GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM P 2400.1

GSA POLICY AND PROCEDURE

SUBJECT: Insider Threat Program

1. Purpose. This Policy and Procedure establishes General Services Administration (GSA) policy and assigns responsibilities for the Insider Threat Program (ITP). The ITP seeks to establish a secure operating environment for GSA personnel, systems, and facilities from insider threats.

2. Background. President Obama signed Executive Order (E.O.) 13587 on October 7, 2011, establishing new Governmentwide requirements to improve responsible sharing and safeguarding of classified information on computer systems. Additional guidance is found in the November 21, 2012, Presidential Memorandum, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs" (Presidential Memorandum), which directed executive-branch departments and agencies to establish Insider Threat Programs that deter, detect, and mitigate actions by employees who may represent a threat to national security.

3. Scope and applicability. This Policy and Procedure applies to all GSA staff offices, regions, and GSA personnel who have access to or are eligible to access classified information and classified information systems (as detailed in E.O. 13587). GSA personnel shall include employees and all others with authorized access to GSA information and systems.

4. Cancellation. None.

5. Implementation. This Policy and Procedure is effective upon publication and will be reviewed and updated as needed or at 2-year intervals, whichever is earlier. The Chief Human Capital Officer shall take all necessary actions to implement the designation herein, including amending the GSA Delegations of Authority Manual, GSA Order ADM P 5450.39D, dated November 16, 2011.

6. Guiding Principles.

a. GSA is subject to insider threats and will take actions to mitigate or eliminate those threats.

b. GSA should continually identify and assess threats to the organization and its personnel and institute programs to defeat the threats.

c. GSA will leverage best practices used by the U.S. Intelligence Community and other Government agencies that operate counterintelligence programs and implement them across GSA.

7. Policy.

a. The ITP is established as a GSA-wide program to protect all GSA personnel, facilities, and automated systems from insider threats. This program seeks to prevent espionage, violent acts against the Nation or GSA, or the unauthorized disclosure of classified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems and classified information; and mitigate the risks to the security of classified information through administrative, investigative, or other responses.

b. The GSA ITP shall meet or exceed the minimum standards for such programs, as defined in E.O. 13587 and the November 21, 2012, Presidential Memorandum.

c. The responsibilities outlined below are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information. The ITP shall consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.

8. Responsibilities.

a. GSA Heads of Services and Staff Offices (HSSO). Each GSA HSSO is responsible for fully supporting the intent and requirements of the ITP and:

(1) Appointing an ITP Program Lead who will act as the HSSO's representative for GSA ITP implementing activities (except for OGC and OIG);

(2) Maintaining all associated records and submitting required reports to GSA's Office of Mission Assurance (OMA);

(3) Enforcing requirements to support the Insider Threat and the related training programs;

(4) Enforcing GSA Foreign Travel, Meeting and Foreign Visitor Programs for the purpose of tracking, documenting, and retrieving relevant information on cleared employee's foreign travel, meetings, and foreign visitor contacts;

(5) Ensuring responsible sharing of all required information pertaining to personnel, systems, and activities in accordance with applicable laws and privacy and civil liberties policies, with designated Insider Threat personnel conducting activities under the ITP.

b. GSA Regional Administrators (RA). Each GSA RA is responsible for fully supporting the intent and requirements of the ITP and:

(1) Enforcing requirements to support the Insider Threat and the related training programs;

(2) Enforcing GSA Foreign Travel, Meeting, and Foreign Visitor Programs for the purpose of tracking, documenting, and retrieving relevant information on cleared employees' foreign travel, meetings, and foreign visitor contacts;

(3) Ensuring responsible sharing of all required information pertaining to personnel, systems, and activities in accordance with applicable laws and privacy and civil liberties policies, with designated Insider Threat personnel conducting activities under the ITP.

c. Senior Agency Official for Insider Threat. The Associate Administrator of OMA is appointed as the Designated Senior Agency Official for Insider Threat. Responsibilities include:

(1) Leading GSA in establishing, implementing, and overseeing the activities of the ITP;

(2) Ensuring the program is executed in accordance with all applicable laws and privacy and civil liberties policies;

(3) Establishing guidelines and procedures for the retention, sharing, and safeguarding of records and documents necessary to complete inquiries and assessments;

(4) Establishing and leading an ITP Core Coordination Council for consultation on all ITP-related issues, conducting program oversight and reviews, as well as identifying and making program resource recommendations. At a minimum, the committee will be comprised of senior representatives from the Office of Human Resources Management, Office of the Chief Information Officer, and Office of the Chief Financial Officer;

(5) Establishing an ITP activity with a centralized analysis and response capability to manually and/or electronically gather, integrate, review, assess and respond to information derived from Counterintelligence, Information Assurance,

Security, Human Resources, the monitoring of user computer activity, and other information sources as deemed appropriate;

(6) Overseeing the collection, analysis, and reporting of information across GSA to support the identification and assessment of insider threats;

(7) Establishing and managing all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee;

(8) Ensuring the ITP establishes procedures for GSA insider threat response action(s) to clarify or resolve insider threat matters. Those procedures will ensure that response action(s) are centrally managed and documented;

(9) Leading the establishment and execution of an Insider Threat Awareness Training Program in accordance with the Presidential Memorandum for National Insider Threat Policy; and

(10) Detailing or assigning volunteer staff, as appropriate and necessary, to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force.

d. The Office of Human Resources Management (OHRM) is responsible for:

(1) Appointing a representative to coordinate with the Associate Administrator of OMA on all matters related to the sharing of all relevant personnel records, to support the identification, analysis, assessment, and resolution of any potential insider threat matter; and

(2) Implementing policies and procedures to inform GSA employees as to the existence of the ITP.

e. The Office of the Chief Financial Officer is responsible for:

Appointing a representative to coordinate with the Associate Administrator of OMA on all matters related to the sharing of all relevant financial records, to support the identification, analysis, assessment, and resolution of any potential insider threat matter;

f. The Office of General Counsel (OGC) is responsible for:

(1) Providing legal advice for the establishment, implementation, execution, management, and oversight of the GSA ITP; and

(2) Providing legal review of all responses to any inquiries stemming from the execution of the ITP.

g. The Office of Chief Information Officer (OCIO) is responsible for:

(1) Appointing a representative to coordinate with the Associate Administrator of OMA on all matters related to the sharing of all relevant Information Technology/Information Assurance records/monitoring, to support the identification, analysis, assessment, and resolution of any potential insider threat matter;

(2) Establishing and enforcing a GSA information system protection program to identify system security threats, vulnerabilities, and mitigation strategies; and

(3) Establishing a comprehensive GSA user awareness program to inform GSA personnel of system monitoring and auditing.

h. The Office of the Inspector General's (OIG) role:

All credible Insider Threat Information will be coordinated and shared with the OIG, which will then take action as the OIG deems appropriate, including coordinating with other law enforcement agencies, such as the Federal Bureau of Investigation.

10. Signature.

_____ June 20, 2014

DAN TANGHERLINI Date
Administrator

Appendix A. Reference and Authorities List
Appendix B. Definitions

Appendix A. Reference and Authorities List

The following list of references and authorities should be used in developing, implementing, and executing the overall Insider Threat Program and any supporting sub-programs. This list will be reviewed and updated as required or at 2-year intervals, whichever is earlier:

Public Laws:

National Security Act of 1947, 50 U.S.C. § 3002, *et seq*.

Counterintelligence Enhancement Act of 2002, 50 U.S.C. § 3382, *et seq* .

Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C § 3002, *et seq*.

Executive Orders:

E.O. 10450, Security Requirements for Government Employment, April 27, 1953, as amended.

E.O. 12333, United States Intelligence Activities, December 4, 1981, as amended.

E.O. 12968, Access to Classified Information, August 4, 1995.

E.O. 12829, National Industrial Security Program, January 6, 1993, as amended.

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. 13526, Classified National Security Information, December 29, 2009.

E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.

Presidential Directives:

Presidential Decision Directive PDD/NSC-12 Security Awareness and Reporting of Foreign Contacts, August 5, 1993.

November 21, 2012 Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.

GSA Policies & Procedures:

GSA Directive, HCO 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information

GSA Directive, CIO P 2100.1I, GSA Information Technology (IT) Security Policy

GSA Directive, CIO 2104.1A, GSA Information Technology (IT) Rules of Behavior

GSA Directive, CPO 1878.1, GSA Privacy Act Program

GSA Directive, ADM P 9732.1D, Suitability and Personnel Security

GSA Directive, ADM P 5400.1, Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contacts

Appendix B. Definitions

Agencies: Pursuant to section 7 of E.O. 13587, the term “agencies” has the meaning set forth in section 6.1 (b) of E.O. 13526, which includes any “executive agency” as defined in 5 U.S.C. 105 and “any other entity within the executive branch that comes into the possession of classified information.”

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

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

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 GSA; an expert or consultant to GSA; an industrial or commercial contractor, licensee, certificate holder, or grantee of GSA, including all subcontractors; a personal services contractor employee; or any other category of person who acts for or on behalf of GSA as determined by the Administrator.

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 GSA resources or capabilities.