National Counterintelligence and Security Center

INSIDER THREAT PROGRAM

FOUNDATIONAL DOCUMENTS

NATIONAL INSIDER THREAT TASK FORCE

CONTENTS

Executive Order 13587

OF OCTOBER 7, 2011

Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Section 1. *Policy.*

Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. *General Responsibilities of Agencies.*

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. *Senior Information Sharing and Safeguarding Steering Committee.*

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government- wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD-1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. *Classified Information Sharing and Safeguarding Office.*

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM-ISE to provide expert, full-time, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. *Executive Agent for Safeguarding Classified Information on Computer Networks.*

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD-42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD-42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. *Insider Threat Task Force.*

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. 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 agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice,

Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government- wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. *General Provisions*.

(a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM-ISE under Executive

Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD-42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD-42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:
(1) the authority granted by law to an agency, or the head thereof; or
(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,

October 7, 2011

Presidential Memorandum

NATIONAL INSIDER THREAT POLICY AND MINIMUM STANDARDS FOR EXECUTIVE BRANCH INSIDER THREAT PROGRAMS

Memorandum For the Heads of Executive Departments and Agencies

SUBJECT: National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs

This Presidential Memorandum transmits the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Minimum Standards) to provide direction and guidance to promote the development of effective insider threat programs within departments and agencies to deter, detect, and mitigate actions by employees who may represent a threat to national security. These threats encompass potential espionage, violent acts against the Government or the Nation, and unauthorized disclosure of classified information, including the vast amounts of classified data available on interconnected United States Government computer networks and systems.

The Minimum Standards provide departments and agencies with the minimum elements necessary to establish effective insider threat programs. These elements include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

The resulting insider threat capabilities will strengthen the protection of classified information across the executive branch and reinforce our defenses against both adversaries and insiders who misuse their access and endanger our national security.

BARACK OBAMA

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 ITIF 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 (ENS) 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), ENS, 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 assassination

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 l. l(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 of2004; 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. § I 02; 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 (BOD), 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.

Maturity Framework Frequently Asked Questions

What is the Maturity Framework (Framework) designed to do?

Answer: The "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," (November 21, 2012) provides executive branch departments and agencies (D/As) with the minimum elements necessary to establish functional insider threat programs (InTPs); therefore, the Minimum Standards serve as milestones in the InTP maturity process. To help prevent the compromise of sensitive or classified information and to protect the resources and capabilities of the US Government (USG), InTPs must continue to enhance their policies, processes, methodologies, and capabilities. The Framework is designed to help programs evolve beyond the Minimum Standards to become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk.

How was the Maturity Framework developed?

Answer: As part of its assigned responsibilities under Executive Order (EO) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," (October 7, 2011) and the National Policy and Minimum Standards, the National Insider Threat Task Force (NITTF) is charged with reviewing, and, if appropriate, adding to or modifying the Minimum Standards and guidance, in coordination with executive branch D/As. Beginning in the Fall of 2017, NITTF held a series of working groups to solicit ideas from the USG Insider Threat Community. Based upon the feedback received in the working groups, NITTF then developed a draft framework, modeled on the capability maturity model (CMM) process improvement approach used in industry. The resulting framework was vetted through a series of NITTF-hosted focus groups held throughout the Spring of 2018 that included representatives from Intelligence Community, Department of Defense, and Federal Partner insider threat programs.

Why did NITTF decide to use a Framework format instead of Standards?

Answer: The Minimum Standards established a baseline of capabilities for all InTPs within the USG Insider Threat Community. Over time, armed with the body of knowledge gleaned through the independent assessment process, NITTF recognized that beyond this baseline, each D/A must be allowed to mature its capabilities to assess and mitigate the threats from within their unique environment. New standards applicable to all would take away flexibility and replace it with a one-size-fits-some solution. The Framework construct allows D/As to choose among the maturity elements for those that best fit with their workplace environment, technology infrastructure, and mission.

Why introduce the Framework now, when many D/As are still working to achieve Minimum Standards Full Operating Capability (FOC)?

Answer: Achieving FOC is not a prerequisite for employing elements of the Framework. Those programs that are close to FOC will benefit from the increased capabilities gained through implementation of Framework elements. For other programs, the challenges they face in achieving FOC will likely require additional effort and resources to overcome. The elements of the Framework will help sharpen their ability to identify and mitigate possible insider threat risk while they continue to address those challenges.

Does the Framework replace the Minimum Standards?

Answer: No. The Minimum Standards must still be met. Executive branch D/As subject to EO 13587 must still comply with the National Policy and Minimum Standards. The Framework provides guidance for maturing programs beyond the minimum requirements.

Is the Framework a new set of standards for InTPs?

Answer: No. The Framework identifies key elements within the existing Minimum Standards construct that when enhanced, enable D/As to increase the effectiveness of program functionality, garner greater benefit from InTP resources, procedures, and processes, and tightly integrate InTP goals and objectives with their D/A's missions and challenges. Each element within the Framework has been identified as a capability or attribute exhibited by an advanced insider threat program. However, each D/A should evaluate the applicability of Framework elements to their environment.

Are D/As required to implement the Framework elements?

Answer: No. The Framework is a general blueprint for D/As as they seek to advance their InTP's capabilities and evolve beyond the Minimum Standards. When using the Framework, D/As should employ risk management principles tailored to meet the needs of their workplace environment, technology infrastructure, and mission. InTPs must also ensure compliance with their D/A's policies, regulations, and all applicable legal, privacy and civil liberties, and whistleblower protections when evaluating and incorporating Framework elements.

Is there a timeframe or deadline for InTPs to implement Framework elements?

Answer: No. InTPs should review the Framework and assess which elements might be appropriately incorporated into their program in consultation with their D/A's Office of General Counsel (OGC), Office of Inspector General (OIG), and privacy and civil liberties officials. Once a determination has been made on the element(s) to be incorporated, InTPs may wish to develop a program of action and milestones to help facilitate implementation of the Framework element(s).

Will InTPs be assessed against the Framework elements?

Answer: Since the Framework is not a new set of standards, InTP implementation of maturity elements (MEs) will not be formally assessed. However, the NITTF will note during an independent assessment when an InTP has incorporated MEs into its program construct and documentation. NITTF is gathering best practices that can be used throughout the USG Insider Threat Community to help other programs mature and optimize their capabilities. As the National InTP matures its overall effectiveness through these best practices, many of which can be found in the Framework, the NITTF will evolve its assessment process to include measures of effectiveness.

How can an InTP use the Framework?

Answer: InTPs can use the Framework as a roadmap to develop strategic goals and objectives to evolve their capabilities, processes, procedures and resources to meet current and future challenges in countering the insider threat. InTPs should also incorporate considerations for their unique D/A mission, workforce environment, and technology infrastructure as they develop their course of action and implementation plans. Additionally, InTPs should engage their OGC, privacy and civil liberties officials, and OIG early on in their planning process to ensure what is developed complies with all applicable legal, privacy and civil liberties rights, and whistleblower protections.

What assistance is available to a D/A in implementing the Framework?

Answer: The NITTF is prepared to provide continued support, advice and assistance, not only as D/As continue to implement the Minimum Standards but also as their InTPs begin to employ the Framework. As with efforts to develop programs to date, the resources to implement the elements of the Framework will be the responsibility of the individual D/As. The NITTF stands ready to offer best practices as well as introductions to other D/A programs that may have the information programs need to move forward.

My D/A is small/has a small number of cleared employees/not much access to classified information. How does the Framework apply to my InTP?

Answer: Unlike the Minimum Standards, which require that all specified requirements be met, the Framework is specifically designed to give D/A's the flexibility to implement the MEs the D/A sees as beneficial to enhancing the capabilities of its InTP.


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA