

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

DEPARTMENTAL REGULATION	Number: DR 3440-001
SUBJECT: USDA Classified National Security Information Program	DATE: June 9, 2016
	OPI: Office of Homeland Security and Emergency Coordination

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 (DM) 3440-001, USDA Information Security Program Manual.

2. CANCELLATION

This regulation supersedes Departmental Regulation (DR) 3440-001, dated October 5, 2011.

3. BACKGROUND

The Secretary of Agriculture has been delegated the Original Classification Authority (OCA) by Presidential Order (75 Federal Register [FR] 735), effective December 29, 2009, and may classify USDA information as either Confidential or Secret.

Executive Order (E.O.) 13526 “Classified National Security Information” (hereafter, E.O. 13526) and 32 Code of Federal Regulations (CFR) Part 2001 “Classified National Security Information Implementing Directive No.1” (hereafter 32 CFR Part 2001) establish the minimum standards and procedures for protecting classified national security information (hereafter, classified information). Security procedures and guidance are detailed in DM 3440-001 “Classified National Security Information Program Manual.”

4. POLICY

Departmental Agencies and Offices must comply with E.O. 13526, 32 CFR Part 2001, 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 (1) or more of the following categories:

- (1) Military plans, weapons systems, or operations;

- (2) Foreign government information;
 - (3) Intelligence activities (including covert action), intelligence sources or methods or cryptology;
 - (4) Foreign relations or foreign activities of the United States, including confidential sources;
 - (5) Scientific, technological, or economic matters relating to the national security;
 - (6) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to the national security; and
 - (7) The development, production or use of weapons of mass destruction.
- b. Information may be originally classified under the terms of E.O. 13526, only if all the following conditions are met:
- (1) An original classification authority is classifying the information;
 - (2) The information is owned by, produced by or for, or is under the control of the United States Government;
 - (3) The information falls within one (1) or more of the categories of information listed above in paragraph 4 (a); and
 - (4) The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.
- c. Classified national security information consists of information that has been determined pursuant to E.O. 13526 to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form in accordance with E.O. 13526 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.
- d. If there is any significant doubt about the need to classify information, it shall not be classified. This provision does not:
- (1) Amplify or modify the substantive criteria or procedures for classification; or
 - (2) Create any substantive or procedural rights subject to judicial review.
- e. 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. Whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or unclassified form.

- f. 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. 13526.
- g. Continuous security awareness training is required of all employees holding national security clearances. Training will be coordinated and presented by the Office of Homeland Security and Emergency Coordination (OHSEC), Personnel and Document Security Division (PDSB).
- h. Destruction and disposal of classified information must be done in compliance with E.O. 13526 and 32 CFR Part 2001. 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.
- i. Incidents involving the mishandling of classified information must be reported to the Agency's Information Security Coordinator and the PDSB Classified National Security Program Branch immediately upon discovery.

5. ROLES AND RESPONSIBILITIES

- a. The Secretary of Agriculture is delegated as the OCA for USDA. The Secretary must designate a Senior Agency Official (SAO) responsible for the development and administration of the Classified National Security Information Program (CNSIP). This designation is currently in a delegation of authority made to the Assistant Secretary for Departmental Management and has been re-delegated to the Director of OHSEC. 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 Information Security Oversight Office (ISOO). This position is responsible for identifying necessary resources to manage the CNSIP 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 PDSB;
 - (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 carry out USDA program responsibilities;
 - (5) Ensuring employees who hold a security clearance receive initial security indoctrination training, annual security refresher training, derivative classification training, and a debriefing after classified information access is no longer required;
 - (6) Providing PDSO an annual updated list of individual within their Agency who is authorized to apply derivative classification marking;
 - (7) Ensuring their organization conduct, complete and report the finding of the self-inspection to PDSO no later than the second week of August annually; and
 - (8) Ensuring the performance standards includes the designation and management of classified information as a critical element, or an item to be evaluated in the rating of:
 - (a) Original classification authority;
 - (b) Security managers or security specialist; and
 - (c) Of all personnel who duties significantly involve the creation or handling of classified information and personnel who regularly apply derivative classification markings.
- d. The Director of OHSEC is responsible for:
- (1) Establishing and administering the USDA CNSIP in accordance with E.O. 13526, 32 CFR Part 2001, and this DR;
 - (2) Maintaining an oversight role to ensure consistent and effective implementation of the Information Security Program throughout USDA;
 - (3) Serving as the Deciding Official for the suspension, denial, and revocation of security clearances involving USDA personnel;
 - (4) Granting a waiver for individuals who fail to complete required training for original classification and derivative classification authority due to unavoidable circumstances;
 - (5) Suspending classification authority of those individuals who fail to complete mandatory training for original classification to include declassification or derivative classification and has not been granted a waiver;

- (6) Ensuring USDA Classification Guide is reviewed at a minimum of once every five (5) years, or upon regulatory changes;
 - (7) Establishing a system for processing, tracking and recording formal classification challenges made by authorized holders;
 - (8) Advising authorized holders of their rights to appeal to the Interagency Security Classification Appeals Panel (ISCAP) the decisions of the Agency on their challenge;
 - (9) Ensuring PDSO reports the annual completion of self-inspections report by Agencies that receive, generate, process and store classified information;
 - (10) Verifying the accuracy of information provided on the self-inspections reports prior to submitting report to ISOO;
 - (11) Coordinating with the SAO the submission of the annual report to ISOO; and
 - (12) Reporting security violations and/or improper declassifications to the Director of ISOO.
- e. The Chief Information Officer is responsible for:
- (1) Certifying and accrediting USDA computer systems for processing collateral classified information;
 - (2) Coordinating with PDSO 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 systems protection.
- f. PDSO is responsible for implementing E.O. 13526, 32 CFR Part 2001, DR 3440-001 and DM 3440-001. This includes:
- (1) Day-to-day management of the Department's information security program;
 - (2) Issuing and/or updating Department-wide information security policies, and procedures;
 - (3) Reviewing and updating the Security Classification Guide a minimum of every five (5) years, or upon regulatory changes and incorporate original classification decisions as soon as practicable;
 - (4) Coordinating the Security Classification Guide updates with users and subject matter experts;

- (5) Coordinating and providing initial security indoctrination training, annual refresher training, and security debriefings;
 - (6) Developing and coordinating statistical data use by Agencies and Staff Offices for self-inspection report;
 - (7) Approving rooms for the storage, discussion, and processing of classified information up to and including Sensitive Compartmented Information;
 - (8) Receiving reports of incidents of suspected mishandling or inadvertent disclosure of classified information and conducting requisite security inquiries when appropriate;
 - (9) Providing mandatory training for Original Classification Authorities each year and training every two (2) years for those personnel who create derivatively marked classified documents in accordance with §2001.71(c) and (d) of 32 CFR 2001;
 - (10) Recommending suspension of access to classified information for individuals who failed to complete mandatory training; and
 - (11) Providing support via training or individual support to Agencies requesting guidance on the development and marking of derivatively classified documents with respect to Part 2 of E.O 13526 and § 2001.22 of 32 CFR Part 2001.
- g. Information Security Coordinators are responsible for being the primary liaison between their Agency and 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;
 - (6) Reporting security violations and concerns to PDSD; and
 - (7) Maintaining a list of all individuals within their Agency with authority to apply derivative classification markings.
- 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;
- (3) Completing the initial security indoctrination training, annual security refresher training, security debriefings and derivative classification training as required;
- (4) Requesting a waiver for completing mandatory training in the required time and ensuring training is completed as soon as practicable. Requests must be submitted in writing with justification for waiver; and
- (5) Exercising their right to challenge classified information they believe to be improperly classified and the right to appeal the agency's decision to the ISCAP.

-END-