



NASA Procedural Requirements

NPR 1600.2Effective Date: October 11,
2011Expiration Date: October 11,
2016**COMPLIANCE IS MANDATORY**[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: NASA Classified National Security Information (CNSI) w/Change 2 (2/12/2014)

Responsible Office: Office of Protective Services[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [ALL](#) |

Chapter 1. Introduction

1.1 Overview

1.1.1 NASA generates, receives, disseminates, and maintains an enormous amount of information, much of which is of an unclassified/non-sensitive nature with few restrictions on its use and dissemination.

1.1.2 NASA also generates, receives, stores, disseminates, and maintains CNSI under a variety of Agency programs, projects, and through partnerships and collaboration with other Federal agencies, academia, and private enterprises.

1.1.3 In accordance with Exec. Order No. 13526 and ISOO Directive No. 1, this NPR establishes Agency procedures for the proper implementation and management of a uniform system for classifying, accounting, safeguarding, and declassifying national security information generated by or in the possession of NASA.

1.1.4 Nothing in this chapter or the applicable Executive Order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act of 1974, or the National Security Act of 1947.

1.1.5 Further, this chapter defines the security review requirements for programs and projects, pursuant to NPR 7120.5 series, establishes procedures for the creation of security classification guides (SCG), as well as requirements for reviewing permanent historical documents, pursuant to Exec. Order No. 13526, as amended, and NPR 1441.1, NASA Retention Schedule, before retirement into the Federal Records Centers or the National Archives and Records Administration (NARA).

1.2 Responsibilities

1.2.1 Pursuant to Exec. Order No. 13526, the Administrator shall demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order as outlined in this section. The Administrator has designated a senior agency official (SAO) to direct and administer the information security program for managing and safeguarding CNSI in accordance with the Order.

1.2.2 The Assistant Administrator for Protective Services has been designated as the SAO responsible for providing direction and oversight for an Agency-wide administrative information security program and implementation of Aeronautics and Space Information Security Program, 14 C.F.R. Part 1203-Information Security Program, Exec. Order No. 13526, as amended, and ISOO Directive No. 1 for the protection of CNSI in NASA's custody. The AA for Protective Services shall:

- a. Establish Agency-wide procedures pertaining to the management of CNSI and material generated by or in the custody of NASA.
- b. Periodically review procedures and systems of Headquarters, Centers, (including Component Facilities), technical

support centers, and service support centers to ensure CNSI are properly protected against unauthorized disclosure or access.

c. Be responsible for the funding, maintenance, and operation of systems supporting CNSI.

1.2.3 Center Directors shall be responsible, through the respective CCPS/CCS, for ensuring proper planning and implementation of Exec. Order No. 13526 and managing classified information and material under the jurisdiction and custody of their respective Centers. This responsibility includes component activities at facilities or locations geographically separated from the parent Center.

1.2.4 The CCPS/CCS shall ensure an information security program for CNSI is developed, implemented, and maintained at a level sufficient to meet the requirements of this chapter and national-level requirements. This includes:

a. Developing and implementing appropriate processes and procedures for classifying NASA information pursuant to Exec. Order No. 13526 and other national-level requirements.

b. Developing and implementing appropriate processes and procedures for automatic declassification pursuant to Exec. Order No. 13526.

c. Developing and implementing procedures for the appropriate safeguarding of CNSI.

d. Developing and implementing an annual self-inspection program. The annual self-inspection program should evaluate the effectiveness of Center programs covering original classification, derivative classification, safeguarding (to include telecommunications, automated information systems, and network security), security violations, security education and training, and management and oversight. In addition, self-inspections include regular reviews of representative samples of Centers' original and derivative classification actions; these samples must encompass all Center activities that generate classified information. Annual self-inspection results shall be reported annually to the Director Security Management Division and will include:

(1) A description of Center's self-inspection program that provides an account of activities assessed, program areas covered, and methodology used.

(2) A summary and assessment of the findings from the self-inspection.

(3) Specific information from the review of Center's original and derivative classification actions.

(4) Actions taken or planned to correct deficiencies; and

(5) Best practices identified during self-inspections.

e. Conducting regular and periodic reviews in coordination with the OPS Security Management Division Director. The CCPS/CCS shall conduct regular and periodic reviews of NASA organizational units involved in original and derivative classification work and storage of classified material to ensure compliance with Exec. Order No. 13526, 32 C.F.R. Parts 2001 and 2003, this NPR, and any applicable local procedures. Reviews shall meet the intent of ISOO Directive No.1, Subpart C and shall be reported annually on Standard Form (SF) 311, Agency Security Classification Management Program Data Form. The annual SF-311 form is used to report all classification, declassification, derivative actions, inspections, and other security-related activities at the Center. The Center Protective Services Office will complete the SF-311 and submit the completed form to the OPS. The SF-311 is not an audit. The reviews will also help to find misclassifications that need to be corrected.

f. Losing or compromising classified information or material shall be reported immediately to the CCPS/CCS upon discovery of the incident. The Center Security Office will appoint a lead from the Center Protective Services Office to head the investigation and to contact the appropriate organizations required to complete this action.

g. The CCPS/CCS may be required to raise the security threat level or develop temporary procedures to handle national security incidents.

h. In accordance with Exec. Order No. 13526 and ISOO Directive No. 1, NISPOM, and this NPR, the CCPS/CCS are responsible for developing and administering initial training, annual refresher training, specialized training as required, and termination briefings for all NASA civil service employees and for contractor personnel as required in accordance with an official NASA contract. The training will be developed in coordination with the OPS to ensure the minimum requirements of Federal policies are met. The training will include information, industrial, personnel, and industrial security policies and procedures.

1.2.5 NASA supervisors shall ensure that personnel entrusted with classified information attend the required briefings and security awareness training provided by the Center Protective Services Office or other Government agencies that provide classified information to NASA personnel. Individuals who handle CNSI shall be fully knowledgeable of and in compliance with the provisions set forth in this NPR and Exec. Order No. 13526, as amended, established for governing, accessing, protecting, accounting for, and safeguarding classified information and material. The management of classified information will be included in individual performance plans as a critical

element as required by Section 5.4, (7) of Exec. Order No. 13526.

1.2.5.1 The Center COMSEC Officer will serve as the focal point for all COMSEC issues. The Center COMSEC Account Manager (CAM) and Alternate CAM serve as the focal point for all Center COMSEC issues.

1.2.6 All NASA and contractor personnel.

1.2.6.1 Employees entrusted with CNSI shall immediately report the following to the CCP/CCS:

- a. Loss or suspected compromise of classified information or material.
- b. Known or suspected practice or condition that compromises the proper safeguarding and handling of classified information or material.
- c. Attempts by uncleared personnel or personnel without a need-to-know to gain access to CNSI.
- d. Initial classification, downgrading, or declassification actions associated with NASA-generated information or material.

1.2.6.2 All personnel entrusted with CNSI are encouraged and expected to challenge the classification of information that they believe is improperly designated as being either classified or unclassified. Section 2.2.1.1 provides additional information. The Center Protective Services Office should be contacted for further assistance.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [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>
