



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

NASA Procedural Requirements

NPR 1660.1C
Effective Date: May 07,
2015
Expiration Date: May 07,
2020

COMPLIANCE IS MANDATORY

NASA Counterintelligence and Counterterrorism w/Change 1, May 28, 2015

Responsible Office: Office of Protective Services

Table of Contents

Change History

Preface

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

Chapter 1. Introduction

- 1.1 Overview
- 1.2 Organization
- 1.3 Responsibilities

Appendix A. Definitions

Appendix B. Acronyms

Appendix C. References

Change History

Change#	Date	Description/Comments
1	05/28/2015	Updated administrative changes to cancel NPD 1660.1B, NASA Counterintelligence and Counterterrorism Policy

Preface

P.1 Purpose

- a. This NASA Procedural Requirement (NPR) establishes requirements, responsibilities, and procedures for maintaining an Agency Counterintelligence/Counterterrorism (CI/CT) program as prescribed by the National Aeronautics and Space Act and in conformance with other applicable laws, Executive Orders (EO), Presidential Decision Directives (PDD), and Federal regulations.
- b. This NPR defines the requirements for the conduct of a Non-Title 50 Federal agency defensive CI/CT program to protect NASA personnel, information, and resources from espionage or other unauthorized intelligence collection activities undertaken on behalf of a Foreign Intelligence Entity (FIE).

P.2 Applicability

- a. This NPR is applicable to NASA Headquarters and all NASA Field Centers, including Component Facilities and Technical and Service Support Centers. This language applies to JPL, a Federally Funded Research and Development Center, other contractors, grant recipients, and parties to agreements to the extent specified or referenced in the appropriate contracts, grants, or agreements.
- b. Nothing in this NPR shall be construed as limiting the authorities of the NASA Office of Inspector General (OIG) under the Inspector General Act of 1978, as amended.
- c. This NPR stipulates the authority, procedures, and restrictions associated with CI/CT services, inquiries, and support to national security investigations conducted by appointed CI Special Agents (CISA) at Headquarters and at each NASA Field Center.
- d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

P.3 Authority

- a. National Aeronautics and Space Act, 51 U.S.C. § 20113 and 20132.
- b. NPD 1600.2, NASA Security Policy.
- c. NPD 1600.4, National Security Programs.

P.4 Applicable Documents and Forms

- a. EO 12333, December 4, 1981, United States Intelligence Activities, reprinted as amended (3 CFR 1981 Compilation).
- b. U.S.C. Title 51, National and Commercial Space Programs.
- c. The Intelligence Authorization Act for FY95, Section 811, as amended, 50 U.S.C. § 402a.
- d. EO 13556, November 4, 2010, Controlled Unclassified Information (CUI).

- e. PDD/National Security Council-12, Security Awareness and Reporting of Foreign Contacts.
- f. PDD 39, U.S. Policy on CT.
- g. NPD 2810.1, NASA Information Security Policy.
- h. NPD 1600.9, NASA Insider Threat Program.
- i. NPR 2810.1, Security of Information Technology.
- j. NPR 1080.1, Requirements for the Conduct of NASA Research and Technologies.
- k. NPR 1441.1, NASA Records Retention Schedules.
- l. NPR 1600.1, NASA Security Program Procedure Requirements.
- m. NPR 1600.2, NASA Classified National Security Information.
- n. NPR 1600.4, Identity and Credential Management.
- o. NPR 2810.1, Security of Information Technology.
- p. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.
- q. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.
- r. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.
- s. NPR 7500.2, NASA Technology Transfer Requirements.
- t. NPR 9700.1, Travel.
- u. NASA Interim Directive (NID) 1600.55, Sensitive But Unclassified (SBU) Information.
- v. National Intelligence Priorities Framework (classified).
- w. Security Environment Threat List (classified).
- x. Memorandum of Understanding (MOU) between NASA and the Federal Bureau of Investigation (FBI) (classified).
- y. MOU between the OIG and OPS, dated February 3, 2011.

P.5 Measurement/Verification

The Office of Protective Services (OPS) CI/CT Division conducts program management reviews of its ten CI/CT offices to evaluate compliance and implementation of this NPR. The reviews are conducted at least every three years or as required. Findings of these reviews are provided to the Director of CI/CT for Protective Services, Assistant Administrator for Protective Services for NASA, and when warranted, the applicable Center Director to be resolved no later than 30 days from the completion of the reviews.

P.6 Cancellation

- a. NPR 1660.1, NASA Counter Intelligence and Counterterrorism, dated November 10, 2011.

b. NPD 1660.1B, NASA Counterintelligence and Counterterrorism Policy, dated November 18, 2008.

Chapter 1: Introduction

1.1 Overview

The NASA CI/CT Program is administered in accordance with the National Aeronautics and Space Act and in conformance with other applicable laws, EOs, PDDs, Federal regulations, to include NASA CI/CT Operating Instructions (OI), NPDs and NPRs, the MOU established with the FBI, and programmatic standards established by the National CI Executive, i.e., Defensive CI/CT programs. The OI and MOU provide additional and more specific guidance not included in this NPR due to the classified nature of the information. Responsibilities and procedures were developed to allow flexibility to mitigate Center-specific national security threats.

1.2 Organization

The NASA CI/CT Program is centrally managed by the OPS CI/CT Division, and the Division is administered locally at each of the NASA Field Centers. Headquarters staffing consists of the Director of CI/CT for Protective Services (DCI), Regional Program Managers and analysts who establish policy, provide centralized program management, and provide CI/CT support to Headquarters managers and employees. The CI/CT offices at the Field Centers and their associated support facilities are staffed by CISAs responsible for implementing the core CI/CT Program services, inquiries, and support to national security investigations.

1.3 Responsibilities

1.3.1. **The Assistant Administrator for Protective Services (AA/OPS)** will oversee Agency implementation, integration of, and compliance with CI/CT national security requirements by providing direction and ensuring that adequate resources are requested to accomplish CI/CT Program services. The AA/OPS shall also provide support to national security investigations in support of the overall NASA mission in accordance with NPD 1600.2, NASA Security Policy, and NPD 1600.4, National Security Programs.

1.3.1.1. The AA/OPS designates the DCI who is responsible for representing the NASA CI/CT Program at national-level meetings, as well as directing, managing, and developing policy and procedures for the program.

1.3.2. **The DCI** is responsible for all CI/CT program services, inquiries, support to national security investigations and cyber CI/CT occurring at NASA Headquarters, Field Centers, Component Facilities and Technical and Service Support Centers, and for coordinating those matters within NASA, the U.S. Intelligence Community (USIC), and other departments and agencies. The DCI shall:

- a. Ensure the AA/OPS, the NASA Administrator, and key NASA senior executives are kept apprised of CI/CT national security matters impacting NASA. The DCI shall serve as NASA's senior subject-matter expert on CI/CT matters.
- b. Prioritize CI/CT program objectives; identify resources, training and equipment needs; and supervise the CISAs assigned at Headquarters and Center CI/CT offices.
- c. Oversee the implementation of CI/CT program policy and procedures and evaluate compliance in

accordance with OPS and CI/CT Division policies.

- d. Ensure NASA-related CI/CT national security matters are coordinated with the FBI. When reasonable belief suggests there may be a basis for an espionage or terrorism investigation, immediately refer the matter pursuant to section 811 of the Intelligence Authorization Act of 1995 [50 U.S.C. 402(a)]. Cooperation and contact with the FBI will be governed by the MOU between NASA and the FBI. The FBI assumes the role of lead investigative agency with CISA support and assistance.
- e. Oversee the NASA CI Investigation Management System for CI/CT services, inquiries, and support to national security investigations. Authorize the initiation and closure of all NASA CI/CT threat assessments and preliminary inquiries and CI/CT national security investigations supported by CISAs. This approval authority is also delegated to the Regional Program Managers.
- f. Direct the Agency's CI/CT awareness and reporting program. Ensure CI/CT offices maintain outreach programs that foster NASA personnel awareness and reporting of espionage, insider threats, FIE, and activities related to domestic and international terrorism.
- g. Maintain a defensive CI/CT foreign travel briefing and debriefing program for NASA personnel traveling on official NASA business to designated countries, Russia, and other high-threat locations as defined by the National Intelligence Priorities Framework (NIPF) or the Department of State's Security Environment Threat List (SETL).
- h. Maintain a defensive CI/CT briefing and debriefing program for NASA personnel hosting and escorting foreign visitors and assignees from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.
- i. Direct CI/CT support to NASA's Foreign National Access Management System (FNAMS) in accordance with NPR 1600.4, Identity and Credential Management. Ensure Headquarters and Center CISAs evaluate CI/CT risks of visits and assignments of foreign visitors and Lawful Permanent Residents (LPR) from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.
- j. Coordinate with the OPS Intelligence Division to obtain CI/CT analytic support.
- k. Direct CI/CT support to NASA's Insider Threat Program, as required by NPD 1600.9, NASA Insider Threat Program.
- l. Direct and prioritize CI/CT support to NASA's major technology protection programs and special activities.
- m. Direct and prioritize cyber CI/CT support to NASA's Information Security Program, which includes the Agency's Chief Information Officer (CIO), OCIO, IT Security (ITS) Division, Center Information Security Officers (CISO), and Security Operations Center (SOC) in accordance with NPD 2810.1, NASA Information Security Policy, and NPR 2810.1, Security of Information Technology:
- (1) Direct cyber CI/CT inquiries and support national security investigations of NASA's cyber environment to identify hostile foreign intelligence cyber operations, Advanced Persistent Threats (APT), and terrorism and provide threat mitigation information to enhance NASA's overall IT security posture.
- (2) Facilitate collaboration, reporting, and information sharing among the Agency's OCIO, ITS, CISO, SOC, OIG, law enforcement, USIC, and the National Cyber Investigative Joint Task Force on cyber CI/CT-related matters.

n. Coordinate CI/CT national security matters with the Office of International and Interagency Relations, Office of General Counsel, the NASA Export Control Program, and other key NASA programs and officials as necessary. Coordinate with the NASA OIG on matters of mutual concern, including cyber CI/CT and matters with potential criminal liability, in accordance with the MOU between the OIG and OPS, dated February 3, 2011, and NPD 1600.4, National Security Programs.

o. Manage and safeguard CI/CT program files and information maintained at Headquarters and Center CI/CT offices in accordance with NPR 1441.1, NASA Records Retention Schedules. Ensure CI/CT facilities meet security requirements for the use and storage of Classified National Security Information (CNSI) and establish procedural requirements that supplement requirements for the maintenance, retention, and disposition of classified information. While supplementary requirements concerning how to maintain and disposition classified records may be able to be set through other directives established by the CI/CT Program, changes to how long to retain the records shall follow the process(es) established in NPR 1441.1, which includes approval by the National Archives and Records Administration.

1.3.3. CISAs at Headquarters and Center CI/CT offices shall:

a. Ensure Headquarters senior managers, Center Directors, and Center Chiefs of Protective Services/Chiefs of Security (CCPS/CCS) are kept apprised of CI/CT national security matters impacting NASA personnel and facilities.

b. Serve as primary advisors to Headquarters senior managers, Center Directors, and CCPS/CCS on CI/CT-related matters.

c. Restrict access to sensitive CI/CT information and classified national security matters to individuals with proper clearances and a strict need to know.

d. Act as liaison and coordinate NASA CI/CT issues with the FBI, USIC, and other Federal, state, and local agencies.

e. Conduct CI/CT services and inquiries and support national security investigations in accordance with CI/CT Division policies, OIs, and the MOU between NASA and the FBI.

f. Maintain a localized CI/CT awareness and reporting program that includes:

(1) General and comprehensive CI/CT awareness briefings and training to NASA personnel. Topics shall include, but are not limited to, an overview of espionage indicators, Foreign Intelligence Entity (FIE), insider threats, terrorism, and NASA personnel reporting requirements;

(2) Refresher briefings designed to reinforce and update awareness of CI/CT issues and reporting responsibilities.

(3) Tailored CI/CT awareness briefings and training for site-specific personnel groups assigned to sensitive positions, programs, or special access programs.

(4) Procedures for reporting suspicious activities or allegations.

(5) Dissemination of CI/CT awareness and education products and materials.

g. Conduct defensive CI/CT foreign travel and foreign contact briefings and debriefings of NASA personnel traveling on official NASA business to designated countries, Russia, and other high-threat locations as defined by the NIPF or SETL in accordance with NPR 9700.1, Travel. Travel and foreign contact briefings and debriefings may be extended to include personnel traveling to international or U.S.-based conferences, symposiums, and workshops where personnel may be exposed to potential CI/CT threats. This includes travel to non-designated countries, or low-threat

locations, which involve meeting with foreign nationals from designated countries, Russia, and other high-threat locations, as defined by the NIPF or SETL.

h. Conduct defensive CI briefings and debriefings of NASA personnel hosting and escorting foreign visitors and assignees from designated countries, Russia, and other high-threat locations as defined in the NIPF or SETL, to include those NASA personnel who maintain close and continuous contact with any foreign national outside official duties.

i. Provide CI/CT support to NASA's FNAMS:

(1) Evaluate visits and assignments of foreign visitors and LPRs from designated countries, Russia, and other high-threat locations as defined by the NIPF or SETL to assess CI/CT threats. Assessments may also be extended to any foreign visitor, regardless of country status, who will be conducting NASA work that permits access to sensitive NASA information, technologies, or security areas.

(2) Provide CI/CT consultation and evaluate foreign national access for the NASA facility foreign national visit approval authority.

j. Provide CI/CT support to Agency and Center-specific technology protection programs, which includes the Office of Chief Technologist, Office of Chief Engineer, Office of Chief Scientist, Office of Chief Information Officer (OCIO), NASA's Technology Transfer Program, Research and Technology Program, Export Control Program, Office of Protective Services, and Space Asset Protection Program in support of NASA Space Flight programs and projects pursuant to NPR 1600.1, NASA Security Program Procedural Requirements; NPD 1600.2, NASA Security Policy; NPR 7120.5, NASA Space Flight Program and Project Management Requirements; NPR 1080.1, Requirements for the Conduct of NASA Research and Technologies; and NPR 7500.2, NASA Technology Transfer Requirements.

k. Provide cyber CI/CT support to Agency and Center-specific Information Security Programs, which includes the OCIO, ITS, CISO, and SOC.

l. Maintain collaborative and reciprocal relationships with NASA OIG offices and coordinate matters of mutual concern, including cyber CI/CT and matters with potential criminal liability, in accordance with the MOU between the OIG and OPS, dated February 3, 2011, and NPD 1600.4, National Security Programs.

m. Provide CI/CT support to NASA's Insider Threat Program.

n. Manage and safeguard CI office files and national security investigation records in accordance with CI/CT program policy and NASA records management and retention schedules.

1.3.4. Headquarters Managers and Center Directors shall:

a. Provide suitable office space (e.g., furniture, small conference area, and IT communication support services) for assigned CISAs to operate in a secure and mission-effective environment.

b. Ensure that all information or allegations of actual or suspected espionage or terrorism received by management are reported to the servicing CI/CT office.

c. Direct NASA personnel under their control to comply with the responsibilities under this NPR.

d. Direct NASA personnel under their control to cooperate fully in the conduct of CI/CT inquiries and national security investigations and make available all relevant NASA files (electronic and paper), documents, premises, and employees; except as limited by law; including access to records, premises, and employees through any access provision governing NASA's arrangement with third parties (e.g., contract access clauses).

e. Direct NASA program/project managers under their control to consider CI/CT support and integration in their pre-project planning, acquisition, and functional activity phases to ensure protection of NASA technology programs and activities, as required by NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

1.3.5. All NASA Personnel (Civil Service and Contractor) are required to protect CNSI, Export Controlled/Export Administrative Regulations (EAR), International Trafficking in Arms Regulations (ITAR), NASA Critical Information (NCI), SBU/CUI, proprietary, trade secret, and dual-use (commercial and military application) technologies affecting U.S. national and economic security in accordance with NPR 1600.1, NASA Security Program Procedural Requirements; NPR 1600.2, NASA Classified National Security Information; EO 13556, November 4, 2010, Implement Controlled Unclassified Information; NID 1600.55, Sensitive But Unclassified (SBU) Information; and PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts. This does not preclude other reporting requirements cited in NPR 1600.1, NASA Security Program Procedural Requirements, and NPR 1600.2, NASA Classified National Security Information. Accordingly, all NASA personnel shall:

a. Report to their servicing CI/CT office any incidents of actual or suspected loss or compromise of CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), Communications Security (COMSEC) Material and Devices, and information regarding National Security Systems (NSS).

b. Report to their servicing CI/CT office any unusual or suspicious overtures by foreign nationals or representatives of a foreign entity to acquire NASA information outside established official channels, whether or not the information is CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), COMSEC Material and Devices, and information regarding NSS according to NPR 7500.2, NASA Technology Transfer Requirements.

c. Report to their servicing CI/CT office any information regarding suspected or actual threats related to espionage or terrorism.

d. Refrain from discussing the details of any CI/CT matter under investigation to anyone not involved in the official investigative process unless authorized by a CISA.

e. Contact their servicing CI/CT office to receive an in-person CI threat briefing prior to hosting or escorting a foreign visitor and participate in a debriefing upon completion of a visit from a designated country, Russia, or other high-threat location as defined in the NIPF or SETL. Visits include meetings that are held outside NASA-controlled facilities.

f. Contact their servicing CI/CT office to receive an in-person CI/CT foreign travel briefing prior to conducting official travel to a designated country, Russia, and other high-threat locations, as defined in the NIPF or SETL. NASA civil service personnel traveling to a non-designated country shall complete an electronic briefing and debriefing e-mailed to them by the CI/CT Safeguards Foreign Travel System. All personnel can request a CI/CT travel briefing for non-official/personal travel, regardless of destination, by contacting their servicing CI/CT office. Immediately upon return from travel, report any suspected security or CI/CT incidents encountered during travel to their servicing CI/CT office. Sensitive Compartmented Information cleared personnel conducting foreign travel must contact their servicing CI/CT office to receive a CI/CT focused foreign travel threat briefing prior to departure. Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel.

g. Cooperate fully with CISAs during CI/CT inquiries and national security investigations; and, following verification of access authorization, make available all relevant NASA files (electronic

and paper), documents, premises, and employees; except as limited by law; including access to records, premises, and employees through any access provision governing NASA's arrangement with third parties (e.g., contract access clauses).

1.3.6. NASA Mission Directorates, Mission Support Offices, Program and Project Managers are responsible for the protection of NASA personnel and resources as specified by NPR 7120.5, NASA Space Flight Program and Project Management Requirements; NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; and NPR 7120.8, NASA Research and Technology Program and Project Management Requirements. Accordingly, Mission Directorates, Mission Support Offices, Program/Project Managers shall:

- a. Provide CISAs access to relevant program/project information and personnel to assist in establishing and providing the proper level of CI/CT support to a sensitive program/project or NASA NCI.
- b. Notify CISAs of any incidents, events, or circumstances of actual or suspected loss or compromise of CNSI, EAR, ITAR, NCI, SBU/CUI, proprietary, trade secret, dual-use (commercial and military application), COMSEC Material and Devices, and information regarding NSS in accordance with NPR 7500.2, NASA Technology Transfer Requirements. This does not preclude other reporting requirements cited in NPR 1600.1, NASA Security Program Procedural Requirements, and NPR 1600.2, NASA Classified National Security Information.
- c. Notify CISAs of any occurrences of unusual or suspicious contact between NASA personnel and foreign nationals.
- d. Direct program/project managers and their personnel that are working on projects with foreign nationals or foreign entities (including space agencies, universities, private companies, and individuals) to receive a tailored foreign intelligence country threat briefing from their servicing CI/CT office prior to beginning the project and on an annual basis. Require managers to track personnel attendance at these briefings by name and the date training was completed.

Appendix A. Definitions

Advanced Persistent Threat (APT) - A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

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

Counterintelligence (CI) - Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, their agents, or international terrorist organizations or activities. NASA CISAs provide defensive CI/CT support to Agency personnel, projects, and program to include CI/CT services, inquiries, and support to FBI national security investigations.

CI/CT Awareness and Reporting Program - Recognizing the best defense is a well-educated and trained workforce, this program is composed of classified and unclassified briefings designed to educate NASA personnel about espionage, insider threats, and terrorism. Includes information personnel can use to mitigate CI/CT threats, as well as guidance on individual reporting obligations.

CI/CT Awareness - A state of being aware of the sensitivity of classified or sensitive but unclassified information one possesses, collaterally aware of the many modes of operation of hostile intelligence persons and others whose interests are inimical to the U.S. while being able to recognize attempts to compromise one's information, and the actions one should take, if approached, to impart the necessary facts to trained CI/CT personnel.

CI/CT awareness products - An analysis of a CI/CT topic, event, situation, issue, or development. These products differ from an assessment in that they are often time sensitive, are published as needed or annually, and normally do not require extensive research to produce. Products of this nature ensure a consistent flow of appropriately classified or categorized threat information is available to the community to increase awareness and action as appropriate.

CI Technology Threat Assessment - A proactive, tailored assessment and analysis of select NASA programs and technologies with the intent of identifying suspected espionage activities or other indicators of FIE targeting of NASA personnel and technologies.

CI Support Plan - A formal plan that outlines and describes the focused CI support to be provided to a NASA research and development facility, program, information, event, or technology.

Cyber CI/CT - The measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. Also, CI/CT, by any means, where a significant target or tool of the adversarial activity is a computer, computer network, embedded processor or controller, or the information thereon.

Cyber CI/CT Investigation - An investigation into threats targeting NASA or U.S. Government information systems by an insider or by an external entity. These investigations may involve unauthorized access/intrusions, exceeding authorized network privileges, denial of service attacks, or the introduction of malicious code.

CI/CT Case Categories.

- a. Request For Assistance - a request normally from the FBI or another USIC entity for NASA administrative information or records for official CI and/or CT national security investigative purposes.
- b. Threat Assessment - A limited review and analysis of an allegation, event, situational issue, or incident of potential CI/CT concern to determine if a basis exists for opening a NASA Preliminary Inquiry/Investigation.
- c. Preliminary Inquiry/Investigation - A limited gathering and examination of information or allegation indicating a NASA employee, information, or resources may be or have been involved with, or targeted by, agents of a foreign power, FIE, or a terrorist group/organization. A CI/CT inquiry is designed to gather information, identify and/or verify the credibility of potential sources and subjects(s) of CI/CT interest and to recommend appropriate action if the inquiry does not resolve the matter. The goal is to establish or refute a reasonable belief that a particular person is acting for, or on behalf of, or an event is related to, a foreign power engaged in spying, or committing espionage, sabotage, or other national security crimes or international terrorist activities. Establishment of reasonable belief provides the basis for opening a CI/CT investigation. Once a reasonable belief is established the matter shall be referred to the FBI [see Section 811 referral]. Refer to the definition of reasonable belief.
- d. Full Investigation - A CI/CT national security investigation conducted jointly with or in support of an FBI full investigation.

CI Special Agent - A Federal civil servant assigned to the NASA CI/CT Program. CISAs operate under the supervision of the DCI and carry a NASA CI badge and credential. CISAs are authorized to conduct CI/CT services, inquiries, and support national security investigations in accordance with U.S.C. Title 51, National Commercial Space Programs and to assist and request assistance from Federal and civilian authorities.

Counterterrorism - NASA CISAs conduct defensive CT activities in support of NASA's National Terrorism Advisory System Program. While the physical security aspects of NASA's CT functions are performed by the Agency's security elements, the CI/CT Division leverages liaison relationships at the Federal, state, and local levels to provide actionable terrorism-related intelligence (i.e., receipt, analysis, and dissemination of CT threat and targeting information) to OPS and the Agency's security elements. This intelligence enables Center Directors and CCPS/CCS to assess potential vulnerabilities and implement appropriate security countermeasures.

Classified National Security Information (CNSI) - Information that shall be protected against unauthorized disclosure in accordance with Executive Order No. 13526, "Classified National Security Information," as amended and is marked to indicate its classified status when in documentary form.

Controlled Unclassified Information - Unclassified information that does not meet the standard for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interest of the United States or originated by entities outside the U.S. Federal Government and under law or policy requires protection from disclosure, special handling safeguards, and prescribed limits on exchange or dissemination.

Damage Assessment - A systematic and documented analysis that determines the damage to national security or other impact on compromised NASA SBU/CUI, CNSI, or NCI.

Designated Countries - A compilation of countries with which the U.S. has no diplomatic relations, countries determined by Department of State to support terrorism, countries under sanction or embargo by the U.S., and countries of missile technology concern.

EAR or Export Administration Regulations - 15 CFR §§ 730-774 is the set of regulations that control the export of commercial and dual-use items that are designed for commercial use, but may have military use as well. The Bureau of Industry & Security within the Department of Commerce has the responsibility for the EAR under the Export Administration Act of 1979, as amended (50 U.S.C. app. §§ 2401, et seq.).

Escort - a NASA civil service employee or contractor responsible for 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 includes the purpose of the visit, where the individual may access the Center, where the individual may go, with whom the individual is to meet, and authorized topics of discussion.

Espionage - (1) intelligence activity directed toward the acquisition of information through clandestine means proscribed by the laws of the country against which it is committed; or (2) overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to injure the United States or provide advantage to a foreign nation. (For espionage crimes, generally, see 18 U.S.C. Sections 792 - 799).

Foreign Travel Briefings and Debriefings - Defensive CI/CT briefings provided to NASA Government and contractor personnel prior to travel outside the U.S. to a specific place or activity. Travel briefings are mandatory for traveling to designated countries, Russia, and/or high-threat locations on official business or assignment. The briefings are also offered for non-official travel upon request. Briefings inform personnel about current CI/CT threats and advisories, alerting travelers of the potential for harassment, exploitation, provocation, violent crime, or entrapment while traveling. These briefings, based on actual experiences of other NASA travelers when available, include information on defensive safeguards to avoid becoming targets of espionage, terrorism, or violent crime. Once travel is completed, personnel are debriefed.

Foreign National Visit Briefings and Debriefings - Defensive CI/CT briefings provided to NASA Government and contractor personnel prior to their hosting or escorting foreign visitors at NASA facilities from designated countries, Russia, and other high-threat locations, as defined in the NIPF or SETL. The briefings inform hosts and escorts of potential CI/CT risks and behaviors associated with foreign visits. Once a visit is completed, personnel are debriefed.

Foreign Intelligence Entity - Any known or suspected foreign organization, person, or group (public, private, or governmental) which conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorist groups/organizations.

Foreign National - Any person who is not a U.S. citizen and who is not a lawful permanent resident as defined by 8 U.S.C. 1101(a) (20) or any person who is not a protected individual as defined by 8 U.S.C. 1324b(a) (3). This also means any foreign corporation, business association, partnership, trust, society or any other entity or group that is not incorporated or organized to do business in the U.S., as well as any international organizations, any foreign government, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

Foreign Visit - Refers to a visit by a foreign national or foreign entity representative to any NASA facility, including NASA Headquarters, NASA Centers, JPL, or other Component Facilities.

Insider - Any person with authorized access to any United States Government resource, to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat - The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

International Traffic in Arms Regulations (ITAR) - The set of regulations that control the export and temporary import of defense articles and services. The ITAR (22 CFR §§ 120-130) is promulgated under the authority of the Arms Export Control Act (22 USC §§ 2778, et seq.). The authority for these controls has been delegated to the Secretary of State by Executive Order 11958, as amended (42 Fed. Reg. 4311).

Lawful Permanent Resident (LPR) - Replaces the term "Permanent Resident Alien" - A non-U.S. citizen, legally permitted to reside and work within the U.S. and issued the Resident Alien Identification (Green Card). Afforded all the rights and privileges of a U.S. citizen with the exception of voting, holding public office, employment in the federal sector (except for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4), and access to classified national security information (CSNI). (NOTE: LPR's are not prohibited from accessing export controlled commodities, but will still have a work-related "need-to-know" and are still considered foreign nationals under immigration laws.

Lead CISA - The senior CISA assigned at a CI/CT office. Lead CISAs represent the DCI with Center officials and the USIC. In addition to being a working agent, Lead CISAs manage the day-to-day CI/CT office activities and CI/CT services, inquiries, and support to national security investigations occurring at their Center.

NASA Critical Information - NCI is information that NASA is responsible for that is related to research, technologies, projects, programs, or systems that, if released outside established protocols, would significantly impact NASA resources, require additional research, development, tests, or evaluation to overcome the adverse effects of unauthorized release; significantly reduce the performance or effectiveness of NASA research, projects, technologies, programs, or systems; or negatively alter the direction of NASA research, projects, technologies, programs, or systems; thus reducing NASA's and the Nation's advantage in space technologies.

NASA Personnel - NASA civil service and contractor employees. For the purpose of this NPR, contractor is any non-NASA entity or individual working on a NASA installation or accessing NASA IT; an expert or consultant to any 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 any agency (but not a Federal employee). In order to perform the work specified under the contract, these persons require access to space, information, IT systems, staff, or assets of NASA.

National CI Executive - Directs national CI for the U.S. Government and is responsible to the Director of National Intelligence.

National Intelligence Priorities Framework - a classified national intelligence document used by the top planners of the USIC, such as the President of the United States and the Director of National Intelligence, that summarizes the U.S.'s intelligence gathering priorities, to include activities that are of greatest concern to the U.S. national security (such as terrorism). The NIPF is updated semi-annually and is available on the classified network. NASA personnel should contact their servicing CI/CT office to obtain the most current NIPF priorities.

Reasonable Belief - A reasonable belief arises when the fact and circumstances are such that a reasonable person would hold the belief. Reasonable belief shall rest on the facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on

experience, training, and knowledge in foreign intelligence or CI/CT work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or CI/CT work might not.

Regional Program Manager - A senior CI/CT professional who acts on behalf of the DCI and provides centralized management and oversight of CI/CT office activities. Regional Program Managers coordinate, de-conflict, and monitor CI/CT services, inquiries, and support to national security investigations conducted jointly with the FBI and USIC. Regional Program Managers also have supervisory responsibilities over the CISAs assigned to their regions.

Section 811 Referral - Section 811 of the Intelligence Authorization Act of 1995 (50 U.S.C. 402a) is the statutory authority that governs the coordination of counterespionage investigations between Executive Branch departments or agencies and the FBI. Section 811 referrals are the reports made by Executive Branch agencies or departments to the FBI under Section 811 (c) (1) (a) that advise the FBI of any information, regardless of its origin, which may indicate that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

Security Environment Threat List - A list of countries with U.S. Diplomatic Missions compiled by the Department of State and updated semi-annually. The listed countries are evaluated based on transnational terrorism; political violence; human intelligence; technical threats; and criminal threats. The SETL is available on the classified network via links on the State Department's Web site. Due to the frequency in changes to overseas threat environments, the assigning of SETL threat ratings (critical or high) occur frequently. As such, NASA personnel should contact their servicing CI/CT office to obtain the most current SETL listing.

Sensitive Information - Information for which the loss, misuse, unauthorized access, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Sensitive But Unclassified - Unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulation, and Government-wide policy, excluding information that is classified under EO 13526, dated December 29, 2009, or the Atomic Energy Act, as amended.

Sensitive Compartmented Information - 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.

Unauthorized Disclosure or Compromise - A communication or physical transfer of classified information to an unauthorized recipient. An unauthorized recipient is someone without a security clearance, or a person that holds a security clearance but has no need to know the information, or any other person or organization that is not routinely authorized access to U.S. classified information and that does not require that information to accomplish a mission in support of U.S. national security.

U.S. Intelligence Community - A coalition of 17 agencies and organizations, including the ODNI, within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities.

AA	Assistant Administrator
APT	Advanced Persistent Threat
CI	Counterintelligence
CCPS	Center Chiefs of Protective Services
CCS	Center Chiefs of Security
CIO	Chief Information Officer
CISA	NASA CI Special Agent
CISO	Center Information Security Officer
CNSI	Classified National Security Information
COMSEC	Communications Security
CT	Counterterrorism
CUI	Controlled Unclassified Information
DCI	Director of Counterintelligence/Counterterrorism
DOS	Department of State
EAR	Export Administrative Regulations
EO	Executive Order
FBI	Federal Bureau of Investigation
FIE	Foreign Intelligence Entity
ITAR	International Traffic in Arms Regulations
ITS	IT Security
JPL	Jet Propulsion Laboratory
LPR	Lawful Permanent Residents
MOU	Memorandum of Understanding
NCI	NASA Critical Information
NID	NASA Interim Directive
NIPF	National Intelligence Priorities Framework
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NSS	NASA Secure Systems
OCIO	Office of Chief Information Officer
OI	Operating Instructions
OIG	Office of the Inspector General
OPS	Office of Protective Services
PDD	Presidential Decision Directive
RFA	Request for Assistance
SBU	Sensitive But Unclassified
SETL	Security Environment Threat List

SCI	Sensitive Compartmented Information
SOC	Security Operations Center
UCI	Unclassified Controlled Information
U.S.C.	United States Code
USIC	United States Intelligence Community

Appendix C. References

5 U.S.C. Section 552, The Privacy Act of 1974 (Public Law 93-579), as amended.

5 U.S.C. 552(b) (1)-(9), Exemptions, Freedom of Information Act (FOIA), as amended.

5 U.S.C. 7312, Employment and Clearance, Individuals Removed for National Security Reasons.

12 U.S.C. 3401 - 3422, The Right to Financial Privacy Act of 1978 (Title XI of Public Law 95-630, November 10, 1978), as amended.

18 U.S.C. 798, Disclosure of Classified Information.

18 U.S.C. 799, Violation of Regulations of National Aeronautics and Space Administration.

18 U.S.C. 951, Agents of Foreign Governments.

18 U.S.C. Sections 1831-1839, Title I of the Economic Espionage Act of 1996 (Public Law 104-294), as amended (as related to CI/CT).

50 U.S.C. 401a, Section 3 of the National Security Act of 1947, as amended.

50 U.S.C. 1801 et seq., Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511, October 25, 1978), as amended.

EO 10450, Security Requirements for Government Employees, April 27, 1953, reprinted as amended (3 CFR 1949 - 1953 Compilation).

EO 12958, Classified National Security Information, April 17, 1995, reprinted as amended (3 CFR 1995 Compilation).

EO 12968, Access to Classified Information, August 2, 1995, reprinted as amended (3 CFR 1995 Compilation).

EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2012.

PDD 39, CT Policy, June 21, 1995, as amended.

PDD 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, May 22, 1998, as amended.

PDD 63, Critical Infrastructure Protection, May 22, 1998, as amended.

National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/ HSPD-23) (classified), January 2008.

Presidential Memorandum, November 21, 2012, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Program.

NPR 1600.3, Personnel Security.

NPR 1620.2, Facility Security Assessments.

NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

NPR 2190.1, NASA Export Control Program.

Comprehensive National Cyber Security Initiative (CNCSI), January 2008.
National CI Strategy of the United States of America.