# Ames Procedural Requirements

## APR 2815.7

Effective Date: 1/24/2018  
Expiration Date: 1/24/2023

**COMPLIANCE IS MANDATORY**

**Subject:** Assessment and Authorization - Information Technology (IT) Security Policies and Requirements at Ames

**Responsible Office:** Code I/ Office of the Chief Information Officer (OCIO)

## DOCUMENT CHANGE LOG

<table>
<thead>
<tr>
<th>Status [Baseline /Revision /Cancelled]</th>
<th>Document Revision</th>
<th>Date of Change</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>0</td>
<td>11/7/17</td>
<td>Initial</td>
</tr>
</tbody>
</table>

Verify current version before use at:  
https://cdms.nasa.gov/directive/library/ARC
TABLE OF CONTENTS

PREFACE

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents
P.5 Measurement/Verification
P.6 Cancellation

CHAPTER 1. Overview
CHAPTER 2. Continuous Monitoring
CHAPTER 3. Personal Devices
CHAPTER 4. Awareness Training
CHAPTER 5. Assessment and Authorization for a New System
CHAPTER 6. External Systems

APPENDIX A. Definitions
APPENDIX B. Acronyms

PREFACE

P.1 PURPOSE

a. This Ames Procedural Requirements (APR) sets forth processes and procedures used to comply with IT standards and guidance for the Ames Research Center (ARC) Information Technology (IT) Security in accordance with APD 2815.1 and with NASA Policies.
b. It assigns authority, roles and responsibilities, and terms of use for the security of IT services and resources.
c. This APR supplements NPR 2810.1B for System Assessment and Authorization.

P.2 APPLICABILITY

a. This document applies to:

1. All Information Technology located at Ames Research Center and all satellite locations
2. All personnel receiving, accessing, connecting, or subscribing to ARC IT network services, data, and systems.
b. Generally excluded are contractor or research facility computing and information technology resources that are not under direct NASA management or that are merely incidental to a contract (e.g., a contractor's payroll and direct personnel system). If these systems are connected as part of the Center's network they are required to follow NASA ARC policies.

P.3 AUTHORITY

NPR 1600.A, NASA Security Program Procedural Requirements w/Change
NPD 2800.1B, NASA Policy Directive, Managing Information Technology
NPR 2841.1, Identity, Credential and Access Management Services
NPD 7120.7, Knowledge Policy on Programs and Projects,
NPR 7120.5E, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements
NID 7120.99, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements

P.4 APPICALBE DOCUMENTS

b. NPR 1450.10D, NASA Procedural Requirements, NASA Correspondence Management and Communications Standards and Style, w/Change 2, (1/21/2011)
e. !All NIST Standards and Guidance for IT Security (http://csrc.nist.gov/)

P.5 MEASUREMENT/VERIFICATION

Measurements will be collected and evaluated by the Ames CIO at least annually to assess:

a. the effectiveness of this procedural requirement by monitoring the degree of compliance with assignments of responsibility for data communication, network
availability, traffic, establishment of security plans, review of security controls, and documented authorizations that security plans are adequately implemented.
b. trends involving security incidents and trends for tracking metrics involving the cost, schedule impact, and impact on a mission, program, and project performance attributed to the loss, alteration, unavailability, misuse, or unauthorized access to or modification of Agency information or IT resources.

**P.6 CANCELLATION**

None

______________________________

/S/

Eugene Tu
Director

**Distribution Statement: CDMS**!
CHAPTER 1. Overview

1.1 This APR is organized to be aligned with the NPR 2810.1 security control chapters covering management, operational and technical controls. For the majority of controls there exists a corresponding NASA Handbook found in a secure location within the agency CIO web page. The NASA Handbooks are the primary source of reference after the NPRs and NASA Interim Directives (NID) and generally define roles and responsibilities. However, some controls must be implemented at the Center level. The remainder of this APR describes Center policy and requirements that further protect the confidentiality, integrity and availability of NASA information and technology. At times one center activity or policy can cover more than one ITS control.

1.2 Information security covers not just information but all infrastructure that facilitates its use such as processes, systems, services, technology, user awareness training, etc., and including computers (government owned & non-government owned), tablets and iPads, voice, and data networks. NASA is required to develop an IT security strategy in the initiation phase per NPD 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements, and NPR 7120.5E, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements, for each system that lays out the end-to-end IT security, which is defined as "safeguarding information from point of origin to point of destination."

1.3 The overall objective of the Information Technology (IT) Security policies is to provide requirements and direction to safeguard the availability, confidentiality, and integrity of all IT resources connected to NASA-Managed networks at Ames Research Center.

1.4 All IT resources at Ames Research Center (ARC), such as data, information, applications, and systems, are subject to the Federal Information Security Management Act (FISMA), the NASA Policy Requirements (NPRs) 2810.1x & 1600.1, all NASA IT Security Handbooks, the Federal Information Processing Standards (FIPS) 199 & 200; and all NIST Standards and Guidance for IT Security.
CHAPTER 2. Continuous Monitoring

2.1 Refer to "ITS-HBK-2810.02-04A: Continuous Monitoring" for details on roles and requirements.

2.2 Continuous monitoring requires the review of the required critical controls annually and all other controls incrementally at the discretion of the system owner, with all controls being reviewed at least once during the 3-year certification life cycle.

2.3 Controls are to be independently assessed (see Appendix A for definition)

2.4 All controls must be reviewed annually and must be tested at least once during the three-year cycle.

2.5 This includes the testing of the Contingency Plan for the system, refer to ITS-HBK-2810.08-01, Contingency Planning, for additional details

2.6 To assist in the annual testing refer to ITS-HBK-2810.08-02, Contingency Planning: Guidance and Templates for Plan Development, Maintenance, and Test

2.7 Testing using various methods is also required, see Table 1 below:

<table>
<thead>
<tr>
<th>System Category</th>
<th>Year 1 – Test Type</th>
<th>Year 2 – Test Type</th>
<th>Year 3 – Test Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Classroom Exercises/Tabletop Written Test</td>
<td>Classroom Exercises/Tabletop Written Test</td>
<td>Classroom Exercises/Tabletop Written Test</td>
</tr>
<tr>
<td>Moderate</td>
<td>Classroom Exercises/Tabletop Test with Scenarios</td>
<td>Classroom Exercises/Tabletop Test</td>
<td>Functional Exercises/Simulation Exercise Integrated Test</td>
</tr>
<tr>
<td>High</td>
<td>Functional Exercises/Simulation Exercise</td>
<td>Functional Exercises/Simulation Exercise</td>
<td>Functional Exercises/Alternate Site Test Integrated Test</td>
</tr>
</tbody>
</table>

Table 1 from ITS-HBK-2810.08-01, Contingency Planning

2.8 Included in the annual testing is an updated Risk Analysis of the system, refer to ITS-HBK-2810.04-01A, Risk Assessment: Security Categorization, Risk Assessment, and Vulnerability Scanning, Expedited Patching, & Organizational Defined Values


2.10 OMB requires that annual security control testing be performed within one year of the issue date of the security plan.
2.11 NASA mandates all FISMA requirements be closed out by the last work day in July.

2.12 System owners are required to maintain a reference to which controls have been tested on what schedule in order to ensure that ALL controls have been tested every three years. System owner’s knowledge of this schedule will be audited by A&A.
CHAPTER 3. Personal Devices


3.1 NASA civil servants and contractor employees (including co-ops, students, remote staff, etc.) shall be individually responsible and accountable for proper and legal use of IT resources owned by, or operated on behalf of, the U.S. Government.

3.2 All NASA civil servants and contractor employees (including co-ops, students, remote staff, etc.) are collectively responsible for protecting public confidence and financial investment in NASA.

3.3 At ARC Personal Devices used for official NASA business (e-mails, documents, etc.) are to be treated the same as any external contractor system.

3.3.1 Personal Device hardware owner will be known as the ISO. The ISO will submit documents in accordance with ITS-HBK-2810.02-05, Security Assessment and Authorization: External Information Systems

3.3.2 ARC CIO will be the authority to sign the NF1776, Authorization to Store/Process NASA Information on an External System

3.3.2.1 In the event that the ARC CIO or immediate staff request the use of a personal device then the ARC Deputy Center Director or designee will sign as the authority on the NF1776, Authorization to Store/Process NASA Information on an External System.

3.3.2.2 Authorization not to exceed one-year

3.4 ISO & equipment shall comply/meet NASA Agency PKI directives and usage instructions for encrypting NASA information resources (see http://pki.nasa.gov).

3.5 Any device (government owned or non-government owned) connecting to a NASA or ARC networks shall meet or exceed NASA IT Security requirements.

3.5.1 Personal Devices on NASA & ARC Networks:

3.5.1.1 Connecting any IT resource to NASA or ARC networks is prohibited without ensuring that it meets the minimal ITS standards by having the system scanned for vulnerabilities.

a. Vulnerabilities discovered shall be corrected or mitigated before the system is utilized on NASA & ARC networks.
b. Vulnerabilities discovered by NASA after the system is already on the network must be remediated within 30 days or the device will be banned from the network.

3.5.1.2 Using personal devices connected to NASA or ARC networks is prohibited except when connecting to the Center VPN system or to the Center guest network.

3.6 Storing any NASA information on unapproved non-NASA online storage facilities (drop box, box.net, g-mail, yahoo mail, etc.) is prohibited without advance concurrence by the ARC CIO.

3.7 Storing any NASA SBU, CUI, or PII data on non-NASA equipment, devices, online storage facilities, etc. is strictly prohibited.

3.8 Protect NASA information against accidental leakage in accordance with the requirements of the National Institute of Standards and Technology (see NIST SP800-88).

3.9 Any electronic storage device that has ever contained NASA information, even for a brief period of time, must be sanitized before it can be reassigned, transferred, or discarded. (See ITS-HBK 0035, Digital Media Sanitation.)
CHAPTER 4. IT Security Awareness Training

NASA civil servants and contractor employees (including co-ops, students, remote staff, etc.) shall be individually responsible and accountable for proper and legal use of IT resources owned by, or operated on behalf of, the U.S. Government. All NASA civil servants and contractor employees (including co-ops, students, remote staff, etc.) are collectively responsible for protecting public confidence and financial investment in NASA.

4.1 All NASA civil servants and contractor employees (including co-ops, students, remote staff, etc.) shall complete the annual required training for their NASA role pertaining to IT Security, refer to ITS-HBK-2810.06-01, Security Awareness and Training.

4.2 NASA users shall complete appropriate role-based information security-related training, as outlined in ITS-HBK-2810.150-02, that addresses the procedures and processes necessary to meet the security requirements of the position before being authorized privileged access to the information, information system and/or IT resources and complete the training annually thereafter.

4.3 Employee managers, supervisors, and system owners shall ensure that their staff and/or end-users accessing NASA information, information systems and/or IT resources under their authority are in compliance:

4.3.1 Compliance shall be renewed annually – annual deadline is set each year by NASA OCIO.

4.3.2 If staff and/or end-users accessing NASA information, information systems and/or IT resources under their authority are not in compliance, then the employee’s managers, supervisors, and system owners shall remove the staff and/or end-users access to all NASA information, information systems and/or IT resources until such a time that the staff and/or end-user come into compliance.

4.4 Training methods:

4.4.1 Preferred method for administering and tracking training is via SATERN (Agency training tool).
4.4.2 Employee’s managers, supervisors, system owners, and organizational Computer Security Officials (CSO) can administer the training to individuals or groups by projecting the SATERN course in a meeting or by using presentation material.

4.4.2.1 An ink signature sign-in log (include staff’s full name, AUID, employer name, supervisor name, phone number, and signature) or an “Appropriate Use Form” will need to be provided to the ARC CISO.

4.4.2.2 Once the ARC OCIO receives the log or form, the information will be manually uploaded into SATERN.
CHAPTER 5. Assessment and Authorization for a New System

Assessment and Authorization Resources: Current Assessment & Authorization (A&A) related resources, including Policies, Procedures, Standards, and Guidelines, can be accessed via the following links and publications:

5.1 http://nodis3.gsfc.nasa.gov/policy_lib.cfm
5.2 https://nodis-dms.gsfc.nasa.gov/NASA_Wide/restricted_directives/OCIO/OCIO_list.cfm
5.3 https://teams.share.nasa.gov/hq/ocio/security/itscommunity/GRC/SitePages/Home.aspx?InitialTabId=Ribbon.ListItem&VisibilityContext=WSSTabPersistence
5.4 https://sp.ksc.nasa.gov/sites/cso/CA/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fcso%2FCA%2FSecurity%2FSA%2FRMS%20to%20ITSC%20Transition
5.5 A&A Handbooks and Publications:
5.5.1 The NASA handbooks and NIST publications that pertain to A&A of Federal IT systems are contained within the collection of ITS-HBKs located at https://nodis-dms.gsfc.nasa.gov/NASA_Wide/restricted_directives/OCIO/OCIO_list.cfm
5.5.2 NIST SP documents at http://csrc.nist.gov/publications/PubsSPs.html. Please follow these procedures when processing A&A for any NASA IT System.

5.6 IT Purchasing Requirements:

5.6.1 All information technology components purchased that fall under an existing certified system must provide a current and valid System Security Plan (SSP) number. Current listing of active/approved IT Systems at ARC are posted at:

https://teams.share.nasa.gov/arc/i/bmo/Lists/SSP%20List/AllItems.aspx?InitialTabId=Ribbon%2ERead&VisibilityContext=WSSTabPersistence#InplviewHash20330c7c-ce92-493f-a355-412b1f2043e2=InitialTabId%3DRibbon%252EREad-VisibilityContext%3DSortField%3DOrg_x0020_Code-SortDir%3DAsc

5.6.2 Purchase orders for components not associated with an SSP will not be processed.
5.6.3 Those systems that are "new" and are not yet associated with a Security Plan must work with the ARC CISO office and provide at least Security Categorization level documents (which include but not limited to a Risk Analysis, a NF1748 & a NF1746A) that would show the type of data being processed and the categorization.

5.7 Core A&A Life Cycle Requirements:
NPR 7120.5E, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements, 12/03/2015, shall be used.

5.7.1 All systems must be certified through the A&A process every year as a minimum, refer to NASA ITS-HBKs for details.

5.7.2 Any significant change to a system shall require the system to undergo another A&A prior to Authorization to Operate (ATO) expiration, refer to NIST SP 800-37 for further guidance. Examples of significant changes to system that should be reviewed for possible re-accreditation may include but are not limited to:

5.7.2.1 Installation of a new or upgraded operating system, middleware component, or application;
5.7.2.2 Modifications to system ports, protocols, or services;
5.7.2.3 Installation of a new or upgraded hardware platform or firmware component; or
5.7.2.4 Modifications to cryptographic modules or services.

5.7.3 Each case should be discussed with relevant CISO for Center or Mission Area.

5.7.4 Changes in laws, directives, policies, or regulations, while not always related directly to the information system, can also potentially affect the security of the system and trigger an A&A action.

5.7.5 IT System controls shall be compliant with NIST SP 800-53 Rev x within one year of final release date or by deadline set by NASA HQ OCIO.

5.8 Reporting Requirements:

5.8.1 Organizations that have systems undergoing A&A must keep the ARC AAO and CISO appraised of their A&A status on a monthly basis.

5.8.2 System Owners must have ongoing communication and coordination with their assigned Computer Security Officials (CSO) towards keeping current with Federal, Agency, and Center IT security policies, procedures, standards, and guidelines.

5.9 Plan of Actions and Milestones (POA&Ms):

5.9.1 POA&Ms generated either by an A&A, OIG, OMB, or other audit must be entered into the current NASA System Security Plan Repository (NSSPR).
5.9.2 The current NSSPR is the application all NASA system owners shall use to create, store, and process their authorization packages, which contain their system security plans and all associated security, assessment, and authorization documentation.

5.9.3 Where possible documents are to be entered into the NSSPR natively. POA&Ms are to be updated in NSSPR monthly but no later than 5-working days after the scheduled due date of the POAM closure.

5.9.4 FISMA and Agency guidelines require POA&Ms to be resolved within one year from date of discovery.

5.9.5 POA&Ms shall not be extended. If resolution due date is missed the POA&M will be reported to HQ OCIO and OMB as past due at 30, 60, 90 and 120 day intervals. This will be reflected on the Federal Scorecard for NASA.

5.9.6 NIST SP 800-53 Security Controls under consideration for risk acceptance are required to be entered into NSSPR as findings during the assessment process.

5.9.7 A POA&M is to be generated for the finding until the Authorizing Official (AO) formally approves the risk acceptance via the authorization review process.

5.9.8 After the ATO is signed the POA&M can be annotated as risk accepted in NSSPR. Supporting rationale justifying the risk acceptance shall be documented in the test results section of the authorization package associated with the system in NSSPR.

5.10 Independent-Assessment (see Appendix A for definition):

5.10.1 System Owners shall have their IT systems controls independently assessed prior to submitting and requesting an ATO.

5.10.2 Security Plan Assessments shall be recoded directly into NSSPR. Uploading a document specifying the completion of an Assessment will not be accepted during the Security Plan Revalidation.
CHAPTER 6. External Systems

6.1 External Systems connecting to NASA or processing/storing NASA data:
6.1.1 Definition of an External System:
6.1.1.1 An information system or component of an information system that is outside of
the authorization boundary established by NASA and for which the government typically
has no direct control over the application of required security controls or the assessment
of security control effectiveness.
6.1.1.2 The term external should not be interpreted as or equated to meaning
physically external. A distributed system will have elements that are
physically/geographically distributed while being logically within the same authorization
boundary. NIST Special Publication 800-160, at B-5.
Questions to consider:
   a. Connected to NASA network or company network?
   b. IT System to process, analyze, store NASA data (raw, filtered, etc.)?
   c. Company to provide via a contract vehicle software,
   d. application, hardware, etc. to be integrated into a NASA
      project/program (shuttle, space station, rovers, etc.)

6.1.2 External Systems to NASA shall adhere to:
6.1.2.1 NASA ITS-HBK- 2810.02-05, Security Assessment and Authorization: External
Information Systems
6.1.2.2 ITS-HBK-2810.02-04A, Continuous Monitoring
APPENDIX A. Definitions

Access. The ability to obtain or change information or data. Within a system, "access" is the interaction between a subject (e.g., person, process, or device) and an object (e.g., record, file, program, or device) that results in the flow of information from one to the other. The nature or type of access can be read, write, execute, append, modify, delete, and create.

Availability. The state wherein information, data, and systems are in the place needed by the user, at the proper time, and in the form that the user requests.

Boundary. A designated perimeter that is used to differentiate between internal and external entities. In Information Technology (IT) security planning, a boundary is a border that is used to identify the IT resources for which an IT security official is responsible. It identifies the scope of an IT security planning effort.

Confidentiality. Holding sensitive data in confidence such that distribution is limited to those individuals or organizations with an established need to know.

Configuration control. The management process of controlling the specific elements that compose IT and controlling changes to these elements; the process that ensures that only authorized and approved changes of or to these elements are made. Configuration control includes, but is not limited to, hardware, firmware, and software elements.

Controls. Protective measures used to improve security by reducing risks, also known as "safeguards," "countermeasures," or "security features".

Facility. Designated locations in which a logical group of one or more IT resources are located.

Firewall. A computer, router, and/or other communications device that filters access to a protected network. A firewall may also consist of a collaboration of such components geared toward protecting networks from unwarranted intrusion from the Internet while allowing users inside the network access to services on the Internet, such as Web and e-mail services.

Independent assessment. Any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Individual or group (assessor) does not have root access to the system on a daily operations level, nor do they oversee policy, guidance, management, or maintenance on the system.
Integrity. State that exists when computerized data are the same as data in source documents or have been correctly computed from source data and have not been exposed to accidental or malicious alteration or destruction.

Organization computer security official. The designated Government person who is assigned the task of managing and maintaining the security of IT resources within their organizational element.

Physical controls. Barriers and deterrents used against threats to IT resources and sensitive information, including, but not limited to locks, guards, badges, and alarms.

Remote logon. Accessing one system by way of another without having to log on to the destination host. For example, accessing System B by logging on to System A and linking directly from System A to System B without logging on a second time.

Risk. The probability that a system is vulnerable to a threat that may cause harm or loss. If there is no vulnerability, regardless of the seriousness of the threat, there is no risk. Conversely, if there is no threat, regardless of the seriousness of the vulnerability, there is no risk.

Unauthorized access. The accessing of system(s) and/or processes using methods that are neither approved nor certified by the system and/or System Administrators.

Waiver. The determination and documentation by the responsible line manager that the risks of not implementing a given requirement are acceptable to the system in question and to other systems to which it may be networked. A waiver is accomplished by evaluating the threats and vulnerabilities through the normal risk-management process.

Visiting personnel. Any person visiting Ames Research Center (ARC) for a purpose other than NASA business. All visiting personnel must have a NASA sponsor. Visiting personnel students / family members taking a tour of the Center or individuals allowed on the Ames campus for special seminars are examples of visiting personnel.
### APPENDIX B. Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAO</td>
<td>Assessment and Authorization Official</td>
</tr>
<tr>
<td>AC</td>
<td>Access Control</td>
</tr>
<tr>
<td>ACES</td>
<td>Agency Consolidated End-user Services</td>
</tr>
<tr>
<td>AIRM</td>
<td>Agency Incident Response Manager</td>
</tr>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>AODR</td>
<td>Authorizing Official Designated Representative</td>
</tr>
<tr>
<td>ASCS</td>
<td>Agency Security Configuration Standards</td>
</tr>
<tr>
<td>ASUS</td>
<td>Agency Security Update System</td>
</tr>
<tr>
<td>AVAR</td>
<td>Agency Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>CAO</td>
<td>Certification and Accreditation Official (obsolete terminology)</td>
</tr>
<tr>
<td>CCA</td>
<td>Clinger- Cohen Act</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CO</td>
<td>Agency Contracting Officer</td>
</tr>
<tr>
<td>COR</td>
<td>Contracting Officer Representative</td>
</tr>
<tr>
<td>COTR</td>
<td>Contracting Officer Technical Representative</td>
</tr>
<tr>
<td>CPC</td>
<td>Contingency Planning Coordinator</td>
</tr>
<tr>
<td>CPIC</td>
<td>Capital Planning Investment Control</td>
</tr>
<tr>
<td>CPM</td>
<td>Center Privacy Manager</td>
</tr>
<tr>
<td>EA</td>
<td>Enterprise Architecture</td>
</tr>
<tr>
<td>EIT</td>
<td>Electronic and Information Technology</td>
</tr>
<tr>
<td>ELMT</td>
<td>Enterprise License Management Team</td>
</tr>
<tr>
<td>EP</td>
<td>Elevated Privileges</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IO</td>
<td>Information Owner</td>
</tr>
<tr>
<td>IRM</td>
<td>Information Resource Management</td>
</tr>
<tr>
<td>IRM</td>
<td>Incident Response Manager</td>
</tr>
<tr>
<td>ISO</td>
<td>Information System Owner</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information System Security Officer</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITS</td>
<td>Information Technology Security</td>
</tr>
<tr>
<td>ITSATC</td>
<td>Information Technology Security Awareness and Training Center</td>
</tr>
<tr>
<td>ITSD</td>
<td>Information Technology Security Division</td>
</tr>
<tr>
<td>ITS-HBK</td>
<td>Information Technology Security Handbook</td>
</tr>
</tbody>
</table>

Verify current version before use at: https://cdms.nasa.gov/directive/library/ARC
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSM</td>
<td>Information Technology Security Manager (obsolete terminology)</td>
</tr>
<tr>
<td>ITSSP</td>
<td>Information Technology System Security Plan</td>
</tr>
<tr>
<td>NAMS</td>
<td>NASA Access Management System</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NFS</td>
<td>NASA Federal Acquisition Regulation Supplement</td>
</tr>
<tr>
<td>NIRWG</td>
<td>NASA Incident Response Working Group</td>
</tr>
<tr>
<td>NISN</td>
<td>NASA Information Systems Network</td>
</tr>
<tr>
<td>NITR</td>
<td>NASA Information Technology Requirement</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>NODIS</td>
<td>NASA Online Directives Information System</td>
</tr>
<tr>
<td>NPD</td>
<td>NASA Procedural Directive</td>
</tr>
<tr>
<td>NPR</td>
<td>NASA Procedural Requirements</td>
</tr>
<tr>
<td>NSSC</td>
<td>NASA Shared Services Center</td>
</tr>
<tr>
<td>OCIO</td>
<td>Office of the Chief Information Officer</td>
</tr>
<tr>
<td>OCSO</td>
<td>Organizational Computer Security Official</td>
</tr>
<tr>
<td>OGC</td>
<td>Office of the General Counsel</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of the Inspector General</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OPS</td>
<td>Office of Protective Services</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Data Assistant</td>
</tr>
<tr>
<td>PII</td>
<td>Personally, Identifiable Information</td>
</tr>
<tr>
<td>PPM</td>
<td>Privacy Programs Manager</td>
</tr>
<tr>
<td>SA</td>
<td>System and Services Acquisitions</td>
</tr>
<tr>
<td>SAISO</td>
<td>Senior Agency Information Security Officer</td>
</tr>
<tr>
<td>SAOP</td>
<td>Senior Agency Official for Privacy</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Control Assessor</td>
</tr>
<tr>
<td>SCRM</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>SIBC</td>
<td>Summary Investment Business Case</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>TCED</td>
<td>Targeted Collection of Electronic Data</td>
</tr>
</tbody>
</table>