. These distributed operations site operates 24/7/365 and singularly function as the nerve center for all cybersecurity incident monitoring, reporting, detection, prevention, response, mitigation, and cyber threat analysis for the Agency.
- D. Each distributed operations site is designed with operational capabilities to maintain security operations services when a distributed operations site is degraded or disabled for varying reasons or lengths of time.

JPL Security Operations Center Site:

- A. Local incident response and incident management functions for JPL will be located at JPL. The staff that supports the NASA SOC Communications and Reporting services will be distributed between ARC and JSC.
- B. The JPL SOC which provides intrusion detection, risk identification and assessment, event investigation, incident reporting and threat prevention will be located at JPL.

NASA Cybersecurity Infrastructure Sites:

- A. NASA Cybersecurity Infrastructure (CSI) maintains multiple Contingency of Operations Plan (COOP) Parallel Processing sites for the services supporting NASA SOC. These sites are distributed between Johnson Space Center (JSC), Kennedy Space Center (KSC), and Ames Research Center (ARC).
- B. NASA CSI maintains NASA SOC support systems distributed across multiple locations

JPL Cybersecurity Infrastructure Site:

- A. JPL SOC maintains all JPL SOC support systems at JPL located in Pasadena, CA.
- B. JPL has a managed desktop contract with ManTech.

2.0 Service Hours

This section will discuss the times when the core services are available.

NASA SOC Core Hours:

Support Hour Type	Details
Business Hours	<ul style="list-style-type: none"> • Mitigation Action Reports (6:00 a.m. – 5:00 p.m. Eastern) • Situational Awareness Reports (6:00 a.m. – 5:00 p.m. Pacific) • Cyber Threat Analysis (6:00 a.m. – 5:00 p.m. Pacific) • Cyber Threat Hunt and Forensics (6:00 a.m. – 5:00 p.m. Pacific) • SOC Strategic Reporting (6:00 a.m. – 5:00 p.m. Pacific)
24 x 7 x 365	<ul style="list-style-type: none"> • Monitoring and Detection • Incident Reporting • Prevention and Mitigation • Incident Management System (IMS) • Security Event and Information Management (SEIM) • Intrusion Detection Systems (IDS) • Packet Capture (PCAP) • Endpoint Detection and Response (EDR) • Intrusion Prevention Systems (IPS) • Office 365 (O365) Email Extraction • Security Email Gateway (SEG) • IP Sinkhole • DNS Sinkhole • Network Blocks

JPL SOC Core Hours:

Support Hour Type	Details
Business Hours	<ul style="list-style-type: none"> • Sourcing & Collection (6:00 a.m. – 8:00 p.m. PT) • Threat Analysis (6:00 a.m. – 8:00 p.m. PT) • Processing & Exploration (8:00 a.m. – 5:00 p.m. PT) • Production & Dissemination (8:00 a.m. – 5:00 p.m. PT) • Cybersecurity Data Analytics Consulting (8:00 a.m. – 5 p.m. PT) • Vulnerability and Vulnerability Assessment (6:00 a.m. – 5:00 p.m. PT) • Threat Hunting (8:00 a.m. – 5:00 p.m. Pacific)
24 x 7 x 365	<ul style="list-style-type: none"> • Incident Response • Security Event and Information Management (SEIM) • Intrusion Detection Systems (IDS) • Packet Capture (PCAP) • Endpoint Detection and Response (EDR) • Intrusion Prevention Systems (IPS) • Security Email Gateway (SEG)

	<ul style="list-style-type: none"> • IP Sinkhole • DNS Sinkhole • Network Blocks • Monitoring and Detection • Mission Situational Awareness
--	--

3.0 Operational Targets and Metrics

This section will discuss operational service targets and metrics associated with security operations.

3.1 General Service Targets

This section will present general services supported by this OLA. For each service, the service providers and targets will be presented. The targets represent the time that it takes to complete actions associated with the service.

Service	Service Provider	Measurement Target
Incident Reporting	NASA SOC	<ul style="list-style-type: none"> • 1 hour after discovery
Incident Reporting	JPL SOC	<ul style="list-style-type: none"> • 1 hour after discovery
Mitigation Action Reports	NASA SOC	<ul style="list-style-type: none"> • 1 business day after the determination of the need to create the report
Situational Awareness Reports	NASA/JPL SOC	<ul style="list-style-type: none"> • 1 business day after the determination of the need to create the report
IP Sinkhole Blocks	JPL SOC / CP	<ul style="list-style-type: none"> • 2 hours after the determination of the need to submit the block
DNS Sinkhole Blocks	JPL SOC / CP	<ul style="list-style-type: none"> • Standard process, twice daily Monday through Friday for normal cases. • 2 hours for emergency blocks
Network Blocks	JPL SOC / CP	<ul style="list-style-type: none"> • 2 hours after the determination of the need to submit the block
Firewall Exemptions	JPL SOC / CP	<ul style="list-style-type: none"> • 2 hours after the validation that it is acceptable to remove the block
Web Content Filter Exemptions	JPL SOC / CP	<ul style="list-style-type: none"> • 9 hours after the validation that it is acceptable to remove the block
Email Extraction (O365 only)	NASA SOC	<ul style="list-style-type: none"> • 1 hour after the determination of the need to extract the email for cases of a single submitter, target or subject

Email Extraction	JPL SOC	<ul style="list-style-type: none"> 1 hour after the determination of the need to extract the email for cases of a single submitter, target or subject
Email Data Collection (O365)	NASA SOC	<ul style="list-style-type: none"> Response time depends on the size and scope of request; typically under 48 hours.
Email Data Collection	JPL SOC	<ul style="list-style-type: none"> 1 hour after request
IDS Signature Implementations	JPL SOC	<ul style="list-style-type: none"> 4 hours to test and deploy the signature, once it is received by SOC operations

3.2 Operational Availability

Operational availability is a measurement of how long a system has been available to use when compared with how long it should have been available to be used. The operational availability targets for JPL are:

Service/System	Availability Target
JPL IDS	99.81%
JPL PCAP	98.36%
All IMS	99.73%
JPL DNS Sinkhole	99.73%
JPL IP Sinkhole	99.73%
JPL IPS	99.18%
All Secure Email Gateways	99%

$$\text{Availability} = \frac{(\text{Scheduled Service Hours} - \text{Duration of Unplanned Outages})}{\text{Scheduled Service Hours}} \times 100\%$$

3.3 Service Continuity

The staff that supports the NASA SOC Monitoring and Detection services will be physically located at two geographically dispersed NASA Centers -- ARC and JSC. The function that supports JPL SOC Monitoring and Detection services will be physically dispersed through a desktop support contractor. The equipment that supports the NASA SOC is geographically dispersed with alternative standby equipment operating in either a warm or hot state. The equipment that support JPL SOC will be geographically dispersed between JPL and an external site through the desktop support contractor. The expected Service Availability Objectives are as follows:

Service	Service Availability Objective
SIEM	98.0%
IDS	99.9%
PCAP	99.9%
Endpoint Threat Detection and Response	99.9%
Intrusion Prevention Systems	99.99%
DNS Sinkhole	98.0%
IP Sinkhole	98.0%
Security Email Gateway	99.0%

4.0 Incident Management and Service Request

JPL maintains an incident management system and Service Now portal, which is independent of NASA's solution. If an incident meets the defined criteria as stated in this document, to be considered NASA reportable, JPL interfaces with the NASA RSA Archer Incident Management System (NASA SOC IMS) to open, update, or close a report. The NASA SOC IMS will become the authoritative record, containing all official record status, tracking and resolution on the incident. The tables below identify the OLA participant's specific responsibilities for incident management and service request.

NASA SOC Responsibilities
The NASA SOC will provide an Incident Management System to allow JPL to record incident data.
The NASA SOC will provide tactics, techniques and procedures to the JPL SOC, that the NASA SOC leverages to enact network blocks, endpoint sweeps, DNS sinkhole blocks and IP sinkhole blocks.
The NASA SOC will provide Agency-level indications and warnings for threats that impact NASA or JPL systems.
The NASA SOC will collaborate in support for and coordination of planned administrative activities and unplanned incidents/issues.
The NASA SOC will collaborate with the JPL SOC to provide critical information to assist in analyzing and resolving incidents/issues.
The NASA SOC will provide event and incident data for NASA-monitored networks when JPL systems could be impacted.
The NASA SOC will provide incident tracking and reporting for the Agency. CUI, ITAR, EAR and PII incident data sent to Agency and Center CIOs in Daily Reports and Privacy Officials per occurrence. Incident status sent to CISOs, Office of Inspector General (OIG), Office of Protective Services, Office of International and Interagency Relations, Center Incident Response Manager and Center incident response teams.
The NASA SOC will provide the Agency with continuous, uninterrupted (24x7x365) event detection, situational awareness, and incident management capabilities so the Agency can maintain a sound and secure information posture.

In support of NASA SOC, the agency requires capabilities in incident response, computer forensics, incident management, event monitoring, reverse engineering, and security systems administration. The SOC provides three key services to the NASA enterprise:

- Monitoring, Detection and Prevention
- Incident Containment and Mitigation
- Reporting and Communications.

Monitoring, Detection and Prevention provides proactive and timely identification, response, and resolution of issues arising from events that indicate a compromise or that could potentially compromise a NASA information systems.

Incident Containment and Mitigation (IC&M) focuses on the isolation of anomalies which threaten NASA networks to reduce the severity or attack surface from a realized event in order to return systems or networks to normal operations.

Reporting and Communications provides strategic information used in reporting the Agency's incident-response posture to the Centers. At times, NASA also collaborates with other U.S. Federal Government entities, and external partners in furtherance of U.S. cyber security goals, initiatives, as well as responds to incidents and shares threat indicators.

The NASA SOC will provide DNS and IP sinkhole capabilities, operational 24/7 with a 3 hour on-call response time during non-business hours not inclusive of CNOC/DDI SLA's. OSINT data will be mitigated twice a day M-F normal business hours.

The NASA SOC will utilize a SIEM, in order to correlate and filter IT security events.

The OCSS will provide a log aggregation system, for the collection of IT security data. Also, the NASA SOC will provide full access to the collected Agency log data to the Center IT Security Teams. Questions regarding Agency log data should be sent to esd at esd@nasa.gov.

The JPL SOC will provide reporting – through the JPL SOC Database to the NASA IMS – all JPL-related event and incident data originating on networks that JPL manages or over which JPL is cognizant, based on the agreed-upon event/incident types based on DHS Reporting Requirements.

- Coordinates and case manages (tracks) responses to all incidents/issues.
- Serves as the POC for status on incidents/issues and provides updates on demand or via email notification list(s) provided and maintained by an impacted group or the ITSD, as appropriate.

The JPL SOC will input required incident data determined by DHS Reporting Requirements as related to IT security incidents in the SOC Incident Management System (IMS) from initial entry to closure of the incident. The initial entry made by the JPL SOC will be such that the one-hour reporting criteria to US-CERT for security incidents will be met. Further time based requirements may be modified based on DHS Reporting requirements for Federal Agencies.

JPL SOC will review IMS open JPL tickets and tasks daily and update all progress made for each ticket and task. As incidents are resolved in IMS, the JPL SOC Incident Response Manager and CISO is responsible for validating;

- Functional Impact to the system
- Informational Impact to the system

<ul style="list-style-type: none"> • Recoverability Impacts to the system • Threat Vector • Costs associated to local incident response teams <p>The aforementioned validations may change as reporting requirements from DHS are changed.</p>
The JPL SOC will collaborate with NASA Centers to capture and/or investigate forensics images upon request from the NASA SOC on an as-needed basis.
Engineers, sustains, administers, and operates a Cybersecurity infrastructure in order to monitor and assess JPL networks for indications of confirmed or possible compromised systems.
The JPL SOC will promptly review, investigate, and remediate all Tasks, Events, or Incidents recorded by the NASA SOC in the IMS related to a confirmed or suspected Cybersecurity compromise, data spillage, or malicious activity.
The JPL SOC will provide the NASA SOC with indications and warnings gathered from JPL unique toolsets, when lack of collaboration could cause Agency-wide impact.
The JPL SOC will provide After business hour support for end-user reported Cybersecurity events based on urgency of immediate actions required to mitigate a malicious activity, in accordance with the general service targets noted in section 3.1
The JPL SOC will coordinate and case manage (tracks) responses to all incidents/issues In Accordance with DHS reporting requirements.
The JPL SOC will serves as the POC to the NASA SOC for status on incidents/issues and provides updates on demand or via email notification list(s) provided and maintained by an impacted group or the ITSD, as appropriate.
The JPL SOC will provide NASA SOC all relevant logs as stated in Appendix C pursuant to the technical integration of a data stream processor located at JPL SOC. The DSP will stream each required log/data type to NASA's CSI facilities for NASA SOC Tier 1 Monitoring and Alerting.

5.0 Periodic Reviews

All parties will participate in ongoing service measurement, service analysis, and review of this OLA to ensure issues are resolved successfully. At a minimum, this OLA should be reviewed annually. Modifications to the terms of this OLA should be reviewed at a joint NASA/NMO/JPL ITSD/JPL OCM meeting. This meeting may be conducted in tandem with other NASA/JPL IT project/initiative reviews.

6.0 Configuration Management

The configuration changes of NASA managed sensors and IT tools supported by this OLA are governed by configuration control boards (CCB) related to the specific toolsets. CP, EUSP and the Cyber Security Infrastructure (CSI) have CCBs that govern configuration changes.

Scheduled operational changes and unplanned outages to the systems supporting this OLA will be reported to NASA SOC IMS users through a standardized mailing list. The configuration changes for JPL managed sensors and IT Tools supported by this OLA are governed by the JPL ITSD Change Request Management system and the JPL Enterprise Request Board.

7.0 Service Level Management and Escalation

If there are any concerns related to services definitions or service levels, contact the NASA SOC Program Executive or the NASA SOC Operations Manager for resolution.

If issues associated with this OLA are not resolved, then escalation and issue resolution can be obtained based on the table below:

Escalation Level	When to Use	Whom to Escalate
Level 1: Normal Issue Management	<ul style="list-style-type: none">When resolving day to day engagement issues	soc@nasa.gov
Level 2 Escalation	<ul style="list-style-type: none">When normal issue management has failed to achieve resolution	SOC Operations Manager
Level 3 Escalation	<ul style="list-style-type: none">When Level 2 efforts have failed or when multiple services are impacted	Associate CIO for Cybersecurity & Privacy Division, NASA NMO and the JPL CISO

If there are any concerns related to services definitions or service levels, contact the JPL SOC Team Lead or the JPL SOC Operations Manager for resolution.

If issues associated with this OLA are not resolved, then escalation and issue resolution can be obtained based on the table below:

Escalation Level	When to Use	Whom to Escalate
Level 1: Normal Issue Management	<ul style="list-style-type: none">When resolving day to day engagement issues	jplsoc-ops@jpl.nasa.gov
Level 2 Escalation	<ul style="list-style-type: none">When normal issue management has failed to achieve resolution	SOC Operations Manager/CNI Section Manager
Level 3 Escalation	<ul style="list-style-type: none">When Level 2 efforts have failed or when multiple services are impacted	JPL Chief Information Security Officer

8.0 Monitoring and Reporting

A number of deliverables include reports that are rolled into one or more of the following reports; these reports have been added to the deliverable description where applicable as well as the SLA table (attached):

- Daily Activity Report(DAR)
- Weekly CISO Report(WCR)
- Weekly Situation Report(WSR)
- Weekly Task Report(WTF)
- Weekly Threat Report(WThR)
- Weekly Signature Report(WSgR)
- Bi-Weekly Mitigation Report(BWMR)
- Monthly SMG Report(MSMG)
- Monthly CIO Report(MCIO)
- Quarterly CISO Report(QCR)

In order to support the above referenced deliverables, JPL SOC will update IMS in accordance with targets in section 3.1 General Service Targets. NASA will generate the reports.

Service Response Table is included as Appendix D

9.0 Cost

Each party will cover costs associated with the services described in this OLA for their respectively managed assets. JPL anticipates that all costs associated with the JPL provided services described in this OLA will be funded by Institutional Indirect Cost.

10.0 Security and Governance

JPL SOC will be given practicable opportunities to participate in NASA Governance Boards and working groups that deal with matters which are likely to impact JPL.

Appendix A - Acronyms

ARC	Ames Research Center
CCB	Configuration Control Board
CFIA	Computer Forensics and Incident Analysis
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSI	Cyber Security Infrastructure
CSPD	Cybersecurity and Privacy Division
CNI	Cybersecurity, Networking and Identity
CP	Communications Program
CUI	Controlled Unclassified Information
D2E2	Data Discovery Exploration Engine
DHS	Department of Homeland Security
DNS	Domain Name Service
EAR	Export Administration Regulations
EUSP	End User Services Program
FIPS	Federal Information Processing Standards
IR	Incident Response
IRM	Incident Response Manager
IRT	Incident Response Team
IMS	Incident Management System
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITSATC	IT Security Awareness and Training Center
ITSD	JPL Information and Technology Solutions Directorate
JPL	Jet Propulsion Laboratory
JPL SOC	JPL Cybersecurity Operations Center
JSC	Johnson Spaceflight Center
KSC	Kennedy Spaceflight Center
MAR	Mitigation Action Requirements
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NCCIC	National Cybersecurity and Communications Integration Center
NMO	NASA Management Office
NPD	NASA Policy Directives
NPR	NASA Policy Requirements
OCIO	Office of the Chief Information Officer
OCSS	Office of Cybersecurity Services
OIG	Office of the Inspector General
OPS	Office of Protective Services
PII	Personally Identifiable Information
RTO	Return to Operations
SAISO	Senior Agency Information Security Officer
SEG	Secure Email Gateway
SOC	Security Operations Center
TIC	Trusted Internet Connection

URL Uniform Resource Locators

Appendix B - Definitions

The following table contains definitions for key terms used in this document.

Table 1. Definitions

Term	Definition
Cybersecurity Event	A security anomaly that is under initial investigation to determine whether there is a potential threat or impact to the integrity, availability, or confidentiality of information being processed or stored.
Cybersecurity Incident	An adverse event or situation associated with electronic and/or non-electronic information, resulting in a direct and verified exploitation of a system or system of systems that impacts the integrity, availability, or confidentiality of information being processed or stored.
JPL Cybersecurity Operations Center (aka JPL SOC)	Centralized JPL team for Cybersecurity/Identity Operations and management activities.
JPL Information Technology Directorate [aka the Information and Technology Solutions Directorate (JPL ITSD)]	JPL organization responsible for architecting, engineering, managing, implementing and provisioning, and operating and supporting JPL information technology assets and the processes, policies, guidelines, and procedures associated with them.
NASA Security Operations Center (NASA SOC)	NASA organization responsible for the collection, management and DHS Communications of Cybersecurity Incidents.
Privacy Information (PII)	Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Appendix C – JPL SOC Log Integration

Group 1 Data:

- JPL DNS Logs
- JPL Firewall Logs
- JPL IDS Data
- JPL AD Logs

Group 2 Data

- JPL Web Content Filter (WCF)
- JPL Web Application Firewall (WAF)
- JPL Email
- JPL Anti-Virus

Group 3 Data

- JPL Cloud Access Logs
- JPL Boundary Routers
- JPL Intrusion Prevention System (IPS)
- JPL Virtual Privet Network (VPN) gateways

Appendix D – Response Times

Event/Service/Capability		Response Times									
		NASA SOC		Incident Response Team					Service Provider		
		Threshold	Objective	Identification	Analysis	Containment	Eradication	Recovery	Provider	Threshold	Objective
Triage	Incident Reporting - Level 5 Emergency (Black)	Immediate	Immediate	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Immediate	Immediate
	Incident Reporting - Level 4 Severe (Red)	1 Hour	Within 30 min	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		1 Hour	Within 30 Min
	Incident Reporting - Level 3 High (Orange)	Within 1 hour	Within 1 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 1 Hour	Within 1 Days
	Incident Reporting - Level 2 Medium (Yellow)	Within 2 Hours	Within 2 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 2 Hours	Within 2 Days
	Incident Reporting - Level 1 Low (Green)	Within 4 Hours	Within 1 Week	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 4 Hours	Within 1 Week
	Incident Reporting - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days			
Monitoring & Detection (Boundary Protection)	Monitoring & Detection (B.P.) - Level 5 Emergency (Black)	Immediate	Immediate	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Immediate	Immediate
	Monitoring & Detection (B.P.) - Level 4 Severe (Red)	1 Hour	Within 30 min	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		1 Hour	Within 30 Min
	Monitoring & Detection (B.P.) - Level 3 High (Orange)	Within 1 hour	Within 1 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 1 Hour	Within 1 Days
	Monitoring & Detection (B.P.) - Level 2 Medium (Yellow)	Within 2 Hours	Within 2 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 2 Hours	Within 2 Days
	Monitoring & Detection (B.P.) - Level 1 Low (Green)	Within 4 Hours	Within 1 Week	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 4 Hours	Within 1 Week
	Monitoring & Detection (B.P.) - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days			
Cyber Threat Detection (Internal Protection)	Cyber Threat Detection (I.P.) - Level 5 Emergency (Black)	1 Hour	Within 30 min	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		1 Hour	Within 30 min
	Cyber Threat Detection (I.P.) - Level 4 Severe (Red)	Within 1 hour	Within 1 Days	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		Within 1 hour	Within 1 Days
	Cyber Threat Detection (I.P.) - Level 3 High (Orange)	Within 2 Hours	Within 2 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 2 Hours	Within 2 Days
	Cyber Threat Detection (I.P.) - Level 2 Medium (Yellow)	Within 4 Hours	Within 1 Week	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 4 Hours	Within 1 Week
	Cyber Threat Detection (I.P.) - Level 1 Low (Green)	Within 5 Hours	Within 2 Weeks	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 5 Hours	Within 2 Weeks
	Cyber Threat Detection (I.P.) - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Cyber Threat Hunt	Cyber Threat Hunt - Level 5 Emergency (Black)	Identification 12 hours	Analysis 1 Day	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Identification 12 ho	Analysis 1 Day
	Cyber Threat Hunt - Level 4 Severe (Red)	Identification 12 hours	Analysis 2 Days	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		Identification 12 ho	Analysis 2 Days
	Cyber Threat Hunt - Level 3 High (Orange)	Identification 1 day	Analysis 3 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Identification 1 day	Analysis 3 Days
	Cyber Threat Hunt - Level 2 Medium (Yellow)	Identification 2 Days	Analysis 5 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Identification 2 Day	Analysis 5 Days
	Cyber Threat Hunt - Level 1 Low (Green)	Analysis 4 Days	Analysis 10 Days	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Analysis 4 Days	Analysis 10 Days
	Cyber Threat Hunt - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Cyber Forensics & Incident Analysis	Cyber Forensics & Incident Analysis -Level 5 Emergency (Black)	Analysis 1 Day	Recovery 4 Days	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Analysis 1 Day	Recovery 4 Days
	Cyber Forensics & Incident Analysis -Level 4 Severe (Red)	Analysis 2 Days	Recovery 5 Days	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		Analysis 2 Days	Recovery 5 Days
	Cyber Forensics & Incident Analysis -Level 3 High (Orange)	Analysis 3 Days	Recovery 1 Week	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Analysis 3 Days	Recovery 1 Week
	Cyber Forensics & Incident Analysis -Level 2 Medium (Yellow)	Analysis 4 Days	Recovery 2 Weeks	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Analysis 4 Days	Recovery 2 Weeks
	Cyber Forensics & Incident Analysis -Level 1 Low (Green)	Analysis 4 Days	Recovery 2 Weeks	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Analysis 4 Days	Recovery 2 Weeks
	Cyber Forensics & Incident Analysis -Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Cyber Threat Analysis & Intelligence	Cyber Threat Analysis & Intelligence -Level 5 Emergency (Black)	1 Hour	Within 30 min	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		1 Hour	Within 30 min
	Cyber Threat Analysis & Intelligence -Level 4 Severe (Red)	Within 1 hour	Within 1 Days	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		Within 1 hour	Within 1 Days
	Cyber Threat Analysis & Intelligence -Level 3 High (Orange)	Within 2 Hours	Within 2 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 2 Hours	Within 2 Days
	Cyber Threat Analysis & Intelligence -Level 2 Medium (Yellow)	Within 4 Hours	Within 1 Week	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 4 Hours	Within 1 Week
	Cyber Threat Analysis & Intelligence -Level 1 Low (Green)	Within 5 Hours	Within 2 Weeks	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 5 Hours	Within 2 Weeks
	Cyber Threat Analysis & Intelligence -Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Blocks	Incident Reporting - Level 5 Emergency (Black)	Immediate	Immediate	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Immediate	Immediate
	Incident Reporting - Level 4 Severe (Red)	1 Hour	Within 30 min	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		1 Hour	Within 30 min
	Incident Reporting - Level 3 High (Orange)	Within 1 hour	Within 1 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 1 hour	Within 1 Days
	Incident Reporting - Level 2 Medium (Yellow)	Within 2 Hours	Within 2 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 2 Hours	Within 2 Days
	Incident Reporting - Level 1 Low (Green)	Within 4 Hours	Within 1 Week	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 4 Hours	Within 1 Week
	Incident Reporting - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Exemptions	Incident Reporting - Level 5 Emergency (Black)	Immediate	Immediate	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Immediate	Immediate
	Incident Reporting - Level 4 Severe (Red)	1 Hour	Within 30 min	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		1 Hour	Within 30 min
	Incident Reporting - Level 3 High (Orange)	Within 1 hour	Within 1 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 1 hour	Within 1 Days
	Incident Reporting - Level 2 Medium (Yellow)	Within 2 Hours	Within 2 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 2 Hours	Within 2 Days
	Incident Reporting - Level 1 Low (Green)	Within 4 Hours	Within 1 Week	Within 4 Hours	Within 1 Week	Within 30 Days	Within 2 Weeks	Within 20 Days		Within 4 Hours	Within 1 Week
	Incident Reporting - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A
Information Dissemination / Reporting	Incident Reporting - Level 5 Emergency (Black)	Immediate	Immediate	Immediate	Within 1 Day	Within 2 Days	Within 3 Days	Within 4 Days		Immediate	Immediate
	Incident Reporting - Level 4 Severe (Red)	1 Hour	Within 30 min	Within 30 Minutes	Within 2 Days	Within 3 Days	Within 4 Days	Within 5 Days		1 Hour	Within 30 min
	Incident Reporting - Level 3 High (Orange)	Within 1 hour	Within 1 Days	Within 1 Hour	Within 3 Days	Within 4 Days	Within 5 Days	Within 1 Week		Within 1 hour	Within 1 Days
	Incident Reporting - Level 2 Medium (Yellow)	Within 2 Hours	Within 2 Days	Within 2 Hours	Within 5 Days	Within 1 Week	Within 10 Days	Within 2 Weeks		Within 2 Hours	Within 2 Days
	Incident Reporting - Level 1 Low (Green)	Within 4 Hours	Within 1 Week	Within 4 Hours	Within 1 Week	Within 10 Days	Within 2 Weeks	Within 20 Days		Within 4 Hours	Within 1 Week
	Incident Reporting - Level 0 Baseline (White)	N/A	N/A	Within 8 Hours	N/A	Within 2 Weeks	Within 20 Days	Within 30 Days		N/A	N/A

Appendix B: NASA Management Office Letter Subject: Guidance for Authorization To Operate (ATO) Documentation for SMD Systems

National Aeronautics and
Space Administration

NASA Management Office



June 23, 2020

Reply to NASA Management Office

TO: Richard Cook, Laboratory Associate Director

FROM: Christine Bonniksen, Contracting Officer Representative, NASA Management Office

SUBJECT: Guidance for Authorization To Operate (ATO) Documentation for SMD Systems

This memo is provided in support of JPL's request for guidance associated with the transition from the JPL unique system to the NASA Risk Information Security Compliance System (RISCS) for documentation of artifacts needed for the issuance of an Authorization to Operate (ATO). Below is the general guidance for planning purposes:

1. All systems with a PDR after the date of this letter are required to enter all required documentation into the RISCS system.
2. All development systems in Phase D or later may use a combination of Hard Copy and RISCS entry for issuance of an ATO with a plan to finalize the RISCS transition that will not exceed two years from the date of this letter.
3. All development systems not covered by either of the above may have a mixture of Hard Copy and RISCS documentation for evaluation prior to launch. A plan must be developed for transition of all information into the RISCS system with a completion date NLT 6 months after launch.
4. All operational systems shall develop a plan to transition documentation into the RISCS system within 3 years of the date of this letter or as coordinated with SMD per item 5 below with the adjusted due date documented in return correspondence.
5. NASA SMD will work with JPL to identify the project priorities within the above guidelines for completing and submitting the documentation required for the issuance of an informed ATO determination.

If there is concern this request cannot be accomplished within the current provisions of the existing Caltech Prime Contract, please contact me immediately so the necessary modification(s) may be initiated. For concerns or questions related to this request, I may be contacted at 818-354-1682.

Christine K. Bonniksen
Contracting Officer Representative
NASA Management Office

CC: Scott Morgan, JPL/ESD
Charles Whetsel, JPL/ESD
Katrina Christian, JPL/Contract Management Section

Preston Miller JPL/CISO
Randi Levin, JPL/CIO
Robert Binkley, HQ/OCIO
Marion Meissner, HQ/OCIO
Lara Petze, HQ/OCIO
Gerald Smith, HQ/SMD
Betsy Edwards, HQ/SMD
Sandra Connelly, HQ /SMD
Mayra Montrose, HQ/SMD
Marcus Watkins, HQ/NMO
Kaiser Adeni, HQ/NMO
Abe Awwad, HQ/NMO
Lynn Torres, NMO Contracting Officer
David Crouch, NASA Procurement Officer

Office of the Chief Information Officer

ICAM Implementation Plan

Directive Information

NPRs and NPDs:

NPR 2841.1 Identity, Credential, and Access Management

NPR 1600.4A Identity and Credential Management

NASA Responsible Office: Office of the Chief Information Officer

Background

Representatives of the National Aeronautics and Space Administration (NASA) and the Jet Propulsion Laboratory (JPL), hereinafter referred to as Contractor, including both Chief Information Officers, met on November 5, 2019 to discuss the scope of the Identity, Credential and Access (ICAM) Implementation Plan. As input to the implementation plan, the group first reviewed the ICAM Transition Resource Impact Assessment deliverable defined in the IT Transition Plan. Consistent with the Decision Memo Identity, Credential and Access Management (ICAM) dated December 20, 2019, NASA has directed the Contractor to continue to work on the effort for an additional 18-24 months. This Implementation Plan addresses the ICAM requirements referenced in the decision memo. A check-point Face-to-Face will be coordinated by the NASA Management Office (NMO), and include senior leaders from HQ Office of the Chief Information Officer (OCIO), HQ Office of Protective Services (OPS) and the NMO.

Purpose

ICAM is an information technology (IT) discipline that has developed out of industry's need for a branch of knowledge and a community of specialists centering on ICAM research, training, and practice. The ICAM discipline helps organizations standardize (a) management of identities, (b) safeguards related to identity, and (c) norms for referencing identities and/or handling identity data, both within and across organizations, through people, processes, and technology. The Contractor has implemented ICAM solutions in a matrixed fashion to meet the Contractor's business, administrative, and mission needs. However, the resulting ICAM architecture is not fully congruent with NASA's need for standardization and oversight. The implementation plan herein was established to fill key gaps and establish greater ICAM coordination between NASA and the Contractor.

Implementation Strategy

A list and description of each of the projects that conform the ICAM implementation plan follows.

- I. **Establish a Dedicated JPL ICAM Program Office** – the Contractor will designate a cross-functional program office to oversee JPL's ICAM efforts for enterprise risk management, effective governance, and implementation.
- II. **Establish IdMAX as the Authoritative Source for Identities** – the Contractor will streamline the collection and maintenance of identity information to ensure that IdMAX is

the authoritative source of identity for ICAM. Information will be entered directly into NASA's IdMAX.

- III. **Refine Personally Identifiable Information (PII) Data Collection** – the Contractor will analyze ICAM systems that contain PII and implement opportunities to reduce or eliminate collection and storage of PII.
- IV. **Implement Contract Agreement Identification in IdMAX** – the Contractor will analyze its contract agreement management processes and provision agreement information into IdMAX. This will align affiliated identities to their appropriate contractual agreements and document the period of performance.
- V. **Establish NASA Identities for all remote users** - the Contractor will revise the remote user process to ensure all remote users have active NASA identities and UUPICs. In addition, these remote users will be assigned logical assets and vetted via NAMS to coincide with their level of risk.
- VI. **Implement Logical Risk Assessments on JPL IT Assets** – the Contractor will perform risk assessments on logical assets to determine the appropriate NASA level of risk (LOR) and level of confidence (LOC) needed for access.
- VII. **Begin Populating NAMS with JPL IT Assets** – the Contractor will begin entering the results of Logical Risk Assessments into NAMS to facilitate access control governance and administration.
- VIII. **Complete PIV Mandatory Authentication (Logical)** – the Contractor will manage the deployment of PIV authentication for logical access to systems and applications.
- IX. **Business Impact Assessment** – the Contractor will conduct a joint Business Impact Analysis with NASA to further determine potential financial, technical, and administrative impact of the ICAM implementation.

Schedule

ICAM Project Schedule	
Project	Completion Date
Establish NASA Identities for all remote users	2/28/2020 <i>Completed</i>
Complete PIV Mandatory Authentication (<i>Temporary Suspended Due to COVID-19</i>)	*TBD
Begin Populating NAMS with JPL IT Assets	6/30/2020 <i>Completed</i>

Implement Contract Agreement Vehicle Identification in IdMAX	8/31/2020
Business Impact Analysis (BIA)	1/15/2021
Establish IdMAX as the Authoritative Source for Identities	12/31/2020
Establish a Dedicated JPL ICAM Program Office	12/31/2020
Refine Personally Identifiable Information (PII) Data Collection	11/30/2021
Implement Logical Risk Assessment JPL IT Assets	11/30/2021

*Project was scheduled for completion by June 30, 2020. Due to the mandatory telework requirements in response to COVID-19 and the ITSD resources the Contractor needs to support this effort, the Contractor suspended SmartCard/PIV-Mandatory (Logical) rollout as of March 11, 2020. Once normal activities resume the Contractor will reassess status and communicate updated completion date to the NMO.

Resources

The Contractor anticipates engaging the support of sub-contractors to execute the projects within the scheduled due dates. In doing so, the Contractor will provide the maximum practicable opportunities to Small Business Concerns during the acquisition process.

NASA Resources: Ongoing participation in the JPL ICAM workgroup and support communicating with and engaging other NASA stakeholders, as needed.

Surveillance Performance Indicators

- a) A 12-month check-point Face-to-Face will be coordinated by NMO, and include senior leaders from HQ OCIO, HQ OPS and NMO.
- b) Quarterly status reports, highlighting progress and any issues which require leadership assistance, shall be submitted through the JPL contracting office to a parallel distribution of NASA OCIO and NMO.
- c) Monthly working groups with NASA/JPL ICAM SMEs to ensure major technical project milestones/considerations are addressed. New and/or modified deliverables shall be submitted through the JPL contracting office and NMO, respectfully.

Office of the Chief Information Officer

Software License Management Implementation Plan

Directive Information

NASA Responsible Office: NASA Office of the Chief Information Office

1) Scope

Pursuant to the Information Technology Transition Plan, the focus of this Implementation Plan (the Plan) is to create a centralized and consistent set of processes, including consolidation of all commercially off the shelf software (COTS) licenses into a single Software Asset Management (SAM) System, for all categories of software except Computer Aided Engineering (CAE) software. The CAE software licensing process is addressed in the Information and Technology Solutions Directorate (ITSD) Transition Plan (formerly the OCIO Transition Plan).

In support of this goal, the Contractor will:

- Establish a cross discipline Software Acquisition Governance Team.
- Create and staff an Information Technology Asset Manager (ITAM) Position that will work closely with the NASA Agency Software Manager (ASM)
 - ITAM will obtain NASA training
- Create a set of procedures to organize and implement all seven phases of the Software License Management Lifecycle, including:
 - Approval and recording of software purchased with the Contractor Purchase Orders
 - Approval and recording of software purchased with the Contractor P-Cards
 - Approval and recording of software obtained from the Contractor's IT Catalog
- Build out and populate the Software Asset Management module in Service Now for:
 - Productivity Software (Category 1)
 - Individually purchased software for Desktops (Category 2)
 - Individually purchased/obtained software for servers
 - Chargeback software licenses
 - Enterprise Software
 - Software as a Service (SaaS).

- Create a process for identifying Free and Open Software (FOSS) and Trial Software, and work with NASA to establish guidelines for review and acceptance of associated Terms and Conditions and End User License Agreements (EULA).

The Contractor will comply with NASA's Supply Chain Risk Management requirements in accordance with the Information Security Implementation Plan requirements.

2) Exceptions

- In accordance with the ITSD Transition plan approved by NASA, CAE software is outside the scope of this Implementation Plan. The CAE software licensing process is mature, meets our contractual requirements and is auditable.
- This plan covers all COTS, including customized COTS. Unique software JPL develops for mission systems is not included.

3) Implementation Strategy

The Contractor's Implementation Strategy will be accomplished through the following actions. The Contractor, in collaboration with NASA, will:

- Complete an inventory of the Software currently in the Contractor's environment and share its results with the Software License Management System (SLMS) workgroup.
- Continue to develop the Software Asset Module (SAM) to record all software purchases.
- Create a Software Catalog in Service Now that lists the Software approved for use by the Contractor (to include Cyber and Business Governance).
- Continue to develop the Acquisition Division P-Card tracking system to ensure that the proper fields are captured.
- Train the P-Card holders on software purchases. Only trained card holders will be permitted to purchase software.
- Fully implement the SaaS review process, including communication about the use of SaaS in the Contractor's environment to the Contractor's personnel.

The Contractor will implement key areas of this strategy through the following projects:

Project 1: Software Inventory Assessment

The Software Inventory Assessment project will result in an inventory of the Software currently in the Contractor's environment. This includes the following activities.

- Determine where and which software exists in the Contractor's environment.
- Systems with BigFix installed will allow for scanning.
- The Contractor will review the last year of software procurements and renewals to determine what has been purchased and associate those purchases to the appropriate Plans.

Assumptions

- It is expected that the majority of software by titles exists in the Contractor's Information Technology Security Database (ITSDB) Plan 537 Subscribed Computers.

- It is expected that a majority of dollar value software exists in IT Plans that provide services to the Lab; that software will be identified in the Application Security Records for these systems: – Business Systems,
 - Product Data Management,
 - Collaboration, and
 - Data Exchange Architecture (DEA).
- The collection of additional deployment information as part of the Purchase Order process will enable the association of software with the appropriate System Security Plans. The Contractor will ensure that the proper fields are captured and training the P-Card holders on software purchases.

Schedule Status:

The Contractor is studied FY2019 P-Card and Purchase Order data. BigFix Discovery commenced in April 2020. The analysis was complete by the end of June 2020.

Project 2: Software Asset Module (SAM) Enhancements

This project is to continue enhancements for additional data points to be collected in the SAM for recording software purchases.

- The Contractor is working with subcontractors (ManTech and 1901 [the Service Now Developer]) to establish the data fields needed to satisfy the Software Policy.
 - The Contractor's team will create fields in the Service Now Software Asset Module that will allow for the capture of inventory data.
 - Current Fields:
 - Order Number
 - Order Date
 - Requestor
 - Card Holder
 - Card Holder Org.
 - QTY
 - Unit Cost
 - Description
 - Control Point Categories
 - Expenditure Type
 - Account
 - Transaction Date
1. Needed Fields:
 - Computer Asset Tag (system software will be installed on)
 - Manufacturer
 - Software Title
 - Valid Through Date
 2. The Contractor's ITSD will be tracking all Software Purchases including P-Card, Purchase Order and Subcontract, in a Software Asset Management (SAM) System

to ensure that JPL's use of Software is covered by the Contractor's entitlements to use the software.

- The Contractor is working with subcontractors (ManTech and 1901) and its Acquisition organization to determine how to best transmit PO and P-Card software purchase information into the SAM.
- Software as a Service (SaaS) that stores any Contractor data in a Cloud will go through a vetting process with the provider which ensures data is stored in a Fed Ramp Certified data center that meets CyberSecurity reporting requirements. Access to SaaS will require using the Contractor's Single Sign On.
- Strategy will extend to Free and Open and Trial Software. The Contractor will work with NASA to evaluate FOSS and Trial Software.

Schedule Status:

The Contractor has completed development of the SAMf module in the Service Now Sandbox. Testing and review of Stories has been completed.

All software included in the Service Now Catalog will be included in the initial Production module. As of May 2020, the Contractor has started adding new software purchases and migrating enterprise purchases. A full capture of all software could take a year to coincide with annual renewals.

4) Resources

The Contractor anticipates engaging the support of subcontractors to support a portion of the work described herein. In doing so, the Contractor will provide the maximum practicable opportunities to Small Business Concerns.

5) Surveillance Performance Indicators

Performance will be observed through the Contractor's implementation of this IP, reporting of schedule and activities found in Sections 3 and 6, and associated interaction with NASA. The Contractor will continue to participate in NASA's SLMS workgroup. All Contractor programs, plans, procedures, policies, and any guidance/directives are subject to periodic surveillance and audit by the Government. Surveillance will be evidenced by the Contractor performing the activities in this Plan, producing associated products, conducting reviews, performing assessments, reporting, and other aspects of this Plan.

6) Schedule

Action	Due Date
Software Asset management module for Service Now	May 31, 2020 <i>Completed</i>
Software Inventory Assessment	June 30, 2020 <i>Completed</i>
Software Acquisition Governance Team	September 30, 2020

Procedure and Governance Development for Software License Management Lifecycle	September 30, 2020
Data Migration into new system on rolling basis	May 31, 2021

Office of Chief Information Officer

External Websites Implementation Plan

Directive Information

NASA Responsible Office: Office of Chief Information Officer

Introduction:

In order to ensure compliance with Prime Contract No. 80NM0018D0004 (the Contract), the Contractor's Chief Information Officer (CIO) shall provide oversight to all website content developed and maintained by the Contractor, in accordance with the Statement of Work set forth in Section C-1 of the Contract. The Contractor is required to use the NASA.gov web portal for web hosting when appropriate. The Contractor may host some sites outside NASA's web hosting service when a different information architecture or technical capability is needed that is not provided by the existing NASA web portal, in accordance with the strategy set forth in this Plan. NASA.gov websites hosted outside of the NASA.gov portal shall also follow the requirements listed in the Contract. Pursuant to the Information Technology Transition Plan, the focus of this Implementation Plan (the Plan) is to document the strategy for compliance with the May 15, 2019, Memorandum from the NASA Administrator addressing the Web Modernization effort and the 21st Century Integrated Digital Experience Act (IDEA), for websites managed by the Contractor that fall within the scope of this Memorandum.

In support of this work, the Contractor:

- Will establish a new process for creation of external websites by September 30, 2020
- Has worked on developing governance control over website content
 - New JPL Rules expected September 30, 2020
- Has reduced footprint by 20%

Implementation Strategy

- a) Consistent with the directives outlined in the NASA Administrator's May 15, 2019, Memorandum addressing the Web Modernization effort and the 21st Century Integrated Digital Experience Act (IDEA), the Contractor fulfills requirements for websites managed by the Contractor that fall within the scope of the Web Modernization effort and the 21st Century Integrated Digital Experience Act Memorandum and IDEA.
 - i) The Contractor is participating in the NASA OCIO Website Policy Working Group. NASA has established the NASA Web Modernization Team (NWMT) as an Agency working group to determine how NASA, as an Agency, will implement the 21st Century Integrated Digital Experiences Act (IDEA) as well as the NASA Administrator's memorandum concerning the same topic. A copy of the Administrator's Memo is included as Appendix A.

- ii For sites that need to be hosted externally, new sites will be addressed per NWMT process. Existing websites will be reviewed through NWMT processes and documented.

- ii The Contractor's Information and Technology Solutions Directorate (formerly known as OCIO) will assess all recommended actions from the NWMT within 30 days of receipt. The Contractor will respond through NMO with its recommended action or approach for NASA's consideration. In the event a timeline is included as part of the recommended action and the timeline is sooner than 30 days, the Contractor will make its best effort to expedite its response.

Surveillance Performance Indicators

- b) Every 6 months, after initial submittal of the External Website Governance Implementation Plan (IP), the Contractor will submit a status update through the NMO, culminating with the completion of the final recommendation(s) from the NWMT. The status update will identify all actions from the NWMT and how the Contractor plans to implement or has implemented the actions at JPL. If the actions have not been implemented, the process to do so along with a schedule for compliance will be provided.

Project Schedule

Action	Due Date	Status
NWMT Recommendation: Employee-Only Sites	April 20, 2020	Completed
NWMT Recommendation: Eliminate unknown (404 of 403 errors) sites as appropriate	April 20 2020	Completed
NWMT Recommendation: Vanity Sites	June 30, 2020	Completed
NWMT Recommendation: Login Website Audit	June 30, 2020	Completed initial audit. The Contractor completed the Login Website Audit and is developing a strategy to complete all required actions, including the development and launch of a communication

		plan. We anticipate completion of all required actions by end of calendar year 2020.
Establishment of New Process for External Websites Creation	September 30, 2020	In progress
NWMT Recommendation: Redirect Groups of Related Sites to a Single URL	September 30, 2020 Address 75% of sites with aliases and redirects and provide a strategy for addressing 100% of sites.	In progress
Formalize Governance Control through Publication of JPL Rules	September 30, 2020	In progress
Status Update	Every 6-months	Ongoing
Assess NWMT Recommended Actions and Respond with the Contractor's Recommended Approach for NASA's Consideration	Within 30-days of receipt	Ongoing

Appendix A: NASA Administrator's Memorandum

Subject: Web Modernization and Enhanced Security Protocols



May 15, 2019

TO: NASA Workforce

FROM: Administrator

SUBJECT: Web Site Modernization and Enhanced Security Protocols

Every day we communicate NASA's life-changing accomplishments in science, exploration, and discovery. As an Agency, we have much to be proud of – our content is compelling, visually appealing, and reaches millions of viewers around the globe, making us one of the most popular brands on the planet. Yet, our online and strategic communications efforts have not evolved at a speed that appropriately protects our Agency's assets or best represents our brand.

Currently there are an estimated 3,000 public-facing NASA Web sites, yet the top 10 sites receive 80 percent of all Web traffic. Additionally, some NASA partners operate Web sites on our behalf outside of the Agency, creating redundancy and accumulating unnecessary costs. Not only does this duplication of information cause confusion, each Web site provides potential access for a cyber-attack on NASA's assets.

The shutdown earlier this year gave us a clear view of the cyber vulnerabilities inherent in operating thousands of Web sites. We need to take steps to protect our resources in a hostile cyber landscape, examine our digital footprint, reduce costs, and maximize the effectiveness of communications efforts. In addition to security risk, multiple sites dilute our effectiveness in communicating key messages about our missions.

This effort to reduce the number of public-facing Web sites will also enable NASA to move toward full compliance with the 21st Century Integrated Digital Experience Act (IDEA). Signed into law on Dec. 20, 2018, the Act requires agencies to exercise governance over their Web sites and ensure legacy Web sites are regularly reviewed, eliminated, and consolidated.

ACTION:

I am calling for a full modernization of NASA's digital presence to best reflect the priorities and activities of the Agency in this new era of science, discovery, and exploration. To accomplish that we will:

1) Create a team to evaluate and consolidate Web sites

I have asked the Associate Administrator for Communications (OCOM), Bettina Inclán, and the Chief Information Officer (OCIO), Renee Wynn, to do a full review of NASA's Web

footprint and digital presence. They are tasked with improving these resources for the entire Agency, making communications more effective, strengthening our technological and cyber security capabilities, while reducing costs for the Agency. Their top objective is to create a process to consolidate NASA Web sites and help lead a redesign of NASA.gov. I expect this effort to result in an enhanced cyber posture and an improved focus for communicating our messages.

Bettina and Renee will assemble a team to evaluate all of NASA's Web sites and provide a plan for consolidation across the Agency. The team will immediately review the entire Agency's digital footprint that will include universities and other affiliated Web sites. They will follow up with more specific plans to address the ongoing cyber threats and how OCOM and OCIO can best work together to counter these issues, maximize resources, and provide a better platform to communicate NASA's story.

2) Comply with the IDEA Act

The deadline for all newly created Web sites and digital services to comply with the IDEA Act is **June 18, 2019**. Going forward, all Government Web sites must have a consistent appearance and not overlap or duplicate existing sites and services. The law also calls for an increase in analytics and metrics.

3) Enact a moratorium on new Web sites

In order to meet these goals, effective immediately, there is an indefinite freeze on creating any and all new NASA Web sites. This includes programs, projects, Centers, Mission Directorates and institutions creating Web sites in the nasa.gov domain, and contractors creating sites in the *.edu, *.org or any and all other domains.

4) Web site redesign

NASA.gov needs a refresh. For many of our NASA storytellers and creative communicators, the resources on this aging design limit their possibilities and ingenuity. Because of this, and more, NASA.gov will undergo a major redesign in 2019. A new NASA.gov will allow for more compelling content, better design, and additional innovative opportunities and stronger cyber security features.

In collaboration with current site owners, the redesign of NASA.gov will result in the development of a new and expanded suite of site templates, tools, and features that will integrate content from other NASA sites into the Agency's enterprise Web site as part of this consolidation process. The redesign will include important existing infrastructure and include Google Analytics metrics (a requirement for all Federal Web sites), an approved security plan, scalable bandwidth, a content management system, 508 compliance, and a responsive design for mobile devices.

Moving forward, resources should focus on content and protecting NASA from cyber incidents. Visitors to the NASA home page should easily understand and see the breadth of NASA's mission and benefits to society. The goal is to consolidate all NASA content intended for the public under one Web site, www.nasa.gov. As always, this enterprise site is a service provided to the entire Agency.

intended for the public under one Web site, www.nasa.gov. As always, this enterprise site is a service provided to the entire Agency.


The new NASA.gov will be the primary site for Agency news, in-depth reference information on missions, and other topics intended for external audiences. Moving compelling content from separate subdomain Web sites to NASA.gov will be encouraged, and for some content, required.

BUILDING THE TEAM:

If you or any members of your team want to provide feedback or would like to participate in this process, please reach out to Bettina and Renee.

We look forward to working with you to protect NASA assets and help modernize the digital experience for the public and our partners. This is an exciting opportunity to refresh and modernize NASA's digital presence and ensure we have the tools that best represent the NASA brand. With your support, this effort can have a positive and powerful impact in expanding NASA's reach, highlighting the good work being done by our NASA team and improve our cyber security.

Thank you in advance for working together to keep NASA's assets secure and ensuring continued success in communicating NASA's story.



James F. Bridenstine