ATTACHMENT F

RAPID IV
RFP

INFORMATION TECHNOLOGY (IT) SECURITY APPLICABLE DOCUMENTS LIST

March 2021

RFP 80GSFC19R0016 Rev 4

CONTRACT TBD

Information Technology (IT) Security Applicable Documents List
March 2021

Document	Subject
NPR 1382.1	NASA Privacy Procedural Requirements
NPD 1382.17	NASA Privacy Policy
NPD 1440.6	NASA Records Management
NPR 1441.1	NASA Records Management Program Requirements
NPD 2540.1	Personal Use of Government Office Equipment Including Information Technology
NPD 2800.1	Managing Information Technology
NPR 2800.1	Managing Information Technology
NPD 2810.1	NASA Information Security Policy
NPR 2810.1	Security of Information Technology
NPD 2830.1A	NASA Enterprise Architecture
NPR 2830.1A	NASA Enterprise Architecture Procedures
NPR 2841.1	Identity, Credential, and Access Management
NPR 7120.7	NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements

NASA Records Retention Schedules (NRRS)	
Document	**Subject**
NRRS 1441.1	NASA Records Retention Schedule

Document	Subject
ITS-HBK-1382.02-01	Privacy Goals and Objectives
ITS-HBK-1382.03-01	Privacy Risk Management and Compliance: PIAs and SORNs
ITS-HBK-1382.03-02	Privacy Risk Management and Compliance: Annual Reporting Procedures for Reviewing and Reducing Personally Identifiable Information (PII) and Eliminating the Unnecessary Use of SSN
ITS-HBK-1382.04-01	Privacy and Information Security: Overview
ITS-HBK-1382.05-01	Privacy Incident Response and Management: Breach Response Team
ITS-HBK-1382.06-01	Privacy Notice and Redress: Web Privacy & Written Notice, Complaints, Access and Redress
ITS-HBK-1382.07-01	Privacy Awareness and Training: Overview
ITS-HBK-1382.08-01	Privacy Accountability: Overview
ITS-HBK-1382.09-01	Privacy Rules of Behavior and Consequences: Overview
ITS-HBK-2810.002-1	Format and Procedures for an IT Security Policies and Handbooks
ITS-HBK-1441.01.01	Records Retention and Disposition: Overview
ITS-HBK-1440.01.01	Records Planning & Management: Records
IT-HBK-2841.003	Identity, Credential, and Access Management (ICAM)
ITS-HBK-2810.02-01	Security Assessment and Authorization
ITS-HBK-2810.02-02	Security Assessment and Authorization: Information System Security Assessment and Authorization Process
ITS-HBK-2810.02-04	Security Assessment and Authorization: Continuous Monitoring – Annual Security Control Assessments

Document	Subject
ITS-HBK-2810.02-05	Security Assessment and Authorization: External Information Systems
ITS-HBK-2810.02-06	Security Assessment and Authorization: Extending and Information Systems Authorization to Operate Process and Templates
ITS-HBK-2810.02-08	Security Assessment and Authorization: Plan of Action and Milestones (POA&M)
ITS-HBK-2810.03-02	Planning
ITS-HBK-2810.04-01	Risk Assessment: Security Categorization, Risk Assessment, Vulnerability Scanning, Expedited Patching & Organizationally Defined Values
ITS-HBK-2810.05-02	Systems and Service Acquisition
ITS-HBK-2810.06-02	IT Security Awareness, Training, and Education
ITS-HBK-2810.07-02	Configuration Management
ITS-HBK-2810.08-01	Contingency Planning
ITS-HBK-2810.09-01	Incident Response and Management
ITS-HBK-2810.09-02	NASA Information Security Incident Management
ITS-HBK-2810.09-03	Collection of Electronic Data
ITS-HBK-2810.09-04	Incident Response and Management: Guidelines for Data Spillage & Sanitization Procedures
ITS-HBK-2810.10-02	Maintenance
ITS-HBK-2810.11-2	Media Protection and Sanitization
ITS-HBK-2810.12-02	Physical and Environmental Protection
ITS-HBK-2810.13-01	Personnel Security
ITS-HBK-2810.14-03	System and Information Integrity
ITS-HBK-2810.15-01	Access Control
ITS-HBK-2810.15-02	Access Control: Elevated Privileges (EP)

Document	Subject
ITS-HBK-2810.16-02	Audit and Accountability
ITS-HBK-2810.17-02	Identification and Authentication
ITS-HBK-2810.18-02	System and Communications Protection
ITS-HBK-2810.19.01	Operational Technology
ITS-HBK-2810.002-1	Format and Procedures for IT Security Policies and Handbooks: Privacy, Security & Sensitive Information

Document	Subject
NASA-STD-2804	Minimum Interoperability Software Suite
NASA-STD-2805	Minimum Hardware Configurations

Memoranda			
From	**To**	**Subject**	**Date**
Office of the Chief Information Office	Distribution	Annual Cybersecurity and Sensitive Unclassified Information Awareness Training	September 14, 2020
Chief Information Officer, Office of Procurement, and Office of Protective Services	Officials in Charge, Center Directors, CIOs, CISOs	Your Role in Protecting NASA: Ensuring No Use of Prohibited IT/Telecommunications Services or Equipment at NASA	August 26, 2020
NASA Administrator	NASA Workforce	Web Site Modernization and Enhanced Security Protocols	May 15, 2019
Chief Information Officer	Distribution	Authorizing Officials and Authorizing Official Designated Representatives	February 27, 2019
Chief Information Officer	Distribution	Use of Personally-Owned Mobile Devices to Connect to NASA Email, Calendar and Contacts Services	October 25, 2018
Chief Information Officer	Officials-in-Charge of Headquarters Offices Directors, NASA Centers	Use of Unauthorized Devices	April 16, 2018
Administrator	Officials-in-Charge of Headquarters Offices Directors, NASA Centers	Updated Guidance for Traveling Abroad with NASA IT Assets	May 17, 2017
Administrator	Officials-in-Charge of Headquarters Offices Directors, NASA Centers	Managing Software in Support of NASA's Mission	May 5, 2017
Chief Information Officer	Distribution	NASA Federal Source Code Framework	November 7, 2016
Chief Information Officer	Center Chief Information Officers, Associate CIO for Enterprise Services	Remediating Vulnerabilities in Unsupported or End of Life Software	March 30, 2016

ACIO for Information Technology Security Division, ACIO for Enterprise Services and Integration Division	Distribution	NASA Transport Layer Security (TLS) Implementation and Certificate Requirements	March 17, 2016
Chief Information Officer	Distribution	Establishment and Maintenance of Secure Communications	February 28, 2014

Reminder: Within 30 days after contract effective date, the Contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer for approval.