United States
Department of
Agriculture

Departmental Management

Office of Homeland Security &
Emergency Coordination

USDA Insider Threat Program

DR 4600-003

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

# DEPARTMENTAL REGULATION	**Number:** 4600-003
SUBJECT: USDA Insider Threat Program	**DATE:** June 30, 2014
	OPI: Office of Homeland Security and Emergency Coordination (OHSEC)

1. PURPOSE

The purpose of this directive is to set forth the U.S. Department of Agriculture's (USDA) roles and responsibilities for an Insider Threat Program, as directed by Executive Order (EO) 13587 dated October 7, 2011, titled, *Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information* and the *National Insider Threat Policy and the Minimum Standards* issued in November 2012.

2. BACKGROUND

The Secretary of Agriculture, under EO 13587, is mandated to develop and implement an Insider Threat Program with the primary mission to prevent, deter and detect compromises of classified information by malicious insiders.

Although EO 13587 applies only to the safeguarding and sharing of classified national security information, the National Insider Threat Task Force (NITTF) recognizes that an agency may possess information that it considers sensitive but that is not classified. As stated in the NITTF's Guide to Accompany the National Insider Threat Policy and

Minimum Standards, issued in November 2013, the policies and standards under EO 13587 can be applied generally to protect the sensitive but unclassified environment.

The National Insider Threat Policy and Minimum Standards require that the USDA addresses key components to be implemented:

a. Establish a program for deterring, detecting, and mitigating insider threat;, security, information assurance, and other relevant functions and resources to identify and counter the insider threat;

b. 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.

c. 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 security, information assurance, and human resources offices.

d. 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.

e. Consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, or civil liberties issues (including use of personally identifiable information) are appropriately addressed.

f. Promulgate additional department and agency guidance, if needed, to reflect unique mission requirements, but not inhibit meeting the minimum standards issued by the NITTF pursuant to this policy.

g. 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).

h. 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 NITTF.

3. CANCELLATION

This regulation does not supersede any existing regulations.

4. POLICY

Departmental Agencies and Offices are required to comply with EO 13587, to include any associated Departmental Regulations (DR) requiring the safeguarding of classified information and classified networks. This DR is applicable to USDA employees, contractors, and individuals who serve in advisory, consultant, or non-employee affiliate capacities who have been granted access to classified information.

5. AUTHORITIES AND REFERENCES

This directive must be used in conjunction with:

a. White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated 21 November 2012;

b. Executive Order 13587, Structural Reforms to Improve the Security Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, dated 7 October 2011;

c. NITTF Guide to Accompany the National Insider Threat Policy and Minimum Standards, November 2013;

d. Executive Order 13556, Controlled Unclassified Information, dated November 4, 2010;

e. Section 811(c) of the Intelligence Authorization Act for FY 1995;

f. Executive Order 10450, Security Requirements for Government Employment, dated 27 April 1953; and

g. Departmental Regulation 4600-001, USDA Personnel Security Clearance Program, dated 4 April 2008.

6. ORGANIZATION

Through delegation from the USDA Secretary, the Director of the Office of Homeland Security and Emergency Coordination (OHSEC) is the Senior Insider Threat Official,

hereafter referred to as Senior Official, for administration and coordination of the Insider Threat program.
The Senior Official has delegated authority to carry out the Insider Threat program to the Insider Threat Branch, also known as the Hub, lead by an Insider Threat Coordinator. The Hub is a centralized location that will receive and analyze all Insider Threat related concerns.

A group of senior-level officials will serve as Stakeholders (aka Hub Members) who will meet upon notification from the Insider Threat Coordinator that a potential insider threat is present. The Stakeholders will analyze cases with the Insider Threat Coordinator and determine if the matter warrants a Federal Bureau of Investigation (FBI) 811(c) referral and will create an information sharing capability.

The Stakeholders will be represented from the following offices: the Office of Homeland Security and Emergency Coordination, the Office of the Chief Financial Officer, the Office of the Chief Information Office, the Office of Civil Rights, the Office of Ethics, the Office of the Inspector General, the Office of the General Counsel, the Office of Human Resources Management, and the Office of Operations. Each office will identify a primary and alternate representative who will sit on the panel.

All members of the Hub will possess a minimum of a Top Secret (TS) security clearance (as appropriate) with access to Sensitive Compartmented Information (SCI) (if deemed necessary) and will be required to sign a non-disclosure agreement.

7. GENERAL RESPONSIBILITIES

a. Secretary of Agriculture.

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

(2) Implement an insider threat detection and prevention program consistent with guidance and standards developed by the NITTF;

(3) Perform self-assessments of compliance with policies and standards issued, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee;

(4) Provide information and access, as warranted and consistent with law, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the NITTF of compliance with relevant established policies and standards; and

b. Subcabinet Officers, Agency Administrators, and Office Directors.

(1) Ensuring classified information is controlled and that access to classified networks and information is restricted to authorized personnel only;

(2) Ensuring employees who are granted security clearances receive initial security indoctrination, annual security refresher training, and a debriefing after classified information access is no longer required; and

(3) Ensuring timely reporting of any suspicious activity, which may indicate the presence of an insider threat.

c. Director of the Office of Homeland Security and Emergency Coordination.

(1) Developing and disseminating the Department's insider threat policy and implementation plan to be approved by the Secretary of Agriculture;

(2) Providing an annual report to the Secretary of Agriculture on the status of the program, to include documented results of the program's accomplishments, resources allocated, insider threats identified, program goals and impediments and/or challenges;

(3) Collaborating with USDA General Counsel and appropriate privacy and civil liberties officials to ensure that all insider threat program activities are conducted in accordance with applicable laws and privacy requirements and civil liberties policies;

(4) Establishing oversight procedures to ensure only authorized personnel are permitted access to restricted records and data. Such personnel shall receive training on the proper handling and use of records and data while performing their authorized functions;

(5) Establishing guidelines for the retention of records and documents necessary to document USDA activities as required by Executive Order 13587;

(6) Facilitating oversight reviews by cleared officials designated by the USDA to ensure compliance with national and Department policies and standards;

(7) Coordinating all Intelligence Authorization Act Section 811(c) referrals with Departmental Management and Office of Inspector General (OIG), as required, prior to submitting a referral to the Federal Bureau of Investigation (FBI); and

(8) Serving as the USDA liaison to the Intelligence Community for Insider Threat and Counterintelligence activities within the Department.

d. Office of Human Resources Management.

(1) Identifying a primary and alternate member to represent OHRM on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to 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;

(3) Reporting all derogatory issues on an employee possessing a security clearance; and

(4) Reporting all derogatory issues on employees may possess information that it considers sensitive but that is not classified.

e. Office of Inspector General.

(1) Identifying a primary and alternate member to represent OIG on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to all relevant OIG investigations as may be necessary for resolving or clarifying insider threat matters;

(3) Reporting all derogatory issues on an employee possessing a security clearance; and

(4) Reporting all derogatory issues on employees may possess information that it considers sensitive but that is not classified.

f. Office of the Chief Information Officer.

(1) Identifying a primary and alternate member to represent OCIO on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to all relevant unclassified network information 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;

(3) Reporting all derogatory issues on an employee possessing a security clearance; and

(4) Reporting all derogatory issues on employees may possess information that it considers sensitive but that is not classified.

g. Office of the Assistant Secretary for Civil Rights.

(1) Identifying a primary and alternate member to represent OASCR on the Hub Working Group; and

(2) Advising on applicable civil liberty laws and regulations.

h. Office of the General Counsel.

(1) Identifying a primary and alternate member to represent OGC on the Hub Working Group; and

(2) Providing guidance and assistance to the Insider Threat Branch to ensure the Department's compliance applicable laws.

i. Office of Operations.

(1) Identifying a primary and alternate member to represent OO on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to all relevant OO databases and files to include, but not limited to, facility access records, workplace violence records, and hotline complaints;

(3) Reporting all derogatory issues on an employee possessing a security clearance; and

(4) Reporting all derogatory issues on employees may possess information that it considers sensitive but that is not classified.

j. Office of Ethics.

(1) Identifying a primary and alternate member to represent OE on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to all relevant OE databases and files to include, but not limited to, financial disclosure and reports of outside activities; and

(3) Advising on applicable civil liberty laws and regulations.

k. Office of the Chief Financial Officer.

(1) Identifying a primary and alternate member to represent OCFO on the Hub Working Group;

(2) Providing timely access, through manual and/or electronic means to all relevant OCFO databases and files to include, but not limited to, travel cards, purchase cards, wage garnishments, and other financial information as applicable;

(3) Reporting all derogatory issues on an employee possessing a security clearance; and

(4) Reporting all derogatory issues on employees may possess information that it considers sensitive but that is not classified.

l. <u>USDA Employees, Contractors, and Individuals who serve in Advisory, Consultant, or Non-Employee Affiliate capacities.</u>

(1) Complying with EO 10450, Security Requirements for Government Employment, that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States;

(2) Reporting Insider Threat-related incidents, behavioral indicators or other matters concerning national security to the Insider Threat Branch; and

(3) Complying with DR 3440-001, USDA Classified National Security Information Program.

-END-