



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1A

Effective Date: August 12,
2013

Expiration Date: August 12,
2018

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements

Responsible Office: Office of Protective Services

[| TOC](#) | [| Preface](#) | [| Chapter1](#) | [| Chapter2](#) | [| Chapter3](#) | [| Chapter4](#) | [| Chapter5](#) | [| Chapter6](#) | [| AppendixA](#)
[| AppendixB](#) | [| AppendixC](#) | [| AppendixD](#) | [| AppendixE](#) | [| AppendixF](#) | [| AppendixG](#) | [| AppendixH](#) | [| ALL](#)

Appendix A. Definitions

Access — The ability, opportunity, and authority to gain knowledge of information or gain authorized entry onto a NASA property, leased facilities, and IT resources.

Adjudication — The evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is: suitable for Government employment; eligible for logical and physical access; eligible for access to classified information; eligible to hold a sensitive position; or fit to perform work for or on behalf of the Government as a contractor employee.

Arrest — Seizure of the person without warrant based on probable cause he/she has committed a felony or a misdemeanor in the presence of the officer. Subjecting the person to the will and control of the officer; circumstances that would lead a reasonable person to believe that he/she was not free to leave the presence of the officer. Brief detention for purposes of ascertaining a person's identity and/or activities, without more, is not an arrest.

Arrest Authority — The power to execute arrests, without a warrant, and to conduct searches incident to an arrest, granted to designated NASA security officials and security services contractors, as defined in 14 C.F.R. Part 1203b.

Asset — A system, object, person, or any combination thereof, that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Center Chief of Protective Services/Center Chief of Security (CCPS/CCS) — The senior Center security official responsible for technical management and day-to-day operations of the Center's security program.

Certification — A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Certifying Authority (CA) — Individual responsible for ensuring and certifying to the Designated Approving Authority, that requisite security measures are implemented for IT systems identified for processing of classified information.

Certifying Officials — The AA, OPS or the CCPS/CCS when so delegated, who are, by virtue of this NPR, authorized to certify that an individual has met established requirements (training, firearms qualification), can perform those security functions designated in their position description, and can carry a firearm in performance of their security duties. They can also approve the use of a security room, vault, or container for storage of CNSI.

Classification Category — The specific degree of security classification that has been assigned to CNSI to indicate the extent of protection required in the national interest:

a. **Confidential Information** — The unauthorized disclosure of which reasonably could be expected to cause damage to national security that the Original Classification Authority (OCA) is able to identify or describe.

b. **Secret Information** — The unauthorized disclosure of which reasonably could be expected to cause serious

damage to national security that the OCA is able to identify or describe.

c. Top Secret Information — The unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security that the OCA is able to identify or describe.

Classified information — Information that has been determined pursuant to Executive Order 13526, or a successor or predecessor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.) to require protection against unauthorized disclosure.

Classified Material — Any physical object on which CNSI is recorded or is embodied that shall be discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information (CNSI) — Information that must be protected against unauthorized disclosure IAW Executive Order 13526, "Classified National Security Information," and is marked to indicate its classified status when in documentary form. See definition for "Classification Category" above.

Compromise — The improper or unauthorized disclosure of or access to CNSI.

Contractor — An expert or consultant (not appointed under Section 5 USC § 3109) to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of any agency, including all subcontractors; a personal services contractor; or any other category of person who performs work for or on behalf of NASA (but not a Federal employee).

Counterintelligence (CI) — Information gathered and activities conducted to protect against espionage and sabotage and other intelligence activities conducted for or on behalf of foreign powers, organizations, or persons or international terrorist activities, but not including personnel, physical, document, or communications security.

Critical Infrastructure — Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Public Law 107-56, U.S. Patriot Act Section 1016 (e))

Debarment — Official determination made in writing by OPM or the Center OHCM that bars, for cause, an individual from accessing NASA property.

Denial of Security Clearance — The adjudication decision that an individual's initial access to classified information would pose a risk to national security, after review procedures set forth in Executive Order 12968 have been exercised. Designated Approving Authority (DAA) — Official who formally assumes responsibility for operating an Information Technology Systems or network at an acceptable level of risk.

Director, Security Management Division (DSMD) — Official assigned to OPS responsible for Agency management of physical security, personnel security, industrial security, and program security.

Electronic Access Control System — Electromechanical and electronic devices that monitor and permit or deny entry and exit of a protected area by personnel or vehicles.

Electronic Control Device (ECD) — Designed to disrupt a subject's central nervous system by means of deploying battery-powered electrical energy sufficient to cause uncontrolled muscle contractions and interrupt an individual's voluntary motor responses.

Escort — The management of a visitor's movements and/or accesses implemented through the constant presence and monitoring of the visitor by appropriately designated and properly trained U.S. Government or approved contractor personnel. Training shall include the purpose of the visit, where the individual may access the Center, where the individual may go, whom the individual is to meet, and authorized topics of discussion.

Exception — A request for a one-time exemption for compliance with a specific procedural requirement for a single event granted by the Associate Administrator, Mission Support Directorate (AA, MSD). Exceptions are for a specified period of time, normally not exceeding one year, and are granted after appropriate justification to allow a Center, organization, or program time to achieve compliance.

Executive Order (E.O.) — Official documents, numbered consecutively, through which the President of the United States manages the operations of the Federal Government.

Federal Arrest Authority (FAA) — The arrest authority granted under 14 C.F.R., Section 1203b.103 to NASA security personnel.

Infrastructure — A collection of assets. See definitions for asset and system.

Involved Member — A Protective Services contractor SPO/SO or civil service employee that has discharged a firearm while performing official duties.

Key Resources — Publicly or privately controlled resources essential to the minimal operations of the economy and

Government (Public Law 107-296, The Homeland Security Act, Section 2(9)). Key resources include such facilities as nuclear power plants, dams, Government facilities, and commercial facilities.

Lautenberg Amendment — The Lautenberg Amendment to the Gun Control Act of 1968 became effective 30 September 1996. The Lautenberg Amendment makes it a felony for anyone convicted of a misdemeanor crime of "domestic violence" (assault or attempted assault on a family member) to ship, transport, possess, or receive firearms or ammunition. There is no exception for law enforcement or security personnel engaged in official duties. The Amendment also makes it a felony for anyone to sell or issue a firearm or ammunition to a person with such a conviction. This includes NASA personnel and contractors who furnish weapons or ammunition to persons knowing, or having reason to believe, they have qualifying convictions.

NASA Limited Area — A space in which security measures are applied primarily for the safeguarding of classified information and material or unclassified property warranting special protection and in which the uncontrolled movement of visitors would permit access to such classified information and material or property. But within such space, access shall be prevented by appropriate visitor escort and other internal restrictions and controls.

NASA Critical Infrastructure (NCI) — Key resources/assets that the Agency depends upon to perform and maintain its most essential missions and operations.

NASA Critical Infrastructure Protection Program (NCIPP) — The planning and implementation of an enhanced protection level for Agency key resources identified by a NASA organization to be so crucial to the success of NASA missions as to warrant protection over that which would be routinely provided to NASA assets.

NASA Controlled Area — A space in which security measures are applied to safeguard or control property or to protect operations and functions that are vital or essential to the accomplishment of the mission assigned to a Center or Component Facility.

NASA Employees — NASA civil service personnel.

NASA Exclusion Area — A space in which security measures are applied primarily to safeguard CNSI and material with entry to that space being equivalent to access to such classified information and material.

NASA PHOTO-ID — Refers to the NASA photo-ID that has any number of embedded and external technologies capable of activating any type of facility, IT, or personal recognition access control system. Technology shall include: Exterior bar code and magnetic stripe embedded proximity chip, and embedded "smart card" chip.

NASA Policy Directive (NPD) — NPDs are policy statements that describe what is required by NASA management to achieve NASA's vision, mission, and external mandates and who is responsible for carrying out those requirements.

NASA Procedural Requirements (NPR) — NPRs provide Agency requirements to implement NASA policy as delineated in an associated NPD.

National Agency Check (NAC) — The NAC is a search of the following four indices:

- a. U.S. Office of Personnel Management (U.S. OPM) Security/Suitability Investigations Index (SII) contains investigations completed by U.S. OPM and by other Federal agencies.
- b. FBI Identification Division contains a fingerprint index and name file.
- c. FBI Records Management Division contains files and records of all other investigations (background, criminal, loyalty, intelligence).
- d. Defense Clearance and Investigations Index contains investigations, including criminal investigations, conducted on civilian and military personnel in the DoD. (Note: The NAC is not a background investigation. It is one of the components that make up a background investigation.)

National Agency Check and Inquiries (NACI) — The minimum level of background investigation conducted by the OPM required for a civil service or contractor employee to be issued a Personal Identity Verification (PIV) card.

Non-disclosure Agreement (NDA) — SF 312 is a non-disclosure agreement required under Executive Order 13526 to be signed by employees of the U.S. Federal Government or one of its contractors when they are granted a security clearance for access to classified information. The form is issued by the Information Security Oversight Office of the National Archives and Records Administration and its title is "Classified Information Nondisclosure Agreement." SF 312 prohibits confirming or repeating classified information to unauthorized individuals, even if that information is already leaked. SF 312 replaces the earlier forms SF 189 or SF 189-A. Enforcement of SF-312 is limited to civil actions to enjoin disclosure or seek monetary damages and administrative sanctions, "including reprimand, suspension, demotion, or removal, in addition to the likely loss of the security clearance."

Non-NASA Employee — Any paid worker who is not a NASA civil service employee.

Open Storage — Storage of CNSI in a security container or vault that does not incorporate secondary level storage in security containers.

Original Classification Authority (OCA) — An individual authorized in writing, either by the President, agency heads, or other senior Government officials designated by the President to classify information in the first instance.

Personally Identifiable Information (PII) — Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Reasonable Grounds or Probable Cause — Circumstances which would lead a reasonably prudent person to believe a party committed a crime; more evidence that the person is guilty than evidence the person is not but with room for doubt.

Reasonable Suspicion — Circumstances which induce a reasonable person to believe criminal activity is at hand; it justifies a SO or SPO in stopping a person and inquiring into his activities and/or identity.

Risk Acceptance — An official acknowledgement by a management official that they accept the risk posed by not implementing a recommendation or requirement, designed to reduce or mitigate the risk.

Risk Assessment (RA) — The process of identifying internal and external threats and security vulnerabilities, identifying the likelihood of an event arising from the combination of such threats and vulnerabilities. Further, the RA defines the critical security countermeasures necessary to continue an organization's operations, defines the controls in place or necessary to reduce risk, and evaluates the cost for such controls.

Risk Management — A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

Sensitive Compartmented Information (SCI) — Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or Special Access Program information.

Security Clearance — A designation identifying an individual's highest level of allowable access to classified information based upon a positive adjudication that the individual does not pose a risk to national security.

Security Officer (SO) — An armed officer, who has successfully completed the required NASA training, but who is not to exercise NASA arrest authority, whose duties may include but are not limited to: first response to emergencies, mobile patrols, temporarily detain or seize with reasonable suspicion, inspections, perimeter and internal access control, contingency posts, and crowd control. An SO may request an SPO effect an arrest when he either has directly observed any Federal offense or has reasonable grounds to believe that a felony has been committed.

Security Police Officer (SPO) — An armed officer, who has successfully completed the required NASA training, with NASA Federal arrest authority, whose duties may include but are not limited to: first response to emergencies, enforces Federal law, mobile patrols, inspections and searches, traffic enforcement, investigations, and other duties as required. An SPO may effect an arrest on request of an SO, as stated above.

Security Specialist — A qualified and trained NASA civil service employee assigned to perform certain security duties such as physical, personnel, and program security functions.

Security Survey — A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

Security Violation — An act or action by an individual or individual(s) that is in conflict with NASA security policy or procedure (including the loss or compromise of CNSI; refusal to properly display NASA Photo-ID; violation of escort policy; and security area violations). (NOTE: Does not include incidents of criminal activity, such as theft, assault, or DUI).

Sensitive But Unclassified (SBU) Information — Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises; risks to facilities, projects, or programs; threat to the security and/or safety of the source of information; or to meet access restrictions established by laws, directives, or regulations.

Special Access Program (SAP) — Any program established and approved under Executive Order 13526 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Special Agent — A qualified and credentialed NASA civil service employee assigned to perform specialized security, investigative, or law enforcement duties authorized by statute and this NPR.

Suitability — Refers to identifiable character traits and past conduct, which are sufficient to determine whether a given individual is or is not likely to be able to carry out the duties of Federal employment. Suitability is

distinguishable from a person's ability to fulfill the qualification requirements of a job, as measured by experience, education, knowledge, skills, and abilities. See 5 C.F.R. Part 731.

Suspension — The temporary removal of an individual's access to classified information, pending the completion of an investigation and final adjudication.

Technical Surveillance — Covert installation or modification of equipment to monitor (visually or audibly) activities within target areas or to acquire information by specialized means.

Threat Assessment — A formal, in-depth review and evaluation of the capabilities and interests of identified aggressors for the purpose of determining their potential for targeting NASA operations and assets. Used in conjunction with a Vulnerability Assessment to prepare an RA.

Unauthorized disclosure (Executive Order 13526) — A communication or physical transfer of classified information to a recipient who does not have the appropriate credentials for access or may also be the result of inadvertent disclosure.

Waiver — The approved request for a permanent or extended exemption (more than one year) for compliance with a specific procedural requirement granted by the AA, MSD.

[TOC](#)	[Preface](#)	[Chapter1](#)	[Chapter2](#)	[Chapter3](#)	[Chapter4](#)	[Chapter5](#)	[Chapter6](#)
[AppendixA](#)	[AppendixB](#)	[AppendixC](#)	[AppendixD](#)	[AppendixE](#)	[AppendixF](#)		
[AppendixG](#)	[AppendixH](#)	[ALL](#)					

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
