National Aeronautics and
Space Administration
Washington, DC 20546

Procurement Class Deviation

PCD 21-01B

September 3, 2024

Class Deviation from the NASA FAR Supplement: Implementation of Controlled Unclassified Information (CUI) Program.
NASA Case 2021-N003

PURPOSE: To provide a class deviation from the NFS to revise NFS Clause 1852.204-76 Security Requirements for Unclassified Information Technology Resources, in order to implement the Controlled Unclassified Information (CUI) Program. Also, update security plan requirements to align with the Federal Information System Management Act (FISMA) policy for IT Security Plans for Federal Information Systems (FIS).

GUIDANCE: In November 2010, the United States President issued EO 13556 to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls" pursuant to and consistent with law, regulations, and government-wide policies.

Prior to that time, more than 100 different markings for such information existed across the executive branch. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency specific policies are often hidden from public view has only aggravated these issues.

As a result, EO 13556 established the CUI Program to standardize and simplify the way the executive branch handles unclassified information that requires safeguarding, or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies.

SBU protective markings are already being applied when required to documents related to procurement actions. This action changes the marking being used and in some cases the manner in which the marking is applied to covered documents. Guidance and training is being provided by the OCIO related to the implementation of this new marking.

Federal policies include the FISMA of 2022, Homeland Security Presidential Directive (HSPD) 12, Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.), OMB Circular A-130, Management of Federal Information Resources, and the National Institute of Standards and Technology (NIST) security requirements and standards. These requirements safeguard IT services provided to NASA such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems.

NASA IT security policies and procedures for unclassified information and IT are prescribed in NASA Policy Directive (NPD) 2810, Security of Information Technology; NASA Procedural Requirements (NPR) 2810, Security of Information Technology; and interim policy updates in the form of NASA Information Technology Requirements (NITR). IT services must be performed in accordance with these policies and procedures.

***ACTION REQUIRED BY CONTRACTING OFFICERS*:**

During this transition period from SBU to CUI, NASA personnel have the option to use either the SBU or CUI unclassified information control programs. CUI is required to be fully implemented at NASA by December 31, 2021.

Documents created prior to October 1, 2021, and prior to NASA CUI implementation are considered legacy information and are not required to be reviewed and re-marked unless they contain information that qualifies as CUI AND the information is reused and expected to be transmitted outside of NASA.

Existing contracts issued prior to effective date of the PCD must be modified to include the new version of NFS 1852-204.76 to reflect the changes to IT security requirements for unclassified IT resources. This change can be implemented at any time after the issuance of the PCD, but must occur no later than November 29, 2024, to ensure IT Security Plans and required training are handled in accordance with current policy.

EFFECTIVE DATE: This PCD is effective as dated and shall remain in effect until the NFS is revised. ~~on or about October 1, 2021~~

***CLAUSE CHANGES*:** NFS 1852.240-76

HEADQUARTERS CONTACT: Brittney Chappell, Procurement Analyst, HQs Procurement and Grants Division, Brittney.V.Chappell@nasa.gov

Marvin Horne

Digitally signed by Marvin Horne
Date: 2024.09.03 09:17:21 -04'00'

Karla Smith Jackson
Assistant Administrator for Procurement

Enclosure

- Additions to baseline made by proposed rule are indicated by **[bold text in brackets]**
- Deletions to baseline made by proposed rule are indicated by ~~strikethroughs~~
- Five asterisks (* * * * *) indicate that there are no revisions between the preceding and following sections
- Three asterisks (* * *) indicate that there are no revisions between the material shown within a subsection

* * * * *

PART 1852
SOLICITATION PROVISIONS AND CONTRACT CLAUSES

TABLE OF CONTENTS

* * * * *

1852.204-76 Security Requirements for Unclassified Information Technology Resources.
As prescribed in 1804.470-4(a), insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES
(~~JAN 2011~~**[DEVIATION 21-01B]**)

* * * * *

(b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include Sensitive But Unclassified (SBU) information **[or Controlled Unclassified Information (CUI)]**, for NASA in support of NASA's missions, programs, projects and/or institutional requirements. Applicable requirements, regulations, policies, and guidelines are identified in the **[contract]** ~~Applicable Documents List (ADL) provided as an attachment to the contract. The documents listed in the ADL can be found at: http://www.nasa.gov/offices/ocio/itsecurity/index.html.~~ **[The NASA data requirements description (DRD), "Security Requirements for Unclassified Information Technology Resources," defines specific implementation requirements for this clause.]** For policy information considered sensitive, the documents will be identified as such in the **[contract]** ~~ADL~~ and made available through the Contracting Officer.

* * *

(3) **[Federal information system (FIS). The term "Federal information system" means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency (40 U.S.C. §11331)]**

~~IT Security Management Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Unlike the IT security plan, which addresses the IT system, the IT Security Management Plan~~

~~addresses how the contractor will manage personnel and processes associated with IT Security on the instant contract.~~

(4) **[Information System Security Plan (i.e., System Security Plan, IT Security Plan, or Security Plan) A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.]** ~~IT Security Plan. This is a FISMA requirement; see the ADL for applicable requirements. The IT Security Plan is specific to the IT System and not the contract. Within 30 days after award, the contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer; the approval authority will be included in the ADL. All contractor personnel requiring physical or logical access to NASA IT resources must complete NASA's annual IT Security Awareness training. Refer to the IT Training policy located in the IT Security Web site at https://itsecurity.nasa.gov/policies/index.html.~~

(d) **[Contractors that process, store, or transmit federal information or operate information systems on behalf of the federal government shall meet the same security and privacy requirements as federal agencies. The contractor shall develop and submit an Information System Security Plan when operating a FIS or maintaining or collecting information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government. Such FIS plans are to be accomplished in accordance with the current version of NASA Procedural Requirements (NPR) 2810.1 Security of Information and Information Systems. The security plan and Authorization to Operate (ATO) shall be in place before any system may operate in the NASA environment. When the contractor does not operate a FIS but receives, process, transmits, or stores NASA information in performance of the contract, the contractor shall attest to the ability to secure NASA information within its own IT/information system.]**

(e) The contractor shall afford Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of NASA Electronic Information or to the function of IT systems operated on behalf of NASA, and to preserve evidence of computer crime. **[The contractor shall report immediately upon notification any incident involving NASA information on nonfederal (contractor) systems.]**

~~At the completion of the contract, the contractor shall return all NASA information and IT resources provided to the contractor during the performance of the contract in accordance with retention documentation available in the ADL. The contractor shall provide a listing of all NASA Electronic information and IT resources generated in performance of the contract. At that time, the contractor shall request disposition instructions from the Contracting Officer. The Contracting Officer will provide disposition instructions within 30 calendar days of the contractor's request. Parts of the clause and referenced ADL may be waived by the contracting officer, if the contractor's ongoing IT security program meets or exceeds the requirements of NASA Procedural Requirements (NPR) 2810.1 in effect at time of award. The current version of NPR 2810.1 is referenced in the ADL. The contractor shall submit a written waiver request to the Contracting Officer within 30 days of award. The waiver request~~

~~will be reviewed by the Center IT Security Manager. If approved, the Contractor Officer will notify the contractor, by contract modification, which parts of the clause or provisions of the ADL are waived.~~

(f) **[The contractor shall provide the name and contact information for the contractor's IT Security point of contact during phase in of the contract. Contractor employees ~~subject to this contract~~ requiring physical access to NASA facilities or electronic access to NASA systems] shall complete the NASA Cybersecurity and Privacy Awareness Training]**

[g] The contractor shall insert this clause, including this paragraph in all subcontracts that process, manage, access or store NASA Electronic Information in support of the mission of the Agency.

* * * * *

(End of clause)