National Aeronautics and
Space Administration
Washington, DC 20546

Procurement Class Deviation

PCD 25-22

September 13, 2025

CLASS DEVIATION FROM FEDERAL ACQUISITION REGULATION (FAR) PART 40 TO IMPLEMENT THE REVOLUTIONARY FAR OVERHAUL (NASA Case 2025-N024)

PURPOSE: To provide a Class Deviation from the FAR to implement the FAR Council's model deviation text to FAR Part 40, Information Security and Supply Chain Security, and establish NFS 1840, Information Security and Supply Chain Security**.**

BACKGROUND: On April 15, 2025, the Executive Order (E.O.) 14275, "Restoring Common Sense to Federal Procurement" was signed. Section 2 of the E.O. establishes the policy that the FAR "should only contain provisions required by statute or essential to sound procurement, and any FAR provisions that do not advance these objectives should be removed." To implement E.O. 14275, the Office of Federal Procurement Policy (OFPP) is leading the **Revolutionary FAR Overhaul (RFO)** initiative. This effort is supported by the Federal Acquisition Regulatory Council (the Council) member agencies— General Services Administration, Department of Defense, and NASA, along with other agencies. In line with the E.O., the initiative aims to eliminate unnecessary regulations and policies across all levels of the federal government.

The Office of Management and Budget (OMB) memorandum, M-25-26 issued on May 2, 2025, titled, Overhauling the Federal Acquisition Regulation, provided additional guidance to federal agencies regarding the FAR overhaul.

FAR Streamlining. As part of the RFO, the FAR will be streamlined to include only statutory requirements, while non-statutory content will move to new buying guides, collectively forming the Strategic Acquisition Guidance (SAG). The Council will first issue model deviation guidance by FAR part, followed by formal rulemaking through the notice-and-comment process. Agencies will have 30 days to issue class deviations based on the model text once it is released.

Streamlining Agency Acquisition Supplements. Agencies must streamline their FAR supplements by removing regulations not based on statute or executive orders and aligning with the FAR Council's deviation guidance. Supporting policies must also be updated to reflect these changes. This approach ensures the NASA FAR Supplement (NFS) remains consistent with the streamlined FAR.

FAR Buying Guides and NFS Companion Guide (CG) (coming soon). As the FAR and the NFS are streamlined, helpful non-regulatory content will be moved to new FAR Buying Guides and NFS CG. These guides are intended to offer practical instructions and best practices for implementing effective contracting methods.

RFO Part 40, establishes broad security requirements that apply to acquisitions of products and services. Burdensome, duplicative, or outdated language and language not required by statute have been removed from FAR Part 40. This plain language version of FAR Part 40 shall be adhered to.

GUIDANCE:

(1) Contracting officers shall follow the RFO Part 40 deviated text instead of FAR Part 40 as codified at 48 CFR Chapter 40. The FAR Council's RFO text is available at FAR Overhaul - Part 40 | Acquisition.GOV.

(2) COs shall also follow the NFS Part 1840 text enclosed within this deviation.

***ACTION REQUIRED BY CONTRACTING OFFICERS*:** Effectively immediately, ensure that new contract actions issued on or after the effective date complies with the policy in the PCD.

EFFECTIVE DATE: This PCD is effective as dated and shall remain in effect until implemented in the FAR and NFS or otherwise rescinded.

***PROVISION AND CLAUSE CHANGES*:** NFS Part 1840 includes clauses 1852.240-75, Classification Requirements and 1852.240-75, Security Requirements for Unclassified Information Technology Resources, which were formerly associated with NFS 1804. These clauses have been updated and renumbered to correspond with the requirement's location in Part 1840.

HEADQUARTERS CONTACT: Erica Jones, NFS Manager, HQs Procurement and Grants Policy Division, Erica.D.Jones@nasa.gov

Marvin Horne

Digitally signed by Marvin Horne
Date: 2025.09.11 05:49:14 -04'00'

Marvin L. Horne
Acting Assistant Administrator for Procurement
Enclosure

Changes in the NFS Deviation text below are identified as follows:
Deletions shown as ~~strike throughs;~~ and additions shown as **[bold in brackets]**.

[PART 1840
INFORMATION SECURITY AND SUPPLY CHAIN SECURITY

TABLE OF CONTENTS

[PART 1840
INFORMATION SECURITY AND SUPPLY CHAIN SECURITY]

[Subpart 1840.3 - Safeguarding Information]

[1840.302 Safeguarding Classified Information within Industry

1840.302-3 Contract clause.

The contracting officer must insert clause 1852.240-75, Security Classification Requirements, in solicitations and contracts if work to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the acquisition and installation.]

[1840.370 Safeguarding Unclassified Information Technology (IT) Resources.

This section implements NASA's acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems. Federal policies include the Federal Information System Management Act (FISMA) of 2002, 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.

1840.470-4 Contract clause.

[(a) Insert clause 1852.240-76, Security Requirements for Unclassified Information Technology Resources, in all solicitations and awards when contract performance requires contractors to—

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(b) Parts of the clause and referenced Applicable Documents List (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 must 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.]

[1852.240-75 Security Classification Requirements.
As prescribed in 1840.302-3, insert the following clause:

SECURITY CLASSIFICATION REQUIREMENTS
(DEVIATION SEPT 2025)

Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of _____ [insert the applicable security clearance level]. See Federal Acquisition Regulation clause 52.240-92 in this contract and DD Form 254, Contract Security Classification Specification, Attachment _____ [Insert the attachment number of the DD Form 254].

[1852.240-76 Security Requirements for Unclassified Information Technology Resources.
As prescribed in 1840.470-4(a), insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES
(DEVIATION SEPT 2025)

(a) The contractor must protect the confidentiality, integrity, and availability of NASA Electronic Information and Information Technology (IT) resources and protect NASA Electronic Information from unauthorized disclosure.

(b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include 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 contract. The NASA data requirements description (DRD), "Security 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 and made available through the contracting officer.

(c) *Definitions*.

(1) IT resources means any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

(2) NASA Electronic Information is any data (as defined in the Rights in Data clause of this contract) or information (including information incidental to contract administration, such as financial, administrative, cost or pricing, or management information) that is processed, managed, accessed or stored on an IT system(s) in the performance of a NASA contract.

(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)

(4) Information System Security Plan (i.e., System Security Plan, IT Security Plan, or Security Plan) means 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.

(d) Contractors that process, store, or transmit Federal information or operate information systems on behalf of the federal government must meet the same security and privacy requirements as federal agencies. The contractor must develop and submit an Information 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) must 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 must attest to the ability to secure NASA information within its own IT/information system.

(e) The contractor must afford Government access to the contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access must 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 must report immediately upon notification any incident involving NASA information on non-federal (contractor) systems.

(f) The contractor must provide the name and contact information for the contractor's IT security point of contact during phase in of the contract. Contractor employees requiring physical access to NASA facilities or electronic access to NASA systems must complete the NASA Cybersecurity and Privacy Awareness Training.

(g) The contractor must 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)]