



NASA Policy Directive

NPD 1600.4

Effective Date: July 25, 2011
 Expiration Date: July 28, 2021

COMPLIANCE IS MANDATORY

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

Request Notification of Change (NASA Only)

Subject: National Security Programs (Revalidated with Change 1 on July 28, 2016)

Responsible Office: Office of Protective Services

Chg#	Date	Description/Comments
1	07/28/2016	Updated policy statement; added other applicability statements; updated U.S.C code to 51 U.S.C.; updated responsibility section providing the appropriate language to comply with NPR 1400.1 new requirements.

1. POLICY

- a. It is NASA's policy to define security responsibilities on the oversight and management of all national security programs within NASA. This encompasses Special Access Programs (SAPs) and Sensitive Compartmented Information (SCI), to include all national security programs managed by NASA supporting other United States government organizations.
- b. It is NASA's policy to ensure all risk assumed by NASA to protect national security programs is coordinated with the appropriate offices. This directive establishes and identifies the security responsibilities and functions of the NASA Special Access Program Central Official (SAPCO) and the NASA Office of Protective Services (OPS) and its role as appointed by the NASA Administrator for ensuring the protection of national security programs security policy.

2. APPLICABILITY

- a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.
- b. This directive applies to the Jet Propulsion Laboratory (JPL) a Federally Funded Research and Development Center (FFRDC), and other contractors only to the extent specified or referenced in applicable contracts.
- c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.
- d. U.S. Government agencies whose personnel require access to national security programs relating to NASA are subject to this NPD.
- e. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

- a. National Aeronautics and Space Act of 1958, as amended, 51 U.S.C. 2455, Section 304.

- b. National Aeronautics and Space Act of 1958, as amended, 51 U.S.C. 2473 (c), Section 203 (c).
- c. Classified National Security Information, Executive Order (EO) 13,526, 3 C.F.R. 298 (2009).

4. APPLICABLE DOCUMENTS AND FORMS

None.

5. RESPONSIBILITY

- a. The Administrator or designee:

- (1) Renders the final decision on proposals to establish or terminate NASA national security programs, alter the scope of any approved national security program activity, and use NASA resources to support national security program intelligence activities.
- (2) Establishes and commit NASA to protecting national security programs.
- (3) Establishes and oversee the development of security policy, requirements, and guidance for SAP and SCI national security activities.
- (4) Appoints responsible individuals for all national security program activities. The appointed individuals serve as the primary point of contact with Congress, the agencies of the Executive Branch, and on all issues relating to national security programs.

- b. The Assistant Administrator (AA) or designee for Protective Services:

- (1) Develops, coordinate, and promulgate all NASA national security program policies.
- (2) Performs security oversight of NASA components managing national security program assets in accordance with established security policies and guidance.
- (3) Ensures national security programs' security policies are integrated into and consistent with the development of NASA mission needs, national security and defense strategies, technology development, implementation, and operations (including contingency operations).
- (4) Direct credentialed NASA Counterintelligence Special Agents to assess and/or investigate suspected or actual counterintelligence matters regarding NASA's national security programs. Actions of this nature will be coordinated with the NASA OIG per established protocols.
- (5) Ensures a sufficient cadre of SAP and SCI trained personnel perform Agency-unique tasks associated with national security programs.
- (6) Maintain responsibility for sufficient resources to provide the security needs defined in this directive and other interagency security agreements.
- (7) Reviews all national security program risks, mitigate these risks where applicable, and provide a risk assessment of the Agency's national security programs to the NASA Administrator or designee.
- (8) Submits reporting of national security information (NSI) within NASA program activities to Congress.

- c. The NASA SAP Coordination Official (SAPCO) and SCI Program Manager support the NASA Administrator in carrying out security oversight and management responsibilities for NSI.

- (1) The NASA SAPCO or designee shall:

- (a) Serve as the principal security point of contact in NASA for all SAP security requirements.
- (b) Act as the NASA security liaison for all other U.S. government SAPs.
- (c) Participate in security planning for new projects and testing activities.
- (d) Provide security oversight and guidance to SAP managers within NASA.
- (e) Develop, coordinate, and publish NASA SAP security management policy, instructions, and publications.
- (f) Develop, coordinate, promulgate, and oversee the implementation of special security countermeasures policy, including those associated with arms control and nonproliferation initiatives that could impact DoD- sensitive equities.
- (g) Submit SAP establishment requests to the Office of the President through the National Security Council and coordinate new activities with the DoD Under Secretary of Defense for Acquisition, Technology, and Logistics.

- (h) Develop and maintain a partnership with the program management, providing security cost, risk analysis of the program security posture, and security guidance to NASA program managers.
 - (i) Process program security documents required for approval, validate annual program security requirements, and oversee a security inspection and compliance program.
 - (j) Report cases of fraud, waste, and/or abuse of SAP resources to the appropriate authorities and to the Office of the Inspector General.
- (2) The NASA SCI Program Manager shall:
- (a) Serve as the principal point of contact in NASA for all SCI requirements.
 - (b) Act as the NASA liaison for all SCI.
 - (c) Participate in the budget and program reviews for SCI.
 - (d) Provide security oversight and guidance to SCI managers within NASA.
 - (e) Develop, coordinate, and publish SCI security policy, instructions, and publications.
 - (f) Develop, coordinate, promulgate, and oversee the implementation of Special Security Policy.
 - (g) Process program security documents required for approval, validate annual program security requirements, and oversee a security inspection and compliance program.
- d. Develop and implement processes and procedures for SCI holders to report foreign travel; provide foreign intelligence threat briefings associated with the country/countries to be visited; and conduct debriefings after completion of the travel to determine if the SCI holder was a target of foreign intelligence interest. Inform the NASA Counterintelligence Directorate of the travel so that they can comply with NASA CI policy, as appropriate.

6. DELEGATION OF AUTHORITY

- a. The NASA Administrator may redelegate authority as identified in this NPD.
- b. Each delegation will identify a specific individual to serve as the designee for the positions identified Sections in 5.a and 5.c of this NPD.
- c. The delegation of authority shall not be redelegated further without the approval of the NASA Administrator.
- d. The SAPCO authority may be delegated to a subordinate official. Such a delegation will identify, by name and position title, the subordinate official and the specific authority that is being delegated. Any further delegation of authority must be approved by the SAPCO and must also identify, by name and position title, the subordinate official.

7. MEASUREMENT/VERIFICATION

None.

8. CANCELLATION

NPD 1600.2E, NASA Security Policy dated, April 28, 2004.

Revalidated 7/28/2016, Original Signed by:

**/s/ Charles F. Bolden, Jr.
Administrator**

ATTACHMENT A.DEFINITIONS

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 SAP information.

Special Access Programs (SAP) - Any program established and approved under EO 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

ATTACHMENT B. REFERENCES

Access to Classified Information Procedures, 50 U.S.C. 435.

Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, EO 13467 (2008).

NASA Procedural Requirement 1600.1, Security Program Procedural Requirements.

NASA Special Access Program Security Guide.

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>
