NASA Policy Directive

NPD 1600.9
Effective Date: October 21, 2014
Expiration Date: October 21, 2019

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Insider Threat Program

Responsible Office: Office of Protective Services

1. POLICY

This NASA Policy Directive (NPD) establishes the NASA Insider Threat Program. It is NASA's policy to deter, detect, and mitigate the trusted insider who may represent a threat to national security. A comprehensive insider threat program is essential to the safety and security of our NASA employees, contractors, property, infrastructure and information. NASA's program will strengthen the protection of personnel, information, and resources by:

(1) Enhancing the safety and security of NASA's classified computer networks by establishing an integrated capability to monitor and audit user activity across all classified domains to detect and mitigate activity indicative of insider threat behavior;

(2) Facilitating the sharing of counterintelligence (CI), security, information assurance (IA), law enforcement (LE), human resources (HR), and other related information to recognize and counter the presence of an insider threat;

(3) Evaluating personnel security information for possible insider threat behaviors;

(4) Providing the NASA workforce with training on the insider threat, CI awareness and their reporting responsibilities;

(5) Gathering information to establish a centralized, analysis, reporting and response capability;

(6) Utilizing risk management principles and definitions accepted across the federal government and private industry, tailored to meet the distinct needs of NASA missions and programs; and

(7) Including appropriate protections for privacy.

2. APPLICABILITY

a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This directive applies to the Jet Propulsion Laboratory (a Federally Funded Research and Development Center), and other contractors only to the extent specified or referenced in the appropriate contracts.

b. Nothing in this directive limits the authorities of the Office of the Inspector General under the Inspector General Act of 1978, as amended.

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, and "will" denotes expected outcome, and "are/is" denotes descriptive material.

3. AUTHORITY

a. National and Commercial Space Programs, 51 U.S.C. § 20132, § 20133 and § 20134, Pub. L. No.111—314, 124

Stat. 3328 (December 18, 2010).

b. Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Executive Order 13587, 76 Fed. Reg. 198 (Oct. 13, 2011).

4. APPLICABLE DOCUMENTS

a. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

b. NPD 1600.1, NASA Counterintelligence (CI) Policy.

c. NPD 1440.6, NASA Records Management.

5. RESPONSIBILITY

a. The NASA Administrator has designated the Assistant Administrator for Protective Services (AA, OPS) as the agency's Insider Threat Senior Official, responsible for the NASA Insider Threat Program. The AA, OPS shall principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to OPS, Office of the Chief Information Officer (OCIO), Office of the Inspector General (IG), Office of the General Counsel (OGC), Office of Human Capital Management (OHCM), LE and any other relevant information indicative of a potential insider threat.

b. The AA, OPS, as the NASA Insider Threat Senior Official, shall comply with Executive Order (EO) 13587 and the Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, and the responsibilities listed below.

c. The AA, OPS shall appoint an Insider Threat Program Manager to provide oversight and management of the NASA Insider Threat Program.

d. In addition, as the Insider Threat Senior Official, he/she shall ensure the NASA Insider Threat Program includes:

(1) Procedures for the monitoring of user activity on all classified networks in order to detect activity indicative of insider threat behavior.

(2) Agreements signed, either physically or electronically, by all cleared employees acknowledging that their activity on any agency classified or unclassified network, to include portable electronic devices, is subject to monitoring and may be used against them in a criminal, civil, or administrative proceeding.

(3) Using standardized classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government authorized purposes and that unlawful or improper use of the computer can result in criminal or administrative actions against them.

(4) Developing and implementing, in consultation with the Office of General Counsel and privacy officials, procedures that ensure all insider threat program activities are conducted in accordance with applicable laws, whistleblower protections, and privacy policies.

(5) Developing and implementing reporting guidelines for OPS entities, OCIO, OIG, OGC, OHCM and other relevant organizational components to refer relevant insider threat information directly to the NASA Insider Threat Program Manager or designee.

(6) Procedures providing timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to foreign intelligence adversarial threats.>/p>

e. The NASA Insider Threat Program Manager shall:

(1) Develop an Agency implementation plan for the conduct and execution of a sustainable NASA Insider Threat Program.

(2) Ensure that the NASA Insider Threat Program:

(a) Provides insider threat awareness training, either in person or computer-based (SATERN), to all cleared employees within 30-days of initial employment, entrance on duty (EOD), or following the granting of access to classified information. This training will include basic counterintelligence awareness information as well.

(b) Provides insider threat awareness training annually and verifies that all cleared employees, including senior managers and supervisors, have completed the required annual training.

(c) Provides insider threat awareness training that addresses current, relevant, and potential threats in the NASA work and personal environment and includes, as a minimum, the following topics:

(i) The importance of detecting insider threats by cleared employees;

(ii) The importance of reporting suspicious activity to appropriate authorities;

(iii) Methodologies of adversaries, including foreign intelligence entities (FIE), to recruit trusted insiders and collect classified information;

(iv) Security and CI reporting requirements.

(d) Establishes and promotes an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the insider threat program.

(e) Establishes oversight mechanisms or procedures to ensure proper handling and use of records and data.

(f) Ensures access to such records and data is restricted to personnel who require the information to perform their authorized functions.

(g) Ensures the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by EO 13587 and NPD 1440.6H, NASA Records Management.

(h) Includes a centralized analysis, reporting, and response capability.

(3) Ensure that all personnel assigned to the NASA Insider Threat Program are fully cognizant of:

(a) Security and counterintelligence fundamentals;

(b) Procedures for conducting insider threat response actions;

(c) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information;

(d) Applicable privacy laws, regulations and policies;

(e) If there is any indication that classified information has been, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power the Federal Bureau of Investigation (FBI) will immediately notified in accordance with the procedures contained in NPD 1660.1, NASA Counterintelligence (CI) Policy.

(4) Be responsible for day-to-day operations of the NASA Insider Threat Program, ensuring that the Program:

(a) Build and maintain an insider threat analytic and response capability that manually and/or electronically gathers, integrates, reviews, assesses, and responds to information derived from OPS, OCIO, OIG, OGC, OHCM, and LE, the monitoring of user activity and other sources and methods as necessary and appropriate.

(b) Establish procedures for centrally managing Agency insider threat inquiries, to clarify or resolve insider threat matters.

(c) Develop procedures for documenting each insider threat matter reported and response action(s) taken, and ensure the timely resolution of each matter.

(d) Establish tactics, techniques and procedures for the monitoring of classified IT systems for signs of anomalous activity/espionage.

(e) Coordinate the submission of the quarterly Key Information Sharing and Safeguarding Indicators (KISSI) report to the Senior Information Sharing and Safeguard Sharing Committee.

(f) Serve as Agency liaison to the National Insider Threat Task Force (NITTF) and other federal insider threat organizations.

(g) Work closely with the OPS staff for budget formulation and budget submission for the Insider Threat Program.

e. Center Directors shall be responsible for Center support in compliance with the provisions set forth in this policy directive.

f. Center, Chiefs of Protective Services shall:

(1) Serve as the Center Insider Threat functional lead to assist in the coordination of insider threat activities in coordination with the AA, OPS and/or the NASA Insider Threat Program Manager.

(2) Ensure Center security specialists conduct the additional administrative requirements as required by the NASA Insider Threat Program as directed by the National Insider Threat Policy.

(3) Immediately report any Center insider threat activity to the NASA Insider Threat Program Manager.

g. Supervisors, leads, or any other employees, detailees, and contractors assigned or detailed to NASA shall not obstruct or impede any employee, detailee, or contractor from reporting a contact, activity, indicator or behavior.

h. All employees, detailees, and contractors assigned or detailed to NASA will comply with the requirements of all current and applicable federal laws, rules, regulations and NASA policies concerning the responsible sharing and safeguarding of classified national security information (CNSI).

i. All employees, detailees, and contractors assigned or detailed to NASA will report to the appropriate NASA Insider Threat Program personnel all contacts, activities, indicators or behaviors that they observe or gain knowledge of which could adversely affect the responsible sharing and safeguarding of CNSI.

j. Any NASA employees, detailees, or contractor who intentionally reports a false or fabricated contact, activity, indicator or behavior, which could adversely affect the responsible sharing and safeguarding of CNSI may be subject to disciplinary or administrative action.

6. DELEGATION OF AUTHORITY

None.

7. MEASUREMENT/VERIFICATION

a. Verification of compliance and effectiveness of this NPD will be based on the consistent metrics designed by and submitted to the Senior Information Sharing and Safeguarding Steering Committee, co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff, and the NITTF to determine NASA's compliance with national insider threat policies and procedures. b. The NASA Senior Agency Official for Insider Threat is also required to conduct annual self-assessments of the insider threat program using standards developed by the NITTF. c. In addition, the NITTF conducts periodic external assessments of the NASA insider threat program to assess compliance with national policies.

8. CANCELLATION

None.

/s/ Charles F. Bolden, Jr.
Administrator

APPENDIX A: Definitions

Counterintelligence (CI): Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or their agents, or international terrorist organizations or activities.

CI Awareness: An individual's level of comprehension as to the foreign intelligence entity (FIE) threat, methods, indicators, and reporting requirements.

CI Insider Threat: A person who uses their authorized access to facilities, systems, equipment, information or infrastructure to damage , disrupt operations, compromise information or commit espionage on behalf of an FIE.

Classified National Security Information (CNSI): Information that has been determined pursuant to EO 13526 or any successor order, EO 12951 or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form.

Cleared Employee: A person who has been granted access to classified information, other than the President and Vice President, employed by, detailed, or assigned to a department or agency, including members of the armed forces; an expert or consultant for a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the

appropriate department or agency head.

Foreign Intelligence Entity (FIE): Any known or suspected foreign organization, person, or group (public, private, or governmental) that 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 organizations.

Information Assurance (IA): All relevant unclassified and classified network information generated by IA elements to include, but not limited to, personnel usernames and aliases, levels of network access, audit data, unauthorized removable of media, print logs, and other data needed for clarification or resolution of an insider threat concern.
Insider: Any person with authorized access to any United States Government (USG) 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.

Insider Threat Response Action(s): Activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. The inquiry or investigation can be conducted under the auspices of counterintelligence, security, law enforcement, or the Office of the Inspector General, depending on statutory authority and internal policies governing the conduct of such activity in each agency. The NASA Inquiries Hub coordinates this.

National Insider Threat Task Force (NITTF): A Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. The NITTF develops policies, objectives, and priorities for establishing and integrating security, counter-intelligence, user audits and monitoring. The Attorney General and the Director of National Intelligence co-chair the NITTF.

Safeguarding: Measures and controls that are prescribed to protect CNSI, SBU from unauthorized access and to manage the risks associated with processing, storage, handling, transmission, and destruction of CNSI or SBU.

Sensitive but Unclassified Information (SBU): 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 29 December 2009, or the Atomic Energy Act, as amended.

Unauthorized Disclosure: A communication, confirmation, acknowledgement, or physical transfer of CNSI and SBU including the facilitation of, or actual giving, passing, selling, publishing, or in any way making such information available to an unauthorized recipient.

APPENDIX B: Acronyms

AA Assistant Administrator

CI Counterintelligence

CNSI Classified National Security Information

EO Executive Order

EOD Entrance on Duty

FBI Federal Bureau of Investigation

FIE Foreign Intelligence Entity

HQ Headquarters

HR Human Resources

IA Information Assurance

IG Inspector General

KISSI Key Information Sharing and Safeguarding Indicators

LE Law Enforcement

NITTF National Insider Threat Task Force

NPD NASA Procedural Directive

OCIO Office of the Chief Information Officer

OGC Office of General Counsel

OHCM Office of Human Capital Management

OIG Office of the Inspector General

OPS Office of Protective Services

SBU Sensitive but Unclassified

(URL for Graphic)

DISTRIBUTION:
NODIS