Defense Security Service
REGULATION

NUMBER 05-06
January 30, 2014

ITIMP

SUBJECT: Defense Security Service Insider Threat Identification and Mitigation Program

References: See Enclosure 1.

1. PURPOSE. This Regulation establishes the Defense Security Service (DSS) Insider Threat Identification and Mitigation Program (ITIMP) and sets forth policy and procedures intended to deter all DSS personnel from becoming insider threats; detect insiders who pose a risk to DSS operations or classified information; and mitigate insider threat risks through appropriate and authorized measures.

2. APPLICABILITY. This Regulation applies to DSS employees, employees of other Federal agencies assigned or detailed to DSS, and to contractor personnel performing work at DSS facilities or who have access to DSS information systems, collectively referred to in this Regulation as "DSS personnel."

3. DEFINITIONS. See Enclosure 3.

4. POLICY. It is DSS policy that:

a. DSS will operate an effective and efficient ITIMP that complies with the requirements of the Presidential memorandum of November 21, 2012 (Reference (a)), Executive Order 13587 (Reference (b)), and any applicable current DoD or Federal guidance on insider threat.

b. The ITIMP will be carried out by subject matter experts from the following DSS offices and functional areas of responsibility: Security (including Anti-Terrorism/Force Protection), Information Assurance (IA), Office of the Chief Information Officer (OCIO), Counterintelligence (CI) Directorate, Human Capital Management Office (HCMO), Office of the Inspector General (OIG), and the Office of the General Counsel (OGC). The intent is for this collected group, together with ITIMP personnel, to form an integrated information sharing and analysis capability that can identify matters that raise insider threat concerns, develop sufficient

information from appropriate functional inquiries to resolve the concerns, or have the appropriate functional office make an appropriate referral for action.

c. The ITIMP will employ risk management principles, tailored to meet the distinct needs, mission, and systems of DSS, and will include appropriate protections for privacy, civil rights, and civil liberties.

d. This Regulation does not supersede or replace counterintelligence or security awareness and reporting requirements stated in laws or other Federal, Department of Defense or DSS regulations or other issuances.

e. All DSS personnel must comply with the requirements of all current and applicable federal laws, rules, regulations and policy concerning the responsible sharing and safeguarding of classified and controlled unclassified information (CUI).

f. Because of the functions assigned to DSS, all DSS personnel have a special and continuing security obligation to be aware of the risks associated with insider threats, foreign intelligence operations and/or possible terrorist activities directed against them in the United States and abroad.

(1) DSS personnel also have a responsibility to recognize and understand those behaviors and activities that may adversely impact their continued eligibility for access to classified information or eligibility to hold a sensitive position.

(2) ITIMP personnel must be provided with timely access to the information necessary to identify, report, and conclude that insider threat matters have been appropriately resolved.

g. ITIMP personnel must protect the information, documents, files and material they handle in connection with their ITIMP duties in accordance with the sensitivity or classification of the information, and in accordance with current and applicable Federal laws, rules, regulations, and policy.

h. The ITIMP will be developed and implemented so that all activities, to include training, are conducted in accordance with applicable laws, civil liberties, and privacy policies.

i. ITIMP personnel who require access to particularly sensitive or protected information or Special Access Programs (SAPs) must, before being given access to such information, have successfully completed all requirements for access to that sensitive or protected information or SAP (e.g., fully adjudicated current personnel security investigation and, when required by another agency for access to information controlled by that agency, a CI scope polygraph examination). Failure to meet the access requirements may be grounds for removal from an ITIMP position. Agency personnel participating in the ITIMP at any level will complete a non-disclosure agreement regarding their insider threat-related activities.

j. All DSS employees who visit high threat countries (as defined in the National Intelligence Priorities Framework) on official or unofficial travel must receive a defensive travel

briefing from the DSS Office of Security before departure and, when necessary, participate in a travel debrief upon return.

k. Failure to comply with the mandatory provisions of this Regulation could result in disciplinary, administrative or possible criminal actions.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Regulation is approved for public release. Copies may be obtained through the Internet from the DSS website.

8. EFFECTIVE DATE. This Regulation is effective immediately.

Stanley L. Sims
Director

Enclosures
1. References
2. Responsibilities
3. Definitions

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," November 21, 2012
(b) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
(c) Presidential Decision Directive/NSC-12 of August 5, 1993, "Security Awareness and Reporting of Foreign Contacts"
(d) White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996
(e) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953
(f) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(g) Executive Order 12968, "Access to Classified Information," August 2, 1995
(h) Executive Order 13526, "Classified National Security Information," December 29, 2009
(i) Committee on National Security Systems Directive No. 504, "Directive on Protecting National Security Systems from Insider Threat," January 2012
(j) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended
(k) DoD Instruction 5240.26, "Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat," May 4, 2012
(l) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007, as amended
(m) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(n) Section 811 of Public Law 103-359, "Intelligence Authorization Act for Fiscal Year 1995," October 14, 1994

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DSS. The DSS Director is responsible for the overall operation and functioning of the DSS ITIMP.

2. DEPUTY DIRECTOR, DSS. The DSS Deputy Director will:

a. Serve as the DSS senior official for insider threat and provide leadership, management, direction and oversight to the ITIMP.

b. Chair the Insider Threat Executive Advisory Group (ITEAG).

c. Schedule meetings of the ITEAG to provide necessary oversight to the ITIMP, as needed but not less than twice a year.

d. Ensure the ITIMP operates in accordance with approved internal guidelines and procedures for implementing the standards in Reference (a) and any published DoD standards.

e. Chair the Insider Threat Working Group (ITWG) when present for ITWG meetings.

f. Review, approve, and publish agency guidelines on referral of relevant insider threat information directly to the ITWG.

3. DIRECTOR, COUNTERINTELLIGENCE (CI). The CI Director is the ITIMP Executive Agent and will:

a. Assign a qualified individual to be the ITIMP manager.

b. Ensure the ITIMP has timely access, as otherwise permitted, to available U.S. Government intelligence and counterintelligence reporting information and analytic products pertaining to adversarial threats.

c. Establish a method to identify high threat countries that pose an intelligence threat to the agency. These high threat countries should be placed on an appropriately classified list that documents the intelligence threat and mitigating strategies. The list must be approved by the Deputy Director and updated as necessary, but at least once a year.

d. Use available classified and unclassified resources to help determine travel risk, which will be provided to the DSS Office of Security. Resources used to determine travel risk will include the following lists:

(1) Office of National Counterintelligence Executive National Threat Identification and Prioritization Assessment

(2) Department of State Security Environment Threat List

(3) Department of State Travel Warning List

(4) Defense Intelligence Agency Threat List

e. Establish procedures and actions to follow if a foreign visitor or assignee is determined by appropriate authority to have affiliations or relationships that could jeopardize the responsible sharing and safeguarding of classified and sensitive information.

f. Provide all necessary administrative support to the ITEAG.

4. INSIDER THREAT IDENTIFICATION AND MITIGATION PROGRAM MANAGER. The ITIMP manager will:

a. Develop, making maximum use of Center for Development of Security Excellence (CDSE) resources, insider threat awareness training required by Reference (a), combined with counterintelligence awareness and reporting (CIAR) training required by DoD Directive O-5240.02 (Reference (l)), either through instructor-led or eLearning courses.

b. Provide, or make available, combined insider threat awareness/CIAR training to all DSS personnel within 30 days of initial employment, entry on duty, or after access to classified information is granted.

c. Provide, annually, combined insider threat awareness/CIAR training that addresses current and potential threats in work and personal environments and includes, at a minimum, the following insider threat awareness topics in addition to the topics required by Reference (l):

(1) The importance of detecting insider threats by DSS personnel.

(2) The importance of reporting suspicious activity.

(3) Methodologies of adversaries to recruit trusted insiders and illegally collect classified information.

d. Track the progress of all agency personnel in completing any required insider threat awareness/CIAR training.

e. Establish and promote, in coordination with the ITWG, an internal network site accessible to all agency personnel to provide insider threat reference material, including indicators of insider threat behavior and applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the ITIMP.

f. Establish and follow, in accordance with applicable laws and regulations, oversight mechanisms and procedures for the proper handling, use, referral, reporting, storage and destruction of ITIMP records and data.

g. Establish and follow appropriate procedures to ensure that access to ITIMP records and data is restricted to personnel who require the information to perform their authorized functions.

h. Establish and follow appropriate guidelines and procedures for retaining records and documents necessary to complete assessments required by Reference (b) or other controlling issuances.

i. Ensure personnel assigned to the ITIMP are fully trained in:

(1) Counterintelligence and security fundamentals.

(2) Department or agency procedures for conducting insider threat response actions.

(3) Laws and regulations that apply to the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information, through coordination with OCIO, OIG and OGC.

(4) Applicable civil liberties and privacy laws, regulations, and policies through close coordination with OGC.

(5) Investigative referral requirements of Section 811 of the Intelligence Authorization Act for Fiscal Year 1995 (Reference (n)), as well as other policy or statutory requirements that require referrals to an internal entity.

(6) Performing self-assessments of compliance with insider threat policies and standards, the results of which will be reported to the Insider Threat Executive Advisory Group (ITEAG).

j. Ensure any Privacy Act System of Records Notices required pursuant to ITIMP activities are amended or filed as necessary.

k. Coordinate ITIMP policies and procedures with OGC and other appropriate DSS offices before adoption.

l. Establish a centralized auditing and activity monitoring capability for DSS unclassified and classified networks, to include analysis, reporting, and response mechanisms, and ensure that all triggers or thresholds that provide a basis for initiating or continuing an insider threat activity receive legal review.

m. Prepare, as required by directive or instruction, reports for the National Counterintelligence Executive and appropriate DoD offices.

n. Monitor changes in Executive, DoD or Intelligence Community insider threat requirements and recommend adjustments to DSS practices, processes and triggers as necessary.

o. Provide all necessary administrative support to the ITWG.

5. CHIEF, OFFICE OF SECURITY. The Chief, Office of Security will:

a. Maintain records based on the reporting of official foreign contacts by DSS employees and report these contacts to the ITWG to assess whether insider threat response action(s), such as an inquiry to clarify or resolve a potential insider threat, is warranted.

b. Provide initial and follow-up reports of significant unofficial foreign contact(s) by DSS employees to the ITWG to assess whether insider threat response action(s), such as an inquiry to clarify or resolve a potential insider threat, is warranted.

c. Notify the ITWG of any credible information raising insider threat concerns regarding foreign influence, habits or other behaviors of security significance (e.g., excessive debt, addictions, or anomalous behaviors) discovered during the performance of the office's assigned functions.

6. DSS CHIEF INFORMATION OFFICER. The Chief Information Officer will:

a. Establish, and ensure OCIO personnel follow, processes for notifying the ITWG of any significant events or incidents that raise insider threat concerns detected through its assigned computer network defense/information assurance operations. Reportable events may also be indicators of terrorism, espionage, workplace violence, or fraud.

b. Establish, and ensure OCIO personnel follow, processes for reporting to the ITWG any incidents or events that indicate insider action or inaction and degrade (or attempt to degrade) the integrity of the agency's classified and unclassified information systems, communications systems, and associated hardware/software; classified and unclassified data systems and associated hardware/software; the integrity and viability of function systems; the agency's reporting and data collation competencies, or its legacy and active data retrieval competencies.

c. Provide all necessary technical support to the ITIMP.

7. CHIEF, HUMAN CAPITAL MANAGEMENT OFFICE (HCMO). The Chief, HCMO, will:

a. Establish, and ensure HCMO personnel follow, processes for notifying the ITWG of any anomalous/aberrant misconduct, foreign influence, or significant behaviors (e.g. excessive debt, addictions, or other behaviors) discovered during the normal functions of HCMO's mission that raise insider threat concerns.

b. Report to the ITWG any unusual use/abuse of systems and personnel rosters that contain personally identifying information of DSS personnel, or of populations across the Department of Defense.

8. DSS INSPECTOR GENERAL. The Inspector General will perform program reviews, as directed by the DSS Director or Deputy Director, of the ITIMP to assess its compliance with applicable insider threat policy directives, instructions or other guidelines.

9. DSS GENERAL COUNSEL. The General Counsel will:

a. Establish processes for providing legal support and advice to the ITIMP.

b. Provide all legal reviews required by this Regulation.

10. INSIDER THREAT EXECUTIVE ADVISORY GROUP (ITEAG). The ITEAG is composed of the DSS Chief of Staff and senior officials from the CI Directorate, OCIO, HCMO, Office of Security, OIG, and OGC. The DSS Deputy Director will chair the ITEAG. The ITEAG will:

a. Provide management oversight and policy review of the performance and operation of the ITIMP.

b. Recommend for adoption, after review by OGC and the DSS Deputy Director, specific agency guidelines governing reporting of insider threat information by ITIMP offices and other DSS organizational components to the ITIMP manager or ITWG.

c. Propose a DSS process for performing oversight reviews by cleared officials designated by the DSS Director to ensure compliance with insider threat policy guidelines.

11. INSIDER THREAT WORKING GROUP (ITWG)

a. The ITWG will be composed of subject matter expert DSS employees appointed by the heads of DSS directorates. The ITWG will convene at the request of the ITIMP manager to review and consider potential insider threat-related incidents and foundational process activities.

b. The primary pillar organizations (CI, IA, and Security), along with OGC and OIG, will be permanent members of the working group and will be involved in all potential incidents where insider threat situations must be assessed and/or follow-on action is required.

c. HCMO, Industrial Security Field Operations Directorate, Business Enterprise Directorate, and CDSE will provide representatives to attend ITWG meetings on an “as required” basis.

d. The ITIMP manager will serve as Executive Agent and administrator of the ITWG.

e. The ITWG will socialize among its members incident reports for review, discussion and recommendation of appropriate action by the affected activities.

f. The ITWG will collect and consolidate reports of actions taken to identify potential insider threat vulnerabilities, gaps in controls, corrective actions or recommendations for corrective actions and lessons learned.

g. Within 30 days of the close of a calendar quarter, the ITWG will prepare a quarterly report for the ITEAG of incidents, identified threats, and corrective actions taken in the previous quarter. The quarterly reports will be consolidated into an annual report to the ITEAG.

h. The ITWG will task, as required, DSS support/enabling elements for information, expertise or follow-up action on an insider threat incident.

i. Upon the concurrence of a majority of the ITWG involved in reviewing an incident, the ITIMP manager will forward a coordinated report of the situation to the Deputy Director when there is reasonable cause to believe a serious compromise of classified information has occurred.

j. The ITWG, in reviewing an incident report, will consider, as necessary and in accordance with applicable law and policy, audit data collected and other data that may include, but is not limited to, facility access, foreign contacts, foreign travel, personnel security, personnel records and financial disclosure information.

12. ALL DSS PERSONNEL

a. All DSS personnel must:

(1) Follow applicable requirements in Executive Order 13526 (Reference (h)) and DoD Directive 5240.06 (Reference (j)) regarding any required reporting of planned or completed foreign travel. Personnel with access to sensitive compartmented information or a SAP must notify the DSS Office of Security before traveling to any foreign country.

(2) Notify the Office of Security, whenever possible, of proposed official or unofficial travel to a high threat country (as defined in the National Intelligence Priorities Framework and posted to the DSS SIPRNet website). All travelers to high threat countries must receive a defensive travel brief before departing.

(3) Report any deviation from approved itineraries, or unanticipated border crossings into any foreign country, regardless of location or duration, to Security personnel immediately upon return. Travelers returning from high threat countries must receive a post-travel debriefing from Security personnel.

(4) Notify the Office of Security, whenever possible, of proposed official or unofficial travel to countries that are not high threat. These employees may be required to receive a defensive travel brief prior to travel.

(5) Attend required training and comply with the reporting requirements of Reference (j), which identifies specific reportable contacts, activities, indicators, behaviors and cyber threats associated with foreign intelligence entities and other applicable reporting requirements.

b. All DSS employees who travel to foreign countries, or otherwise visit or have significant contact with foreign personnel, facilities, agencies, diplomatic facilities, or research or academic institutions, are encouraged to provide the Office of Security the names and background data, if known, of the primary foreign individuals with whom they expect to come in contact. The Office of Security will assess available information about these individuals for affiliations or relationships that could jeopardize the responsible sharing and safeguarding of classified information and CUI.

ENCLOSURE 3

DEFINITIONS

Anomaly: Activity or knowledge, outside the norm, that suggests or indicates U.S. Government facilities, systems, equipment, information or infrastructure are being used to damage, disrupt operations, compromise information and/or commit espionage.

Anomaly-based detection: The process of comparing counterintelligence, security, information assurance, law enforcement, and anti-terrorism/force protection behaviors and activities that are deemed normal against other observed events to identify significant deviations and or anomalous behavior.

Asset: Any resource, person, group, relationship, instrument, installation, process, or supply at the disposition of an organization for use in an operational or support role.

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 their elements, 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 information: Information that has been determined pursuant to Reference (h) 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 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 employee, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a person performing personal services under contract; 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.

Controlled unclassified information (CUI): 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 Reference (h), or the Atomic Energy Act, as amended.

Counterintelligence risk assessment: Examines threat information and identified organizational vulnerabilities to make an informed determination about the likelihood and consequence of the loss or compromise of critical assets to hostile actions of foreign intelligence services or non-state actors using intelligence tradecraft.

Critical asset: Any asset whose loss or compromise would negatively impact the capability of a department or agency to carry out its mission; or may impact the ability of another U.S. Government department or agency to conduct its mission; or could result in substantial economic loss; or which may impact on the national security of the United States.

Defensive travel brief: A classified or unclassified briefing on a specific country or countries to which an employee, detailee, or contractor employee assigned or detailed to DSS will travel in the near future. The travel brief will include the foreign intelligence threat, technical threat (to laptop computers and cell phones for example), criminal threat and, if known, the health threat, facing the employee, detailee or contractor. The brief should give the traveler strategies to mitigate those threats. The brief should also provide helpful in-country telephone numbers, such as the nearest U.S. Embassy or Consulate.

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.

Foreign national: Any person who is not a citizen or national of the United States.

High threat country: Any country that the National Intelligence Priority Framework has determined poses an intelligence threat to the responsible sharing and safeguarding of classified and sensitive information. The Office of the Director of National Intelligence publishes an appropriately classified list of high threat countries and updates it annually.

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

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

Insider threat: The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through violent acts, espionage, terrorism, unauthorized disclosure of national security information, or through the loss, denial 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. An inquiry or investigation pursuant to insider threat response actions can be conducted under the auspices of counterintelligence, security, law enforcement, or Inspector General elements, depending on statutory authority and internal policies governing the conduct of such activity in each agency.

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

Sensitive position: Any position so designated by the head of any department or agency in accordance with section 3(b) of Executive Order 10450 (Reference (e)), or its successor provision.

Special Access Program (SAP): Security protocols that provide highly classified information with safeguards and access restrictions that exceed those for regular (collateral) classified information. In addition to collateral controls, a SAP may impose more stringent investigative or adjudicative requirements, specialized nondisclosure agreements, special terminology or markings, exclusion from standard contract investigations (carve-outs), and centralized billet systems.

Substantial unofficial foreign contact: Recurring contacts with any foreign entity or foreign national not related to official duties; that is social, business-related, romantic, or sexual in nature; or is marked by bonds of affection, obligation or other commitment; or with whom the individual shares a residence. This does not refer to incidental, one time contact with foreign nationals where there will be no continuing relationship. Reportable contact includes in-person, written, telephonic, or any other electronic communication.

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