NATIONAL INSIDER THREAT POLICY

The National Insider Threat Policy aims to strengthen the protection and safeguarding of classified information by: establishing common expectations; institutionalizing executive branch best practices; and enabling flexible implementation across the executive branch.

A. Policy

Executive Order 13587 directs United States Government executive branch departments and agencies (departments and agencies) to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information (as defined in Executive Order 13526; hereinafter classified information), and requires the development of an executive branch program for the deterrence, detection, and mitigation of insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure. Executive Order 12968 promulgates classified information access eligibility policy and establishes a uniform Federal personnel security program for employees considered for initial or continued access to classified information. Consistent with Executive Orders 13587 and 12968, this policy is applicable to all executive branch departments and agencies with access to classified information, or that operate or access classified computer networks; all employees with access to classified information, including classified computer networks (and including contractors and others who access classified information, or operate or access classified computer networks controlled by the federal government); and all classified information on those networks.

This policy leverages existing federal laws, statutes, authorities, policies, programs, systems, architectures and resources in order to counter the threat of those insiders who may use their authorized access to compromise classified information. Insider threat programs shall employ risk management principles, tailored to meet the distinct needs, mission, and systems of individual agencies, and shall include appropriate protections for privacy, civil rights, and civil liberties.

B. General Responsibilities of Departments and Agencies

1) Within 180 days of the effective date of this policy, establish a program for deterring, detecting, and mitigating insider threat; leveraging counterintelligence (CI), security, information assurance, and other relevant functions and resources to identify and counter the insider threat.
2) Establish an integrated capability to monitor and audit information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) gathering information for a centralized analysis, reporting, and response capability.
3) Develop and implement sharing policies and procedures whereby the organization's insider threat program accesses, shares, and integrates information and data derived from

offices across the organization, including CI, security, information assurance, and human resources offices.

4) Designate a senior official(s) with authority to provide management, accountability, and oversight of the organization's insider threat program and make resource recommendations to the appropriate agency official.
5) Consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, civil liberties issues (including use of personally identifiable information) are appropriately addressed.
6) Promulgate additional department and agency guidance, if needed, to reflect unique mission requirements, but not inhibit meeting the minimum standards issued by the Insider Threat Task Force (ITTF) pursuant to this policy.
7) Perform self-assessments of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee (hereinafter Steering Committee).
8) Enable independent assessments, in accordance with Section 2.1(d) of Executive Order 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the ITTF.

C. Insider Threat Task Force roles and responsibilities

The ITTF, established under Executive Order 13587, is the principal interagency task force responsible for developing an executive branch insider threat detection and prevention program to be implemented by all departments and agencies covered by this policy. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within departments and agencies.

The ITTF shall:

1) In coordination with appropriate agencies, develop and issue minimum standards and guidance for implementing insider threat program capabilities throughout the executive branch. These standards shall include, but are not limited to, the following:
   - Monitoring of user activity on United States Government networks. This refers to audit data collection strategies for insider threat detection, leveraging hardware and/or software with triggers deployed on classified networks to detect, monitor, and analyze anomalous user behavior for indicators of misuse.
   - Continued evaluation of personnel security information whereby information is gathered from, including but not limited to, an individual's security background investigation, clearance adjudication, foreign travel reporting, foreign contact reporting, financial disclosure, polygraph examination results (where applicable) or other personnel actions, and made available to authorized insider threat program personnel to assess, in conjunction with anomalous user behavior data, and/or any other insider threat concern or allegation.
   - Employee awareness training of the insider threat, the inherent risk posed to classified information by malicious insiders and, specifically, recognition of insider threat behaviors; developing a reporting structure to ensure all employees and contractors

report suspected insider threat activity consistently and securely; informing employees, subject to monitoring, of the policies and processes in place to protect their privacy, civil rights, and civil liberties rights against unnecessary monitoring (to include retaliation against whistleblowers); and, ensuring employee awareness of their responsibility to report, as well as how and to whom to report, suspected insider threat activity.

- Analysis, Reporting and Response: gathering and integrating available information to conduct a preliminary review of any potential insider threat issues; and, where it appears a potential threat may exist, taking action by referring the matter as appropriate to CI, security, information assurance, the Office of Inspector General, or to the proper law enforcement authority.

2) Review and update ITTF standards and guidance, as appropriate.
3) Provide continual assistance to departments and agencies to establish and/or improve insider threat detection and prevention programs. The nature of assistance will involve a collaborative process wherein subject matter expert(s) provide expertise, guidance, and advice through various forums including on site visits.
4) Conduct independent assessments at individual organizations, as directed by the Steering Committee and in coordination with Executive Agent for Safeguarding (EA/S) and the Classified Information Sharing and Safeguarding Office (CISSO) established by Executive Order 13587, to determine the level of organizational compliance with this policy and minimum insider threat standards.
5) Use the results of relevant insider threat data sources to include, but not limited to, the agency's Key Information Sharing and Safeguarding Indicators self-assessments, applicable portions of the Office of the National Counterintelligence Executive Mission Reviews and Program Assessments, and the results of assistance visits and independent assessments to determine the adequacy of insider threat programs at individual agencies, and Government-wide.
6) Coordinate with the Information Security Oversight Office (ISOO), EA/S, and the CISSO to report results of independent assessments to the Steering Committee for use in the annual reports submitted to the President assessing the executive branch's effectiveness in implementing insider threat programs, and to inform related program and budget recommendations.
7) Refer to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards.
8) Provide strategic analysis of new and continuing insider threat challenges facing the United States Government.

D. Definitions

Classified information: Information that has been determined pursuant to Executive Order 13526, or any successor order, Executive Order 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 is marked to indicate its classified status when in documentary form.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations

conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended)

Departments and agencies: Any ''Executive agency,'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102; any "independent establishment," as defined in 5 U.S.C. 104(1).

Employee: For purposes of this policy, "employee" has the meaning provided in section 1.1(e) of Executive Order 12968; specifically: a person, 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 to 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.

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 her/his 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.

Key Information Sharing and Safeguarding Indicators: The Steering Committee developed these key performance indicators to serve as the basis for addressing reporting requirements directed by the President, and to assist in tracking progress and identifying areas for attention or additional funding to continue and strengthen the sharing and safeguarding of classified information on computer networks.

E. General Provisions

Nothing in this policy shall be construed to supersede or change the requirements of the National Security Act of 1947, as amended; the Atomic Energy Act of 1954, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order 12333, as amended (2008); Executive Order 13467, (2008); Executive Order 13526, (2009); Executive Order 12829, as amended, (1993); Executive Order 13549 (2010); and Executive Order 12968, (1995) and their successor orders or directives.

MINIMUM STANDARDS FOR EXECUTIVE BRANCH INSIDER THREAT PROGRAMS

A. AUTHORITY: Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; Executive Order 12968, Access to Classified Information; National Policy on Insider Threat.

B. PURPOSE

1. Executive Order 13587 establishes the Insider Threat Task Force, co-chaired by the Director of National Intelligence and the Attorney General, and requires, in coordination with appropriate agencies, the development of minimum standards and guidance for implementation of a government-wide insider threat policy. This policy provides those minimum requirements and guidance for executive branch insider threat detection and prevention programs.

2. Insider threat programs are intended to: deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative or other response actions as outlined in Section E.2.

3. The standards herein shall serve as minimum requirements for all applicable executive branch agencies. Nothing in this document shall be construed to supersede existing or future Intelligence Community or Department of Defense policy, which may impose more stringent requirements beyond these minimum standards for insider threat programs. Agencies may establish additional standards, provided that they are not inconsistent with the requirements contained herein.

4. Agency heads are ultimately responsible for the establishment and operations of their respective insider threat programs. Designated senior official(s), as described in Section D, shall be responsible for implementing the minimum standards contained herein.

C. APPLICABILITY: These standards shall apply to any "executive agency," as defined in 5 U.S.C. §105; any "military department" as defined in 5 U.S.C. §102; any "independent establishment" as defined in 5 U.S.C. §104(1); any intelligence community element as defined in Executive Order 12333.

D. DESIGNATION OF SENIOR OFFICIAL(S): Each agency head shall designate a senior official or officials, who shall be principally responsible for establishing a process to gather, integrate, and centrally analyze, and respond to Counterintelligence (CI), Security, Information Assurance (IA), Human Resources (HR), Law Enforcement (LE), and other relevant information indicative of a potential insider threat. Senior Official(s) shall:

1. Provide management and oversight of the insider threat program and provide resource recommendations to the agency head.

2. Develop and promulgate a comprehensive agency insider threat policy to be approved by the agency head within 180 days of the effective date of the National Insider Threat Policy. Agency policies shall include internal guidelines and procedures for the implementation of the standards contained herein.

3. Submit to the agency head an implementation plan for establishing an insider threat program and annually thereafter a report regarding progress and/or status within that agency. At a

minimum, the annual reports shall document annual accomplishments, resources allocated, insider threat risks to the agency, recommendations and goals for program improvement, and major impediments or challenges.

4. Ensure the agency's insider threat program is developed and implemented in consultation with that agency's Office of General Counsel and civil liberties and privacy officials so that all insider threat program activities to include training are conducted in accordance with applicable laws, whistleblower protections, and civil liberties and privacy policies.

5. Establish oversight mechanisms or procedures to ensure proper handling and use of records and data described below, and ensure that access to such records and data is restricted to insider threat personnel who require the information to perform their authorized functions.

6. Ensure the establishment of guidelines and procedures for the retention of records and documents necessary to complete assessments required by Executive Order 13587.

7. Facilitate oversight reviews by cleared officials designated by the agency head to ensure compliance with insider threat policy guidelines, as well as applicable legal, privacy and civil liberty protections.

E. INFORMATION INTEGRATION, ANALYSIS AND RESPONSE: Agency heads shall:

1. Build and maintain an insider threat analytic and response capability to manually and/or electronically gather, integrate, review, assess, and respond to information derived from CI, Security, IA, HR, LE, the monitoring of user activity, and other sources as necessary and appropriate.

2. Establish procedures for insider threat response action(s), such as inquiries, to clarify or resolve insider threat matters while ensuring that such response action(s) are centrally managed by the insider threat program within the agency or one of its subordinate entities.

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

F. INSIDER THREAT PROGRAM PERSONNEL: Agency heads shall ensure personnel assigned to the insider threat program are fully trained in:

1. Counterintelligence and security fundamentals to include applicable legal issues;

2. Agency procedures for conducting insider threat response action(s);

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

4. Applicable civil liberties and privacy laws, regulations, and policies; and

5. Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995, as well as other policy or statutory requirements that require referrals to an internal

entity, such as a security office or Office of Inspector General, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative services.

G. ACCESS TO INFORMATION: Agency heads shall:

1. Direct CI, Security, IA, HR, and other relevant organizational components to securely provide insider threat program personnel regular, timely, and, if possible, electronic access to the information necessary to identify, analyze, and resolve insider threat matters. Such access and information includes, but is not limited to, the following:

a. Counterintelligence and Security. All relevant databases and files to include, but not limited to, personnel security files, polygraph examination reports, facility access records, security violation files, travel records, foreign contact reports, and financial disclosure filings.

b. Information Assurance. 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 use of removable media, print logs, and other data needed for clarification or resolution of an insider threat concern.

c. Human Resources. All relevant HR databases and files to include, but not limited to, personnel files, payroll and voucher files, outside work and activities requests disciplinary files, and personal contact records, as may be necessary for resolving or clarifying insider threat matters.

2. Establish procedures for access requests by the insider threat program involving particularly sensitive or protected information, such as information held by special access, law enforcement, inspector general, or other investigative sources or programs, which may require that access be obtained upon request of the Senior Official(s).

3. Establish reporting guidelines for CI, Security, IA, HR, and other relevant organizational components to refer relevant insider threat information directly to the insider threat program.

4. Ensure insider threat programs have timely access, as otherwise permitted, to available United States Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

H. MONITORING USER ACTIVITY ON NETWORKS: Agency heads shall ensure insider threat programs include:

1. Either internally or via agreement with external agencies, the technical capability, subject to appropriate approvals, to monitor user activity on all classified networks in order to detect activity indicative of insider threat behavior. When necessary, Service Level Agreements (SLAs) shall be executed with all other agencies that operate or provide classified network connectivity or systems. SLAs shall outline the capabilities the provider will employ to identify suspicious user behavior and how that information shall be reported to the subscriber's insider threat personnel.

2. Policies and procedures for properly protecting, interpreting, storing, and limiting access to user activity monitoring methods and results to authorized personnel.

3. Agreements signed 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 could be used against them in a criminal, security, or administrative proceeding. Agreement language shall be approved by the Senior Official(s) in consultation with legal counsel.

4. Classified and unclassified network banners informing users that their activity on the network is being monitored for lawful United States Government-authorized purposes and can result in criminal or administrative actions against the user. Banner language shall be approved by the Senior Official(s) in consultation with legal counsel.

I. EMPLOYEE TRAINING AND AWARENESS: Agency heads shall ensure insider threat programs:

1. Provide insider threat awareness training, either in-person or computer-based, to all cleared employees within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information, and annually thereafter. Training shall address current and potential threats in the work and personal environment, and shall include, at a minimum, the following topics:

   a. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials;

   b. Methodologies of adversaries to recruit trusted insiders and collect classified information;

   c. Indicators of insider threat behavior and procedures to report such behavior; and

   d. Counterintelligence and security reporting requirements, as applicable.

2. Verify that all cleared employees have completed the required insider threat awareness training contained in these standards.

3. Establish and promote 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.

J. DEFINITIONS

"Agency Head" means the head of any: "executive agency," as defined in 5 U.S.C. §105; "military department" as defined in 5 U.S.C. §102; "independent establishment" as defined in 5 U.S.C. §104; intelligence community element as defined in Executive Order 12333; and any other entity within the executive branch that comes into the possession of classified information.

"Classified Information" means information that has been determined pursuant to Executive Order 13526, or the Atomic Energy Act of 1954 (42 U.S.C. §2162), to require

protection against unauthorized disclosure and that it is marked to indicate its classified status when in documentary form.

"Cleared Employee" means a person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to 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.

"Insider Threat" means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of 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)" means activities to ascertain whether certain matters or information indicates the presence of an insider threat, as well as activities to mitigate the threat. Such an inquiry or investigation can be conducted under the auspices of CI, Security, LE, or IG elements depending on statutory authority and internal policies governing the conduct of such in each agency.

"Subordinate Entity" means an office, command, or similar organization, subordinate to the agency, which manages its own insider threat program.