DEPARTMENTAL REGULATION	Number: DR 3441-001
SUBJECT: USDA Sensitive Compartmented Information Security Program	DATE: January 18, 2012
	OPI: Office of Homeland Security and Emergency Coordination

1. PURPOSE

This regulation establishes the responsibilities and procedures for accessing, safeguarding, and disseminating Sensitive Compartmented Information (SCI) within U.S. Department of Agriculture (USDA). SCI is defined as classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence. This Departmental Regulation (DR) is applicable Departmental employees, contractors, and individuals serving in advisory, consultant, or non-employee affiliate capacities who have been granted access to SCI materials.

2. REFERENCES

a. National Security Act of 1947;
b. Executive Order 13526, December 29, 2009;
c. Intelligence Community Directive (ICD) 503 Information Technology Systems Security Risk Management, Certification and Accreditation, September 15, 2008;
d. Intelligence Community Program Memorandum (ICPM) 2006-700.8 Directive Administrative Security, July 12, 2006;
e. ICD 700 Protection of National Intelligence, September 21, 2007;
f. ICD 701 Unauthorized Disclosures, March 14, 2007;
g. ICD 703 Protection of SCI Sources and Methods;
    (1) ICPG 703.1 Continuing Reporting
    (2) ICPG 703.2 SCI Management
    (3) ICPG 703.3 Non-Title 50
    (4) ICPG 703.4 Foreign Partners
    (5) ICPG 703.5 Dissemination Controls
    (6) ICPG 703.6 Risk Management
h. ICD 705 Physical/Technical Security Standards, May 26, 2010;
i. ICPM 2007-700-33 Foreign Travel, September 13, 2007

j. ICD 710Classification and Control Markings System, September 11, 2009

3. POLICY

USDA will safeguard SCI within its control from unauthorized disclosure. It is the policy of USDA that:

a. USDA agencies must provide a legitimate justification when requesting SCI access for each individual and limit the number of SCI clearances to the minimum necessary to meet USDA mission requirements;

b. SCI shall not be released or shared with persons who do not possess an active security clearance equal to or higher than the classification level of the material in question and without a verified need to know;

c. SCI material may only be processed, stored, discussed, or safeguarded in facilities within USDA identified and accredited as SCI Facilities (SCIFs);

d. Annual security awareness training is required of all employees cleared to access SCI;

e. Destruction of SCI shall be completed by shredding with a National Security Agency certified shredder;

f. Incidents involving the alleged mishandling and potential compromise of SCI must be reported immediately upon discovery to the Personnel and Document Security Division (PDSD) of the Office of Homeland Security and Emergency Coordination; and

g. SCI cleared persons must report any personal foreign travel in advance to PDSD and may be required to attend specialized briefings or debriefings related to the travel itinerary.

4. ROLES AND RESPONSIBILITIES

a. The Secretary of Agriculture is responsible for designating a Senior Agency Official to manage, develop and administer the SCI Security Program. This designation is currently made to the Director, Office of Homeland Security and Emergency Coordination (OHSEC). The Senior Agency Official is required to maintain a Top Secret clearance, with SCI access.

b. The Senior Agency Official is the primary liaison between USDA and the CIA and the National Security Agency (NSA). This position is

responsible for identifying necessary resources to manage the SCI Security Program and providing program oversight.

c. Subcabinet Officials, Agency Administrators, and Staff Office Directors, whose organizations require access to SCI material, are responsible for:

(1) Ensuring the number of persons granted access to SCI material is based on clearly-articulated, mission related "need-to-know" criteria, endorsing the written justification, and submitting the SCI request to OHSEC; and

(2) Ensuring employees who hold a security clearance with access to SCI receive initial SCI security indoctrination training, annual security refresher training, and a debriefing after SCI access is terminated.

d. The Director, OHSEC, is responsible for:

(1) Establishing and administering the USDA SCI Security Program in accordance with all applicable authorities, regulations and manuals;

(2) Maintaining an oversight role to ensure consistent and effective implementation of the SCI Security Program throughout USDA;

(3) Approving or denying requests for access to SCI;

(4) Serving as the focal point for intelligence liaison between USDA and the intelligence community for matters of national security and intelligence related matters, excluding cyber-security;

(5) Approving all requests for installation, maintenance, upgrade and disposal of all Information Technology (IT) systems and equipment whereby SCI is accessed, stored, and processed;

(6) Approving all requests for the construction, modification, or closure of any SCIF within USDA operations; and

(7) Obtaining final accreditation for SCIFs and ensuring such facilities are adequately justified by USDA mission requirements.

f. The Chief, Office of Chief Information Office is responsible for:

(1) Providing Communications Security support to maintain the integrity of technical equipment to support the ongoing requirements for secure telecommunications and SCI connectivity;

(2) Incorporating, where appropriate, applicable USDA information security policies and procedures into USDA policies and standards for IT system protection;

(3) Serving as the focal point for intelligence liaison between USDA and the intelligence community for matters related to cyber security;

(4) Coordinating with OHSEC to investigate the potential breaches or mishandling of classified information occurring within classified IT systems, conducting requisite forensic investigations; and

(5) Sharing with OHSEC the results of any forensic investigation to confirm or mitigate mishandling or compromise of classified information.

g. PDSD is responsible for implementing all policies and directives noted herein to maintain proper control and protection of collateral and SCI related documents and systems. This includes:

(1) Day-to-day management of the Department's SCI information security program;

(2) Processing and sponsoring all SCI clearance requests to the CIA and notifying appropriate officials of all approvals and denials of access;

(3) Issuing and updating Department-wide SCI information security policies and procedures;

(4) Coordinating and providing initial SCI security indoctrination training, annual refresher training, and security debriefings;

(5) Coordinating approval, construction, accreditation, and maintenance of all SCIFs and

(6) Receiving reports of incidents of suspected mishandling or inadvertent disclosure of classified information; conducting requisite security inquiries/investigations; and making referrals to external agencies when a compromise of SCI has occurred; and

(7) Notifying CIA of any personnel security issues or concerns that may jeopardize an individual's continued eligibility for SCI access.

h. Employees, contractors, and other individuals maintaining SCI access at USDA are responsible for the following:

(1) Adhering to the provisions of this DR;

(2) Immediately reporting security irregularities and security violations to their respective information security coordinators and supervisors;

(3) Completing an initial SCI security indoctrination briefing, annual security refresher briefing, and security debriefings in a timely manner;

(4) Notifying PDSD of impending personal travel to or through foreign countries by completion of form AD-1196 and participating in any required defensive threat briefings, and

(5) Reporting to PDSD any close and continuing contact with foreign nationals by submitting a completed Foreign Contact Questionnaire. Contact includes personal and/or intimate relationships, outside employment, domestic help, and any situation that causes SCI cleared persons to believe they are being targeted by a foreign government.

END