

Insider Threat Policy

- 1. REASON FOR POLICY:** To establish the Department of Veterans Affairs (VA) policy for the Insider Threat Program (ITP).
- 2. SUMMARY OF CONTENT/MAJOR CHANGES:** Identifies applicable ITP requirements, department responsibilities, subject matter references, and applicable definitions.
- 3. RESPONSIBLE OFFICE:** The Office of Operations, Security, and Preparedness (007).
- 4. RELATED HANDBOOK:** None
- 5. RECESSION:** None

CERTIFIED BY:

**BY DIRECTION OF THE
SECRETARY OF VETERANS
AFFAIRS:**

/s/
Stephen Warren
Executive in Charge for the Office of
Information Technology

/s/
Kevin T. Hanretta
Assistant Secretary
Operations, Security, and Preparedness

INSIDER THREAT POLICY

1. PURPOSE.

The purpose of this directive is to establish Department-wide policy and assign responsibilities for the Department of Veterans Affairs' (VA) Insider Threat Program (ITP). These efforts will enable a secure operating environment for VA employees, systems, facilities, and Veterans from insider threats as defined by Executive Order (E.O.) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011). E.O. 13587 applies to all Federal agencies that access and/or maintains classified material and/or classified information systems and to all individuals assigned thereto with access to them. Authorities: Section 3381 of title 50 of the United States Code; Presidential Memorandum on National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012); E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011); E.O. 13526, Classified National Security Information (Dec. 29, 2009); E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008); E.O. 12968, Access to Classified Information (Aug. 4, 1995); E.O. 12333, United States Intelligence Activities (Dec. 4, 1981); and E.O. 10450, Security Requirements for Government Employment (Apr. 27, 1953).

2. POLICY.

a. The ITP is established as a VA-wide program for the protection of unauthorized disclosure of classified National Security Information (NSI) on Classified National Security Systems (CNSS), and classified Automated Information Systems (AIS). The program is designed to prevent espionage related activities from cleared employees who have been granted access to classified information, accounts with access to CNSS, and classified AIS.

b. The VA ITP will meet or exceed the minimum standards for such programs, as defined in E.O. 13587 and Presidential Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012).

c. All VA-cleared employees who have been granted national security classified accounts for access to CNSS and classified AIS are required to take insider threat awareness training, either in-person or computer-based, within 30 days of initial employment, entry-on-duty (EOD), or following the granting of access to classified information systems, and annually thereafter. Failure to comply with training requirements will result in the loss or suspension of access to VA CNSS or classified

VA DIRECTIVE 0327

AIS systems. VA's Office of Operations, Security, and Preparedness (OSP) will develop and prescribe policy, and manage the ITP in accordance with E.O. 13587, the Presidential Memorandum on National Insider Threat Policy and the Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), and relevant National Insider Threat Task Force (NITTF) guidance.

d. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information that has the potential to compromise or damage classified NSI and/or systems. Insider threat detection and prevention requires an integrated effort across the entire Department. The ITP will coordinate with VA's Office of Human Resources and Administration (OHRA) and VA's Office of the General Counsel (OGC) to ensure legal, privacy, civil rights, and civil liberties concerns (including, but not limited to, the use of Personally Identifiable Information (PII) or Protected Health Information (PHI)) are appropriately addressed. Specifically, the Senior Agency Official (SAO) will:

- (1) Establish and assign responsibilities for the ITP.
- (2) Establish guidelines specific to the implementation and oversight of the ITP.
- (3) Direct the integration of counterintelligence (CI), information assurance (IA), antiterrorism, security/law enforcement, and human resources (HR) information for the purpose of insider threat detection and prevention.
- (4) Coordinate material and technical support from OGC and OHRA.

e. While the principles and practices discussed herein are written to help VA execute E.O. 13587 they can also be applied to protect sensitive unclassified environments.

3. RESPONSIBILITIES.

a. The Secretary of Veterans Affairs delegates authority to ensure implementation of this Directive and all policies, roles and responsibilities herein to the Assistant Secretary for Operations, Security, and Preparedness who serves as VA's Senior Agency Official (SAO) for the ITP.

b. Assistant Secretary for Operations, Security, and Preparedness (OSP):

- (1) Serves as the SAO for the ITP and provides management and oversight of the ITP.
- (2) Develops and implements a comprehensive VA insider threat policy.
- (3) Ensures the ITP is executed in accordance with all applicable laws and policies.

(4) Establishes guidelines and procedures for the retention, sharing, and safeguarding of records and documents necessary to complete insider threat related inquiries and assessments.

(5) Establishes and leads an ITP Executive Steering Committee for consultation on all ITP-related issues, conducting program oversight and reviews, as well as identifying and making program resource recommendations.

(6) Establishes an ITP program management office with a centralized analysis and response capability to gather, integrate, review, assess, and respond to information derived from CI, IA, security/law enforcement, HR, and other information sources as deemed appropriate.

(7) Oversees the collection, analysis, and reporting of information across VA to support the identification and assessment of insider threats.

(8) Establishes and manages reporting requirements, to include self-assessments and independent assessments, and reports all findings to the National Senior Information Sharing and Safeguarding Steering Committee.

(9) Establishes and executes an Insider Threat Awareness Training Program.

(10) Details or assigns volunteer staff, as appropriate and necessary, to the Classified Information Sharing and Safeguarding Office (CISSO) and/or the Insider Threat Task Force (ITTP).

(11) Coordinates with OGC, OHRA, the Office of Information Technology (OIT), the Office of the Inspector General (OIG), and other Administrations and Staff Offices, as required.

(12) May designate all or some of the above responsibilities to the Deputy Assistant Secretary for Emergency Management and Resilience (OEM&R).

c. Deputy Assistant Secretary for OEM&R, as delegated by the Assistant Secretary for OSP, will oversee the management and implementation of all phases of VA's ITP.

d. Undersecretaries, Assistant Secretaries, and other Key Officials will:

(1) Support OSP in implementing VA's ITP.

(2) Ensure that all relevant VA employees are aware of and adhere to this policy.

e. ITP Executive Steering Committee will:

VA DIRECTIVE 0327

(1) Consist of representatives from all offices within VA that possesses information about the activities of agency employees pertaining to access of classified information and systems.

(2) Establish program objectives and metrics for the ITP that will drive program requirements and set strategic priorities of VA.

4. REFERENCES.

a. Laws:

- (1) Chapters 44 and 45 of title 50 of the United State Code
- (2) Parts 731 and 732 of title 5 of the Code of Federal Regulations
- (3) Parts 2001 and 2003 of title 32 of the Code of Federal Regulations

b. Executive Orders (E.O.):

- (1) E.O. 10450, Security Requirements for Government Employment (Apr. 27, 1953)
- (2) E.O. 12333, United States Intelligence Activities (Dec. 4, 1981)
- (3) E.O. 12829, National Industrial Security Program (Jan. 6, 1993)
- (4) E.O. 12968, Access to Classified Information (Aug. 4, 1995)
- (5) EO 13388, Further Strengthen the Sharing of Terrorism to Protect Americans (Oct. 25, 2005)
- (6) E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008)
- (7) E.O. 13526, Classified National Security Information (Dec. 29, 2009)
- (8) E.O. 13556, Controlled Unclassified Information (Nov. 4, 2010)
- (9) E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011)

c. Presidential Directives and Memoranda:

(1) Presidential Decision Directive (PDD/NSC-12) Security Awareness and Reporting of Foreign Contacts (Aug. 5, 1993)

(2) Presidential Memorandum, Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies (Aug. 23, 1996)

(3) Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012)

d. VA Policies & Procedures:

(1) VA Directive 0710, Personnel Suitability and Security Program (June 4, 2010)

(2) VA Directive 0730, Security and Law Enforcement (Dec. 12, 2012)

(3) VA Directive 6500, Managing Information Security Risk: VA Information Security Program (Sep. 20, 2013)

e. Intelligence Community Directives (ICD):

(1) ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information (Mar. 14, 2007)

(2) ICD 704, Personnel Security Standards and Procedures Governing Eligibility Access to Sensitive Compartmented Information, and other Control Access Program Information (Oct. 1, 2008)

(3) ICD 710, Classification and Control Markings System (Sep. 11, 2009)

(4) ICD 705, Sensitive Compartmented Information Facilities (May 26, 2010)

(5) ICD 700, Protection of National Intelligence (June 7, 2012)

f. Other Directives and Documents:

(1) Office of the Director of National Intelligence, The National Counterintelligence Strategy of the United States of America (Aug. 2009)

(2) Office of the Director of National Intelligence, The National Intelligence Strategy of the United States of America, (Aug. 2009)

(3) Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, Defensive Counterintelligence Program Blueprint (2010)

VA DIRECTIVE 0327

(4) Office of the Director of National Intelligence, Counterintelligence/Security Risk Assessment Framework for Federal Partners (Mar. 2012)

(5) Office of the Director of National Intelligence, Office of the National Counterintelligence Executive, Security Executive Agent Directive 1, Section 3 (Mar. 13, 2012)

5. DEFINITIONS.

a. Agency Head: 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 E.O. 12333; and any other entity within the Executive Branch that comes into the possession of classified information.

b. Classified information: Information that has been determined pursuant to E.O. 13526, or any successor order, or the Atomic Energy Act of 1954, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

c. Cleared Employee: a person who has been granted a security clearance that permits access to classified information, other than the President and Vice President, and who is: 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.

d. 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.

e. Employee: For purposes of this policy, "employee" has the meaning provided in section 1.1(e) of E.O. 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to VA; an expert or consultant to VA; an industrial or commercial contractor, licensee, certificate holder, or grantee of VA, including all subcontractors; a personal services contractor employee; or any other category of person who acts for or on behalf of VA as determined by the Secretary.

f. Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by, is produced by or for, or is under the control of the United States

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

h. 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 VA resources or capabilities.

i. Insider Threat Program: A coordinated collection of capabilities authorized by the Department or Agency that is organized to deter, detect and mitigate the unauthorized disclosure of sensitive information. At a minimum, for Departments and Agencies that handle classified information, an insider threat program shall consist of capabilities that provide access to information; centralized information integration, analysis, and response; employee insider threat awareness training; and the monitoring of user activity on government computers. For Departments and Agencies that do not handle classified information, these can be employed effectively for safeguarding information that is unclassified but sensitive.