DR 3440-001

United States
Department of
Agriculture

Departmental Administration
Office of Security Services
Personnel and Document Security Division

USDA Classified National Security Information Program Regulation

DR 3440-001

DEPARTMENTAL REGULATION	Number: 3440-001
SUBJECT: USDA Classified National Security Information Program Regulation	DATE: January 9, 2008
	OPI: Office of Security Services

1. PURPOSE

This regulation prescribes Departmental roles and responsibilities for the classification, declassification, and safeguarding of classified national security information, and promulgates a revised Departmental Manual 3440-001, USDA Information Security Program Manual.

2. CANCELLATION

This regulation supersedes Departmental Regulation (DR) 3440-001, dated August 26, 1983.

3. BACKGROUND

The Secretary of Agriculture has been delegated the original classification authority (OCA) by Presidential Order (67 FR 189), effective September 26, 2002, and may classify USDA information as either Confidential or Secret.

Executive Order (E.O.) 12958, as amended by Executive Order 13292, "Classified National Security Information" (hereafter, E.O. 12958), and Information Security Oversight Office (ISOO) Directive 1, "Classified National Security Information," establish the minimum standards and procedures for protecting classified national security information (hereafter, classified information). Security procedures and guidance are detailed in Departmental Manual (DM) 3440-001 "Information Security Program Manual".

4. POLICY

Departmental agencies and offices must comply with E.O. 12958, ISOO Directive 1, and this DR. 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. It is the policy of USDA that:

a. The Secretary may base a classification determination on one or more of the following categories:

(1) Government information;

(2) Foreign relations or foreign activities of the United States, including confidential sources;

(3) Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

(4) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

(5) Weapons of mass destruction.

b. Classified national security information consists of information that has been determined pursuant E.O. 12958 to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form in accordance with the Executive Order and DM 3440-001. Minimum safeguarding of classified information requires storage in a General Services Administration (GSA) approved security container. Security containers meeting the standards and specifications established by GSA may be procured through the Federal Supply System.

c. USDA agencies shall prevent unnecessary access to classified information by establishing a need for access to classified information, limiting access to a minimum consistent with operational and security requirements and needs, and ensuring classified information is not released to, 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.

d. USDA will ensure declassification of information as soon as feasible, but not longer than 25 years from the time of classification. Declassification is accomplished using the systematic, automatic, and mandatory declassification processes outlined in E.O. 12958.

e. Continuous security awareness training is required of all employees holding national security clearances. Training will be coordinated and presented by the Office of Security Services (OSS).

f. Destruction and disposal of classified information must be done in compliance with EO 12958 and the ISOO Directive 1. Confidential and Secret information can be shredded using a National Security Agency (NSA) approved shredder. NSA approved shredders may be procured through the Federal Supply System.

g. Incidents involving the mishandling of classified information must be reported to the agency's Information Security Coordinator, or the OSS, Personnel and Document Security Division (PDSD) immediately upon discovery.

5. ROLES AND RESPONSIBILITIES

a. The Secretary of Agriculture may only re-delegate OCA to the Deputy Secretary. The Secretary must designate a Senior Agency Official responsible for the development and administration of the Information Security Program. This designation is currently in a delegation of authority made to the Assistant Secretary for Administration and has been re-delegated to the Director, OSS. The Senior Agency Official is required to maintain a Top Secret clearance.

b. The Senior Agency Official is the primary liaison between USDA and the ISOO. This position is responsible for identifying necessary resources to manage the Information Security Program and providing program oversight.

c. Subcabinet Officers, Agency Administrators, and Office Directors, whose organizations require access to classified material are responsible for:

(1) Designating an Information Security Coordinator to serve as a liaison to the PDSD;

(2) Providing subject matter experts to assist with the development of recommendations for the Secretary to exercise the OCA;

(3) Ensuring classified information is created, marked, stored, transmitted, and destroyed in accordance with this DR and DM 3440-001;

(4) Ensuring the number of persons granted access to classified information is limited to those with a "need-to-know" to effectively and efficiently carry out USDA program responsibilities;

(5) Ensuring employees who hold a security clearance receive initial security indoctrination training, annual security refresher training,

and a debriefing after classified information access is no longer required; and

(6) Ensuring that applicable performance standards include language requiring the proper protection of classified information for all employees who routinely handle classified information.

d. The Director, OSS, Departmental Administration, is responsible for:

(1) Establishing and administering the USDA Information Security Program in accordance with E.O. 12958, ISOO Directive 1, and this DR;

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

(3) Serving as the Deciding Official for the suspension, denial, and revocation of security clearances involving USDA personnel.

e. The Chief Information Officer is responsible for:

(1) Certifying and accrediting USDA computer systems for processing collateral classified information;

(2) Coordinating with the PDSD requests for processing collateral classified information on USDA computers and establishing secure networks; and

(3) Incorporating, where appropriate, applicable USDA information security policies and procedures into USDA policies and standards for Information Technology system protection.

f. The PDSD is responsible for implementing E.O. 12958, ISOO Directive 1, DR 3440-001 and DM 3440-001. This includes:

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

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

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

(4) Approving rooms for the storage, discussion, and processing of

classified information up to and including Sensitive Compartmented Information; and

(5) Receiving reports of incidents of suspected mishandling or inadvertent disclosure of classified information and conducting requisite security inquiries when appropriate.

g. Information Security Coordinators are responsible for being the primary liaison between their agency and the PDSD. They are responsible for ensuring their agency meets the requirements identified in this DR and DM 3440-001. Information Security Coordinators shall maintain a minimum of a Secret security clearance. Their responsibilities include:

(1) Advising their agency on properly marking, storing, processing, disclosing, transmitting, and destroying classified information;

(2) Conducting self-inspections within the agency to ensure they are properly handling classified information;

(3) Coordinating information security refresher training;

(4) Gathering information annually for ISOO reports;

(5) Assisting with classification, declassification, and challenges to classification; and

(6) Reporting security violations and concerns to PDSD.

h. Employees, contractors, and individuals maintaining a security clearance for working with classified information at USDA are responsible for the following:

(1) Adhering to the provisions of this DR and DM 3440-001;

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

(3) Completing the initial security indoctrination training, annual security refresher training and security debriefings.

END