ATTACHMENT N

DATA REQUIREMENTS DESCRIPTION-2 (DRD-2)
SECURITY REQUIREMENTS FOR UNCLASSIFIED IT RESOURCES

RFP 80GSFC26R0006

1. DRD Title: Security Requirements for Unclassified IT Resources		
2. DRD No.: 2	**3. Data Type:** 1	**4. OPR: OCIO**
5. Solicitation No.: 80GSFC26R0006	**6. Contract No.: TBD**	
7. Date Issued: 12/10/2025	**8. Date Revised:** N/A	**9. DRD Category:** **Technical** ☒ **Administrative** ☐ **S&MA** ☐

10. Description/Use: To ensure that IT security requirements, including training, and Cyber Supply Chain Risk Management (C-SCRM), are met during performance of this contract.

11. Distribution: All deliverables required by this DRD, except for the C-SCRM plan, shall be submitted electronically to the CO, COR, and NASA Organization's Information System Security Officer (ISSO) (i.e., Security Officer). Approval will be provided by the ISSO. If the organization does not have an ISSO, approval will be provided by the NASA Information Owner. C-SCRM plans shall be submitted to and approved by the ICT/C-SCRM Service Element Lead at agency-dl-ocio-cys-cp-scrm@mail.nasa.gov.

Initial Submission:
Information System Security and C-SCRM Plan(s): For contractor-owned systems, due at the start of phase-in. Initial submission not required for existing, approved plans for Government-owned and Contractor-managed systems. For new Federal Information Systems, due with the delivery of the system.

Non-Federal System Certification: Prior to any transfer of NASA non-public information to the contractor, the contractor shall provide documentation of the certification of the non-federal system to the security officer of the NASA organization that owns the information (typically the organization responsible for the contract). If the organization does not have an ISSO, the attestation shall be provided to the NASA Information Owner.

Information on Employees in Sensitive Positions/Assignments Report: At the start of phase-in

IT Security Point of Contact: At the start of phase-in

IT Security Awareness Training: Training required prior to access to NASA information and systems.

IT Security Role Based Training: Foundational training is provided prior to performance of assigned role. Initial evidence showing completion due at the end of phase-in.

Submission Frequency:
Information System Security Plan(s) and C-SCRM Plan: As Required

Non-Federal System Certification: Annually

Information on Employees in Sensitive Positions/Assignments Report: Annually

IT Security Point of Contact: As Required

IT Security Awareness Training: Annual on anniversary date of initial training

IT Security Role Based Training: Annual on anniversary date of initial training. Evidence of completion due annually.

Format: Unless otherwise directed, the data requested in this DRD shall be delivered to the Government in soft-copy via an electronic transfer mechanism (e.g., electronic mail, flash drive, or file transfer protocol) in a format readable by a Government device utilizing the standards in NASA-STD-2804, "Minimum Interoperability Software Suite."

Interrelationship: Contract Requirements and Statement of Work sections related to Information Technology

Applicable Documents: Most current versions of the following:
FAR 52.240-91, Security Prohibitions and Exclusions
FAR 52.240-93, Basic Safeguarding of Covered Contractor Information Systems
FISMA 2014, Federal Information Security Modernization Act 2014
NFS 1852.240-76, Security Requirements for Unclassified IT Resources
NFS 1852.226-73, Major Breach of Safety or Security
NFS 1852.237-72, Access to Sensitive Information
NFS 1852.237-73, Release of Sensitive Information
NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NPR 1382.1, NASA Privacy Procedural Requirements
NPD 2810.1, Information Security Policy
NPR 2810.1, Security of Information and Information Systems
NPR 2810.7, Controlled Unclassified Information
NPR 7120.7, NASA Information Technology Program and Project Management Requirements
OMB Circular A-130, Management of Federal Information Resources

Scope: All contracts that purchase, lease, network to, or otherwise utilize covered articles, which includes Government-funded IT (as defined by the FAR) must comply with NASA IT Security and C-SCRM Requirements.

Contents: The Federal Information Security Modernization Act (FISMA) and Executive Branch policy require external providers that process, store, or transmit federal information or operate information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies.

Information System Security Plan (i.e., System Security Plan, IT Security Plan, or Security Plan):
When the contractor is operating a Federal Information System (FIS) on behalf of NASA or is providing a FIS in the execution of this contract, that system must have an Information System Security Plan in accordance with NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Information Systems and Organizations" at the revision number required at the issuance of the contract. This plan and supporting documents shall be entered into the NASA cybersecurity system of record pursuant to Authorization to Operate (ATO) requirements set forth in NASA Policy Directive 2810.1, "NASA Information Security Policy" and NASA Procedural Requirement (NPR) 2810.1, "Security of Information and Information Systems." The FIS security plan and ATO must be in place before any system may operate in the NASA environment.

NON-FEDERAL SYSTEM SECURITY CERTIFICATION

When the contractor will receive, process, store or transmit NASA non-public information, especially Controlled Unclassified Information (CUI) including Personally Identifiable Information (PII) on a non-federal system (e.g., the contractor's corporate system) the system must meet the requirements for data protections detailed in NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

This documentation may take the form of:

a. A third-party review/audit certifying that the non-federal system meets the requirements of NIST SP 800-171 or equivalent standard of information protection, such as the ISO 27001 standard, for example.
b. A certification from another federal agency such as the DOD Cybersecurity Maturity Model Certification (CMMC) Level 2.

INCIDENT NOTIFICATION

The contractor shall report immediately upon notification any incident involving NASA information on nonfederal (contractor) systems to SOC@nasa.gov.

IT SECURITY POINT OF CONTACT:

The contractor shall identify a point of contact that NASA may reach in its attempt to address IT and cybersecurity issues. The point of contact shall have the authority to ensure the immediate notification of the NASA Security Operations Center of any incident involving NASA information.

IT SECURITY AWARENESS TRAINING:

Contractor employees subject to this contract, defined as those requiring physical access to NASA facilities or electronic access to NASA systems, shall complete the NASA approved IT Security Awareness Training annually. NASA Cybersecurity and Privacy Awareness training is available through the SATERN online system and must be completed prior to access to NASA information and systems. Completion of the training is tracked automatedly by NASA and must recur each year by the anniversary of the initial training as a condition of continued access. Cybersecurity and Privacy training is updated throughout the year as needed, so there is no defined training period.

CYBERSECURITY AND PRIVACY ROLE BASED TRAINING:

Contractor employees subject to this contract shall complete NASA's Cybersecurity and Privacy Role-Based Security Training in SATERN related to the following role-based functions prior to performing the role:

- Information System Owner (ISO)
- Information Systems Security Officer (ISSO)
- Information System Security Engineer (ISSE)

NAMS access to these roles in the Risk Information Security Compliance System (RISCS) will be restricted to those that have completed the role-based training within a year of the previous training. Only the training specified in SATERN will be valid for the purpose of fulfilling the training requirement and those who do not take the training annually may be suspended from RISCS access.

INFORMATION ON EMPLOYEES IN SENSITIVE POSITION(S)/ASSIGNMENTS REPORT:

The Information on Employees is Sensitive. IT Security (ITS) Positions/Assignments Report shall provide information annually for personnel screening as required by NPR 2810.1(series), and NPR 1600.1 on position risk.

CYBER SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) PLAN:

NIST defines C-SCRM as a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, process, and procedures. A C-SCRM plan addressing contractor systems that will be used in performance of the contract, shall be delivered prior to the processing, transmission, or storage of non-public NASA information on these contractor systems. The C-SCRM plan shall be consistent with the template in NIST SP 800-161, "ICT SCRM Plan Template," or the attached, optional questionnaire.

Remarks: None

Maintenance:

Information System Security Plan(s) shall be kept up to date as changes to the baseline configuration of the system(s) occur.

Non-Federal System Certifications shall be maintained annually or per the certifying body's standard.

Information on Employees in Sensitive Positions/Assignments Report shall be maintained annually.

IT Security Point of Contact shall be kept up to date as changes occur.

Completion of Cybersecurity and Privacy Role Based Training is due annually in SATERN and will be tracked by NASA.

C-SCRM plans shall be kept up to date as changes occur to organizational C-SCRM processes, policies, and procedures, and/or new components are introduced.