DM 3440-001

United States
Department of
Agriculture

Departmental Administration
Office of Security Services
Personnel and Document Security Division

USDA Classified National Security Information Program Manual

DM 3440-001

TABLE OF CONTENTS

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

DEPARTMENTAL MANUAL	**Number:** 3440-001
SUBJECT: USDA Classified National Security Information Program Manual	**DATE:** May 1, 2008
	OPI: Office of Security Services

CHAPTER 1

GENERAL INFORMATION

1. PURPOSE

This Manual establishes the policies and procedures that govern the U.S. Department of Agriculture (USDA) Information Security Program, including uniform requirements and guidance for classifying, safeguarding, declassifying, and destroying classified national security information, whether originated by or released to USDA.

2. SCOPE

This Manual applies to all USDA mission areas, agencies, and offices and their contractors who possess, handle, distribute, process, transmit, transport, and/or store classified information. Individuals serving in an advisory or consultant capacity who have been entrusted with USDA classified information are required to protect that information according to standards commensurate with those discussed in this Manual.

3. AUTHORITY

The authority for this guidance is derived from Executive Order 12958, as amended; Classified National Security Information (hereafter, E.O. 12958); the Information Security Oversight Office (ISOO) Directive 1, Classified National Security Information (NSI); and Department Regulation 3440-001, USDA Classified National Security Program.

4. CANCELLATION

This Manual supersedes DM 3440-001, Classification, Declassification, and Safeguarding Classified Information, dated August 10, 1983.

5. RESPONSIBILITIES

E.O. 12958 requires each Department that has been given original classification authority (OCA) to establish an information security program (ISP) that ensures the protection of national security classified information.

a. The Secretary of Agriculture, or delegated official, is responsible for originally classifying USDA information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. The Secretary will:

(1) demonstrate a personal commitment and dedicate senior management to the successful implementation of the ISP;

(2) commit necessary resources to the effective implementation of the ISP established;

(3) ensure that Departmental record systems are designed and maintained to optimize the safeguarding of classified information and to facilitate its declassification under the terms of E.O. 12958 when it no longer meets the standards for continued classification;

(4) receive specific training on how to originally classify USDA information; and

(5) designate a Senior Agency Official (SAO) to direct and administer the ISP.

b. The Assistant Secretary for Administration (ASA) is designated by the Secretary as the SAO who oversees the ISP and serves as liaison between USDA and the National Archives and Records Administration (NARA), ISOO. This designation has been re-delegated to the Director of USDA's Office of Security Services (OSS). The SAO shall maintain a minimum of a Top Secret security clearance and will:

(1) oversee USDA's ISP;

(2) promulgate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public; and

(3) report annually to ISOO as required by ISOO Directive 1.

c. USDA agencies, mission areas, and offices are responsible for identifying an Information Security Coordinator (ISC) and applying adequate resources to protect classified information.

d. The OSS Personnel and Document Security Division (PDSD) is responsible for revisions, additions, or deletions to this document. In addition, OSS will:

(1) establish and maintain security education and training programs to include training each OCA;

(2) establish and maintain a self-inspection program, which shall include the periodic review and assessment of USDA's classified products;

(3) establish procedures to prevent unnecessary access to classified information, including procedures that:

(a) require a justification for access to classified information before initiating security clearance procedures; and

(b) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

(4) develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(5) through the ASA and the Director, Office of Human Capital Management, ensure that applicable employee performance standards include language requiring the proper protection of classified information for all employees who routinely handle such information. For example, standards may include the statement, "Maintains classified information in accordance with E.O. 12958, Classified National Security Information." At a minimum, positions requiring this standard are:

(a) original classification authorities;

(b) security specialists or ISCs; and

(c) all other personnel whose duties significantly involve the creation or handling of classified information.

(6) account for the costs associated with the implementation of E.O. 12958, which shall be reported annually to the Director of ISOO for publication;

(7) handle referrals for any request, appeal, challenge, complaint, or suggestion that pertains to classified information that originated in a

component of the Department that no longer exists, and for which there is no clear successor function;

(8) assist with the preparation of a security classification guide to facilitate the proper and uniform derivative classification and declassification of information (these guides shall conform to standards contained in directives issued under E.O. 12958);

(9) assist in establishing and conducting a program for systematic declassification reviews;

(10) ensure the safeguarding of foreign government information under standards that provide a degree of protection at least equivalent to that required by the providing government or international organization of governments that furnished the information;

(11) ensure that USDA does not disclose information originally classified by another agency without its authorization;

(12) establish classification and marking principles for USDA classified information.

e. The ISC is the liaison between the OSS PDSD and USDA mission areas, agencies, and offices on matters relating to this Manual. Each ISC should maintain a security clearance at the same level of classification as the material maintained by that agency or program or higher. Duties may include, but are not limited to:

(1) initiating a preliminary inquiry when there is suspicion of a possible compromise or loss of classified information;

(2) reporting security violations and infractions to the Chief, PDSD;

(3) assisting the PDSD Information Security Staff (ISS) in collecting information to meet requirements for annual reporting to ISOO;

(4) conducting inventories of security equipment and evaluating agency security needs;

(5) coordinating and/or conducting annual security refresher training;

(6) coordinating document reviews with the ISS for possible classification or declassification;

(7) reviewing, commenting on, and providing recommendations on draft policy documents; and

(8) ensuring that security container combination changes are completed as required.

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

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

(2) Coordinating with 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. System protection functions include communications security, encryption, network security products, and system reliability.

g. USDA employees holding security clearances are responsible for the following:

(1) familiarizing themselves with and adhering to the provisions of this Manual;

(2) protecting classified information from individuals who do not have a need-to-know, maintaining the proper security clearance, and having access to the proper security container to store classified information;

(3) meeting the accountability requirements identified within this Manual;

(4) participating in security awareness and education training; and

(5) reporting any irregularities and security violations/infractions immediately upon discovery to their respective security officer, Information Security Coordinator (ISC), or PDSD.

6. WAIVERS

Waivers to the requirements of this Manual may be approved only by the Chief, Information Security Staff, within the guidelines of E.O. 12958. Waivers may be approved for up to 3 years. Requests for a waiver must be submitted in writing to the Chief, PDSD, and include the following:

a. location for the waiver;

b. requirement(s) for which the waiver is requested;

c. detailed justification for why the requirement(s) cannot be met;

d. proposed compensatory measures;

e. duration of the waiver;

f. impact of denying the waiver request; and

g. point of contact, including the person's name, address, telephone number, and e-mail address.

CHAPTER 2

CLASSIFICATION

Classification is a process to determine if information can potentially cause damage to U.S. national security. Classification includes many formal steps for which the orginal classification authority (OCA) is trained. Sometimes unclassified information combined or associated with other unclassified information may warrant classification. This is referred to as classification by compilation or aggregation of information, and is often the larger picture that classifiers fail to see. When it appears that an office has such an aggregation of information, the Security Officer or information security coordinator (ISC) should be contacted for assistance. A cleared subject matter expert (SME) must review the material and make an initial classification determination. If an agency ISC is not available, PDSD should be contacted for assistance.

In some situations, an aggregation of classified information may warrant a higher classification than its component parts. For example, two elements of information classified as Confidential may warrant a Secret classification when aggregated. Below are the types of classification and what must be determined when classifying information:

1. ORIGINAL CLASSIFICATION

Original classification is the initial decision to designate a certain item of information as classified, at a certain level, and for a certain length of time. These decisions can be made only by persons designated in writing by the President of the United States. The Secretary of Agriculture has been designated as having OCA for up to "Secret" information. If desired, the Secretary can further delegate this authority, in writing, to the Deputy Secretary. As an example of original classification, USDA research may reveal that a specific pathogen creates a high risk to human and animal health when introduced to a food product at a specific stage in its development. The combination of information, such as a specific pathogen, food type, and most vulnerable food processing stage, could cause damage to our national security, and therefore the Secretary may originally classify that information.

a. Levels of Classification. There are three levels of classification.

(1) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe;

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the

national security that the original classification authority is able to identify or describe;

(3) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

b. Classification Categories. E.O. 12958 identifies information that qualifies for being potentially classified. The categories are as follows:

(1) military plans, weapons systems, or operations (1.4a);

(2) foreign government information (1.4b);

(3) intelligence activities (including special activities), intelligence sources or methods, or cryptology (1.4c);

(4) foreign relations or foreign activities of the United States, including confidential sources (1.4d);

(5) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism (1.4e);

(6) United States Government programs for safeguarding nuclear materials or facilities (1.4f);

(7) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism (1.4g); and

(8) weapons of mass destruction (1.4h).

c. Duration of Classification. The OCA is required to determine, at the time of original classification, when the information can be downgraded or declassified. Classification of USDA information cannot extend beyond 25 years. At the time of classification, the information must be evaluated to determine if there is a specific date or event such that once it occurs, the damage the information could cause would be significantly reduced. An example may be a vulnerability assessment of a facility that reveals significant issues which, if discovered by an adversary, could allow access to highly dangerous substances. The report could be classified until the vulnerability is mitigated. At the time of mitigation, the information would be declassified.

If a date or event cannot be determined, then the information is evaluated for a period of classification of up to 10 years. If 10 years may not protect the

information long enough, the OCA can assign a duration of classification of up to 25 years. Information can always be declassified sooner than originally determined. Conversely, if it is determined that a declassification date is upcoming and the information can still cause damage to national security, then the duration can be extended providing it does not exceed the 25- year limit. Requesting continued classification beyond the 25 years must be done by notifying the President through the Assistant to the President for National Security Affairs. This action is initiated through PDSD.

d. Interim Classification. When a USDA employee or government contractor who does not have OCA originates information believed to require classification, the information shall be protected as classified information and in a manner consistent with this Manual. The information should be marked "Secret—Currently Under Classification Review." The markings should be located at the top and bottom of each page and on each paragraph containing the potentially classified information. The document or information is forwarded to PDSD for further evaluation by SMEs and classification experts, who will provide recommendations to USDA OCA.

e. Classification Prohibitions and Limitations. Basic scientific research information that is not clearly related to the national security shall not be classified. In no instance shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;
(2) prevent embarrassment to a person, organization, or agency;
(3) restrain competition; or
(4) prevent or delay the release of information that does not require protection in the interest of the national security.

f. Classification Challenges. Authorized holders of USDA information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status. Under no circumstance will the individual challenging the classification be subject to retribution. USDA assures all individuals that this is an opportunity for a review by an impartial official or panel of SMEs. To the extent possible, this process will be accomplished within 30 calendar days of receipt of the challenge. To challenge a classification, authorized holders must:

(1) prepare written correspondence explaining all concerns relative to the challenge;
(2) identify the exact document or information in question;
(3) provide any backup information or material to support the challenge; and
(4) forward the package, in a manner required for classified information, to PDSD for evaluation.

2. DERIVATIVE CLASSIFICATION

Derivative classification consists of the incorporating, paraphrasing, restating, or generating of a new form of information that has already been determined to be classified and marking the new material consistent with the classification markings of the source information. This ensures that the new material is classified and handled at the level that the OCA has already determined. Anyone with the proper security clearance and authorized access to the information can derivatively classify information. Derivative classifiers are not required to be appointed or designated in writing. This is the most common means of classification.

3. CLASSIFIED FOREIGN GOVERNMENT INFORMATION (FGI)

The following are the requirements of the United States for protecting FGI:

a. Top Secret. Records shall be maintained to include the receipt of the information, internal distribution, destruction, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction will be witnessed.

b. Secret. Records shall be maintained to include the receipt of the information, external dispatch, and destruction of foreign government Secret information. Other records may be necessary if required by the originator. Secret foreign government information may be reproduced to meet mission requirements unless prohibited by the originator. Reproduction shall be recorded unless this requirement is waived by the originator.

c. Confidential. Records need not be maintained for foreign government Confidential information unless required by the originator.

d. Restricted and Other FGI Provided in Confidence. In order to ensure the protection of FGI provided in confidence, such information must be classified under E.O. 12958. If USDA is the receiving agency, then USDA is responsible for providing a degree of protection to the FGI at least equivalent to that required by the government or international organization that provided the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information. If the foreign protection requirement is lower than the protection required for U.S. Confidential, the following requirements shall be met:

(1) Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents shall be

marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).” The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for FGI. If remarking foreign-originated documents or materials is impractical, an approved, classified document cover sheet is an authorized option.

(2) Documents shall be provided only to those individuals who have the required security clearance and an established need-to-know to perform their official duties.

(3) Individuals with access to FGI shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instruction, or by applying specific handling requirements to an approved classified document cover sheet.

(4) Documents shall be stored in such a manner as to prevent unauthorized access.

(5) Documents shall be transmitted in a method approved for classified information unless this method is waived by the originating government.

(6) Declassifying FGI is consistent with U.S. classified information. It must be declassified within 25 years unless exempted. The holder of the information can mark the document as unclassified.

e. Third-country transfers. The release or disclosure of FGI to any third-country entity must have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligations.

The requirements in this section do not apply to North Atlantic Treaty Organization (NATO) information. NATO classified information is safeguarded in accordance with NATO Instruction 1-69. Appendix D, Equivalent Foreign Security Classification, is offered as a translation of foreign countries’ classification markings.

4. NON-USDA AGENCY CLASSIFIED INFORMATION

The Department is required to respect each non-USDA OCA’s decisions, including the level and duration of classification. Under no circumstance should a USDA employee or contractor remove the classification markings without the originating agency’s approval.

CHAPTER 3

DECLASSIFICATION AND REGRADING

The process of declassification must be performed by SMEs and classification specialists. When a decision is made to classify information, the decision of when to declassify the information must be made simultaneously. It is possible that a Freedom of Information Act request may include classified information, or that classified information is discovered published in a journal. Events such as these would require USDA to conduct an unscheduled review of the information to see if it can or should be declassified or regraded. This type of mandatory review, as well as other types of reviews, is explained in this section.

1. DECLASSIFICATION

Information should be declassified when it no longer meets the standards and criteria for classification. The authority to declassify information resides with the OCA and those individuals appointed as declassification authorities. Declassification is subject to the criteria specified in E.O. 12958 and/or successor orders and directives. USDA files and records, potentially eligible for declassification, must be reviewed to determine if continued classification is warranted and authorized. E.O. 12958 contains provisions for four declassification programs, as follows:

a. OCA action: The OCA can decide to declassify information at any time.

b. Automatic: When the document is marked to be declassified on a specific date and the date has arrived, the holder can then declassify the document.

c. Mandatory: When information has been compromised or requested by an uncleared person to be released, security experts, subject matter experts, the Office of the General Counsel (OGC), and PDSD must review the information to determine if it can be declassified. See Appendix C for the Mandatory Declassification Review Process.

d. Systematic: Prior to declassification, originally classified information under E.O. 12958, or its predecessor, shall be reviewed.

2. REGRADING

a. Downgrading. When information no longer requires protection at the current classification level, the information can be downgraded. For example,

information classified as "Secret" may be downgraded to "Confidential" after an event occurs. The OCA should consider identifying downgrading instructions at the time of original classification. If downgrading instructions can be determined at the time classification is determined, they are noted in the declassification section of the OCA's security classification decision. Downgrading information at a later date is permissible, but all holders of the information must be first notified to ensure uniform protection of the information.

b. Upgrading. Classified information can be upgraded to a higher level of classification. However, this is done in rare circumstances when an OCA has the determined the information requires a higher level of protection. When this is done, OCAs are required to notify holders of the information of the change so that the information will be uniformly protected at the higher level. The Secretary of Agriculture can upgrade from Confidential to Secret. Upgrading to Top Secret can be accomplished by other OCAs who have a shared interest with USDA and have Top Secret OCA, such as the Secretary, Department of Homeland Security.

c. Reclassifying. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified. Such information, for example, may be identified while evaluating material requested through the Freedom of Information Act or the Privacy Act of 1974 or in response to the mandatory review provisions of this Manual. Reclassification can occur only if the:

(1) information meets the classification requirements outlined in E.O. 12958;

(2) reclassification is completed on a document-by-document basis with the personal participation or under the direction of the Secretary or the Deputy Secretary, ASA or Deputy ASA should the Secretary further delegate his or her OCA;

(3) information may be reasonably recovered; and

(4) reclassification action is reported to ISOO through PDSD.

CHAPTER 4

MARKING

1. GENERAL

A uniform security classification system requires that standard markings be applied to classified information. The marking of classified information created by USDA employees and its contractors shall not deviate from the following prescribed formats, unless under extraordinary circumstances and with the approval of the PDSD. If markings cannot be affixed to specific classified information or materials, the originator shall provide written instructions for protecting the information to individuals and offices holding the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

2. ORIGINAL CLASSIFICATION MARKING

The following markings shall be applied on the face of each originally classified document, or media containing the information, for the OCA's review and approval:

a. Classification Authority. The name or personal identifier and position title of the OCA shall appear on the "Classified By" line. An example might appear as:

Classified By: *"Secretary's Name"*
Secretary of Agriculture

b. Agency and Office of Origin. If not otherwise evident, the agency and office of origin shall be identified. The name or personal identifier shall appear on the "Classified By" line. An example might appear as:

Classified By: "Secretary's Name"
Secretary of Agriculture

c. Reason for Classification. The OCA shall approve the reason(s) for the decision to classify. The OCA shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.4 plus the letter(s) that corresponds to that classification category shown in Chapter 2, paragraph 1(b). The SME shall provide the OCA the reason that the information should be classified when submitting it for classification approval. Once approved by the OCA, the originally classified document must reflect the reason for classification. An example might appear as:

Classified By: "Secretary's Name"
Secretary of Agriculture
Reason: *1.4(g)*

When the reason for classification is not apparent (e.g., classification by compilation), then the OCA must provide a more detailed explanation for the reason for classification.

d. Declassification Instructions. The duration of the original classification decision shall be placed on the "Declassify On" line. The SME should recommend to the OCA one of the following instructions for approval and application:

(1) A specific date or event for declassification that would require releasing the information to individuals who do not hold a security clearance or a date or event after which releasing the information would no longer cause damage to the national security. The date should be less than 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as follows:

Classified By: "Secretary's Name"
Secretary of Agriculture
Reason: 1.4(g)
Declassify On: *October 14, 2007 (date)*

or

Declassify On: *Upon completion of the 2007 Food Seminar (event)*

(2) When a specific date or event within 10 years cannot be established, then apply the date that is within 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 2003, mark the "Declassify On" line as follows:

Classified By: "Secretary's Name"
Secretary of Agriculture
Reason: 1.4(g)
Declassify On: *October 14, 2013 (10-year date)*

(3) Upon determination that the information must remain classified beyond 10 years, the SMEs must inform the OCA how long they believe the information needs to be classified. The date cannot exceed 25 years from the date of the original classification decision. For example, on a document that contains information classified on October 10, 2003, mark the "Declassify On" line as follows:

Classified By: "Secretary's Name"
Secretary of Agriculture
Reason: 1.4(g)
Declassify On: October 10, 2028 (25- year date)

3. DERIVATIVE CLASSIFICATION MARKING

USDA will primarily use derivative classification markings. This is accomplished when someone is creating a document using classified source documents, a security classification guide, or guidance. In other words, either the Secretary of Agriculture has already determined the information is classified, or the information has been classified by another entity. The derivative classifier is responsible for carrying forward the classification and declassification instructions from the source document(s) to the new document. Derivative classification is completed as follows:

a. Identify Source Document. The derivative classifier shall concisely identify the source document or the classification guide on the "Derived From" line and shall include the agency and, when available, the office of origin and the date of the source or guide. For example:

Derived From: USDA Security Classification Guide (SCG)
Dated January 3, 2007
Declassify On: January 3, 2017

or

Derived From: Food Safety and Inspection Service (FSIS) Food Products Security Report
Dated June 15, 2003
Declassify On: June 15, 2013

b. Multiple Sources. When the document is classified derivatively on the basis of more than one source document or classification guide, the "Derived From" line shall appear as Derived From: Multiple Sources.

c. File Copy of Sources. The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. This list should be included in or with all copies of the derivatively classified document.

d. Reason for Classifying. A derivative classifier is not required to identify a reason for classifying the information because the source documents already identify the reason the information was classified.

e. Declassification Instructions. The derivative classifier shall carry forward the instructions on the "Declassify On" line from the source document to the derivative document or the duration instruction from the classification or declassification guide.

f. Multiple Declassification Instructions. When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources. Since using multiple declassification instructions is complex, PDSD should be contacted for assistance. As an example:

Derived From: Multiple Sources
Declassify on: Dec 15, 2012 (reflects the latest date from the sources)

4. OVERALL DOCUMENT AND NON-DOCUMENT MARKING

a. Document Marking. The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the information text.

(1) Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked "Secret," and other information marked "Confidential," the overall marking would be "Secret."

(3) Each interior page of a classified document can be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified," when it is applicable, or with the highest overall classification of the document.

(4) Portion Marking. Each paragraph, subject, title, graphic, and the like shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding the portion to which it applies. Titles will, however, always be marked at the end. Markings will be reflected (TS) for Top Secret, (S) for Secret, and (C) for Confidential.

b. Non-Document Markings. The appropriate classification markings and declassification instructions assigned by the OCA will be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal,

or similar device on classified material other than documents and on its container, if possible. There should be no question in the mind of the audience, consumer, or user of the level of classification of a given presentation or material. The following are procedures for various types of materials:

(1) Charts, Maps, and Drawings. Each item will bear the appropriate classification marking and declassification instructions under the legend, title block, or scale to differentiate between the classification assigned and the legend or title itself. The higher of those markings shall be annotated at the top and bottom of each document. When the customary method of folding or rolling charts, maps, or drawings would cover the classification markings, additional classification markings will be placed so they are clearly visible when the document is folded or rolled.

(2) Photographs, Negatives, and Prints. These items are marked with the appropriate classification markings and declassification instructions, which should be reflected in a conspicuous location. Roll negatives are marked at the beginning and end of each strip. Single unframed negatives are marked directly with their appropriate classification. All component parts of self-processing film are removed and destroyed as classified waste. Photographs are marked with the appropriate classification at the top and bottom on the front and reverse sides, with the downgrading and declassification instructions at the bottom. The classification marking needs to be applied only once on the front and back on smaller prints and may be affixed by a pressure tape label or stapled strip if a stamp cannot be used. All photographic reproductions must have declassification instructions and classification markings.

(3) PowerPoint Presentations. Classified PowerPoint presentations must be processed on an accredited classified system and marked with the highest classification for each slide. The introductory slide must reflect the highest level of the presentation and the declassification instructions.

(4) Classified Video Recordings. All recordings shall be marked at the beginning and end of the production by the title, bearing the appropriate classification, or spelled out on a separate frame preceding the title frame and following the last frame of the video. Such markings must be visible when the production is played back on a personal computer (PC) monitor or television screen. Cassettes, DVDs, and their containers are to be marked with the appropriate classification markings and declassification and handling instructions. Note that edited waste material should be destroyed in accordance with National Security Agency (NSA) approved means for destroying classified waste, as specified in Chapter 7.

(5) Sound Recordings. Place a classification statement at the beginning and end a sound recording to ensure that the listener knows that classified

information of a specified level is involved. Recordings are to be kept in marked containers or cases that bear the appropriation classification markings and declassification and handling instructions.

(6) External Removable Data Storage. Removable information storage media and devices shall bear sufficient external markings to ensure that any recipient of the media knows the information contained therein involves a specific classification category. Examples include floppy disks, zip disks, CD and DVD disks, memory cards (such as Compact Flash or SmartMedia), PCMCIA "PC Card" memory cards, memory sticks, USB drives, and other memory products. Each media containing classified information will have a label or marking affixed stating the highest classification of the material on the media. Pre-made labels are available through Government supply (e.g., Standard Forms [SF] 706 "TOP SECRET," SF 707 "SECRET," SF 708 "CONFIDENTIAL," SF 709 "CLASSIFIED," and SF 710 "UNCLASSIFIED").

(7) Material for Training Purposes. Training documents created to look like classified documents will be marked in large letters at the top and bottom, "(Classification level)—For Training Purposes Only." Documents that contain classified material used for training purposes will be marked, transmitted, stored, and safeguarded as prescribed in this Manual.

5. FILES OR FOLDERS CONTAINING CLASSIFIED DOCUMENTS

Files or folders of documents, when not in secure storage, will be marked conspicuously to ensure protection commensurate with the highest overall classification included therein. The top and bottom of the folder or file and on the front and back sides shall be marked. Cover sheets identifying the level of classified material in the file or folder can be used.

6. MARKING CLASSIFIED WORKING PAPERS.

Working papers are defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest level of classified information contained in them, and protected at that level, and if otherwise appropriate, destroyed when no longer needed. When any of the following conditions apply, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

a. released by the originator to someone outside of USDA;

b. retained more than 180 calendar days from the date of origin; or

c. filed permanently.

7. MARKING ELECTRONICALLY TRANSMITTED MESSAGES

Electronically classified messages can only be sent using secure communications. They must be marked at the top and bottom with the assigned classification and portion markings prescribed in Chapter 4. In the case of a message printed from an automated system, these classification markings should be applied by that system, provided the markings are made clearly distinguishable from the printed text. The first item of information in the text of a classified message is the overall classification of the message. The originator of classified messages is considered the accountable classifier, and no "CLASSIFIED BY" line is necessary. The originator is responsible for maintaining adequate records to show the source of derivative classifications assigned. This means identifying in writing the information on which the originator is basing the classification. The last line or paragraph of a classified message will show the appropriate abbreviated marking for declassification (DECL) or downgrade (DG), plus the event or date for declassification/downgrading. Messages containing Restricted Data (RD) or Formerly Restricted Data (FRD) do not require downgrading or declassification instructions. However, the originator's copy must indicate a "CLASSIFIED BY" line.

8. MARKING FOREIGN GOVERNMENT INFORMATION (FGI)

a. Documents received and held containing FGI must be marked in a manner that ensures that FGI is not declassified prematurely or made accessible to foreign nationals of a third country without the consent of the originator and that it is protected in accordance with country agreements. Documents classified by a foreign government or an international organization of governments will, if the foreign classification is not in English, be marked with its equivalent U.S. classification. (See Appendix D, Equivalent Foreign Security Classification.)

b. FGI used in creating U.S. documents containing FGI is marked as follows:

(1) Classified by: (Insert identity of source foreign document, memorandum of understanding, or Security Classification Guide) (SCG);

(2) Declassify on: (Insert the specific date of declassification, or event).

(3) Documents containing FGI must include the marking "FOREIGN GOVERNMENT INFORMATION" on the document. If the fact that the

document contains FGI must be concealed, this marking shall not be used, and the document will be marked as if it were wholly of U.S. origin.

9. WARNING NOTICES OR SPECIAL HANDLING INSTRUCTIONS

In addition to classification markings, warning notices offer additional special handling requirements. These warning notices or special handling instructions will be prominently displayed on classified documents or materials as appropriate. Documents carry warning notices on the outside of the front cover or on the front page, if there is no front cover. Portions, paragraphs, or subparagraph classification markings are marked with additional warning notices as required. When these warnings are within a classified document, it would look something like (TS/NOFORN/NOCONTRACT), which means that the paragraph or document is at the Top Secret level, and no foreigners or contractors can have access to the information. Some commonly used acronyms include:

a. Foreign Dissemination (NOFORN). NOFORN restricts U.S. classified intelligence information to U.S. citizens only with the proper security clearance and need-to-know. Portions and paragraphs will be marked with NOFORN following the level of classification (e.g., C/NOFORN).

b. Restricted Data (RD). Portions and paragraphs containing RD information are marked with RD following the level of classification (e.g., S/RD). Documents containing RD information will be marked on the first page or cover page as follows:

RESTRICTED DATA

"This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions."

c. Formerly Restricted Data (FRD). Portions and paragraphs are marked with FRD following the level of classification (e.g., TS/FRD). Material containing FRD information will be marked on the first page or cover as follows:

FORMERLY RESTRICTED DATA

"Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination, in accordance with Section 144.b, Atomic Energy Act, 1954."

d. Critical Nuclear Weapon Design Information (CNWDI). CNWDI is TOP SECRET or SECRET RD information which is controlled by the Department of Defense. This information is comprised of specific nuclear weapon capabilities.

Portions and paragraphs are marked with an N or CNWDI following the level of classification (e.g., TS/N or TS/CNWDI). This information within USDA is controlled and safeguarded as RD information.

e. Dissemination and Extraction of Information Controlled By Originator (ORCON). This marking may be used only on intelligence information that identifies a source or method that is susceptible to countermeasures that would nullify its effectiveness. Portions and paragraphs are marked with ORCON following the level of classification (e.g., S/ORCON).

f. Not Releasable to Contractors or Consultants (NOCONTRACT). NOCONTRACT is used to prohibit dissemination of information to contractors and consultants without the permission of the originator. This marking may be used only on classified information which, if disclosed to a contractor or consultant, would (a) actually or potentially give a company a competitive advantage that could reasonably be expected to cause a conflict of interest with its obligation to maintain the security of the information, or (b) was provided by a source with the express or implied condition that it not be made available to contractors. Portions and paragraphs are marked with NOCONTRACT following the level of classification (e.g., S/NOCONTRACT).

g. Communications Security (COMSEC). This refers to measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emissions security, and physical security of COMSEC material.

h. North Atlantic Treaty Organization (NATO).

(1) Access to NATO information is restricted to personnel given NATO access after receiving a NATO briefing and signing a non-disclosure statement for NATO information. NATO information must be appropriately safeguarded and segregated from U.S. information. Internationally accepted markings for NATO classified information and their U.S. equivalent are listed below:

(a) NATO ATOMAL: For nuclear information, it is equal to U.S. Restricted Data;

(b) COSMIC TOP SECRET: Equal to U.S. TOP SECRET;

(c) NATO SECRET: Equal to U.S. SECRET;

(d) NATO CONFIDENTIAL: Equal to U.S. CONFIDENTIAL;

(e) NATO RESTRICTED: Equal to U.S. For Official Use Only.

(2) Portions and paragraphs containing NATO classified information will be marked with its NATO designation as found in U.S. Security Authority for NATO (USSAN) 1-69:

(a) NATO RESTRICTED information (NR);

(b) NATO CONFIDENTIAL information (NC);

(c) NATO SECRET information (NS);

(d) COSMIC TOP SECRET information (CTS);

(e) NATO CONFIDENTIAL ATOMAL information (NCA);

(f) NATO SECRET ATOMAL information (NSA); and

(g) COSMIC TOP SECRET ATOMAL information (CTSA).

(3) Users of NATO information must ensure that the top and bottom of the pages or documents are marked with the highest level of classification contained therein. Should NATO COSMIC TOP SECRET information be used in a U.S. SECRET document, that document will be marked as NATO COSMIC TOP SECRET and protected as U.S. TOP SECRET information.

i. Special Access Program (SAP). This category of information is usually created and classified by Department of Defense and Intelligence agencies. Access is minimized, and in order to receive access, individuals must receive a special program briefing and sign a non-disclosure agreement. SAP information will have a codename that is placed on the top and bottom of each page following the classification. A codeword will have two words put together that normally would not go together, such as “Santa Bunny” or “Basket Talent.” Individuals who open a package and see what appears to be a codename without having received a briefing on that program should contact their local security office or PDSD immediately for proper handling instructions. USDA is not authorized to create SAPs.

j. Sensitive Compartmented Information (SCI). SCI is intelligence information that involves sources and methods used in its collection. Access is minimized. To receive access, individuals must receive approval by the Central Intelligence Agency (CIA), receive a special briefing, and sign an SCI non-disclosure agreement. Documents will bear the SCI marking along with its classification, and such documents require special storage in an SCI Facility (SCIF). Persons

in receipt of SCI documents should contact their local security office or PDSD immediately for proper handling instructions.

CHAPTER 5

SAFEGUARDING

Classified information will be stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements. Overseas storage standards for facilities under a Chief of Mission are promulgated under the authority of the Overseas Security Policy Board. The following are policies and procedures for storing and safeguarding national security information. Classified information or materials may be used, held, or stored, only where the facilities or conditions are adequate to prevent unauthorized access.

1. STORAGE OF CLASSIFIED MATERIAL

Whenever classified material is not under the personal control and direct observation of an authorized person, it must be stored in an approved area or container. The physical construction standards required for a secure room or vault must meet specific requirements (see Appendix E, Physical Security Standards). The minimum requirements for storage of classified information are as follows:

a. TOP SECRET Information. There are three alternative requirements for storage of TOP SECRET information that allow USDA agencies and offices to meet the minimum safeguards.

(1) TOP SECRET material will be stored in a General Services Administration (GSA)-approved security container with one or more of the following supplemental controls in place:

(a) Continuous protection by cleared guard(s) or duty personnel;

(b) Inspection of the security container every 2 hours by cleared guard(s) or duty personnel;

(c) An Intrusion Detection System (IDS) with personnel responding to the alarm within 15 minutes of the alarm annunciation; or

(d) Pre-approved Security-in-Depth (pre-approval is gained through PDSD).

(2) TOP SECRET information can be stored in a “secure room” approved for “open storage” (see Appendix E). The room must meet specific construction standards, be equipped with an approved IDS, have a 15-

minute response to the alarm, and must have Security-in-Depth. The room must be approved by PDSD.

b. SECRET Information. SECRET information may be stored in the same manner as that authorized for TOP SECRET or in a GSA-approved security container without supplemental controls.

c. CONFIDENTIAL Information. CONFIDENTIAL information may be stored in the same manner as that authorized for TOP SECRET or SECRET information. Confidential material may not be stored in a lockbar file cabinet.

2. REQUESTING ACCREDITATION OF A SECURE ROOM

a. Definition and Approval. A secure room is a room and/or area built for the purpose of protecting collateral classified national security information. Secure rooms are used for open storage of collateral classified information, processing classified information, and holding classified meetings and conferences. Collateral means information classified as Top Secret, Secret, or Confidential and does not include SCI, RD, or FRD. This applies to all USDA facilities and to contracted or leased facilities. All secure rooms will be inspected and accredited by a representative of PDSD in close coordination with the USDA COMSEC Custodian, OCIO, and Departmental Physical Security. Any waivers or approvals of deviations from the construction requirements contained in Appendix E will be issued on a case-by-case basis by PDSD.

b. Open Storage. A Classified National Security Information (NSI) Open Storage Area should be considered when the volume or bulk of classified information or the functions associated with the processing of classified information are such that the use of GSA-approved security containers for the storage of classified information is not practical. In other words, if a computer used for processing classified reports does not have a removable hard drive and the computer cannot be moved into a vault or security container, the equipment would be considered classified and must be stored in an "open" environment. This requires the room to be approved for "open storage of classified information." "Open storage" physical security requirements differ with the levels of classified information being stored within the room. (See Appendix E for requirements.)

c. Approval Process. If an agency determines that an "open storage" room is necessary, it must:

(1) Prepare a written request identifying the reason for the "open storage" area, the location, the level to be stored or processed, a brief description of the program requirements, and a point of contact for the request. This should be submitted through a local security office or agency ISC to PDSD, which is the approving authority for USDA open storage areas.

(2) The following information must be attached to the request for accreditation:

(a) Alarm Certifications (UL 2050)

(b) Proposed standard operating procedures

(c) Room construction specifics (e.g., electrical work, plumbing, and construction materials)

d. Standard Operating Procedures. Standard operating procedures (SOP) provide guidance on the security measures that will be implemented and adhered to for the operation and maintenance of USDA- designated NSI Open Storage Areas. The SOP should include:

(1) the requirement that all persons authorized for unescorted access to the designated area will read and be familiar with the requirements of the SOP;

(2) escorting procedures for visitors and uncleared individuals;

(3) the disarming and rearming of the IDS;

(4) the name and contact information of the local security official or point of contact who should be contacted prior to any room modifications, security devices being introduced, and in the event of a security incident;

(5) procedures for entering and leaving the room for initial entry, daily use, and close of business;

(6) the use of the SF-702, Security Container Check Sheet; and

(7) anything else that applies to local and office procedures.

e. Accreditation Award. Accreditation will be awarded by a memorandum citing the specific location; building; room number; level of classified information authorized for open storage; restrictions, if any; and any other information deemed appropriate. Room accreditations will be valid for 3 years from the date of the approval memorandum. The office responsible for the room must report any construction- or classification-level changes involving the room.

f. COMSEC and SCIF Requirements. When processing classified information on computers, COMSEC requirements must be met. Appendix E does not contain COMSEC requirements for rooms that will be processing classified information. Those requirements must be obtained through the COMSEC

custodian. Requirements for SCIFs are defined and approved by the CIA. Director of Central Intelligence Directive (DCID) 6/9 defines the physical security requirements to request SCIF accreditation. SCIF accreditation must be coordinated with the PDSD.

3. SECURITY CONTAINERS

All security containers must be GSA approved. A label on the front of the container will reflect that it is a GSA-approved security container. Contact a local security office or PDSD to determine if a container is GSA approved.

a. Repairs. Repairs may be required if the security container cannot be opened or will not shut properly. Contact a local security officer or PDSD for assistance. Security containers can only be repaired by a trained and certified locksmith. Locksmiths do not have to maintain a security clearance. While repairing the container, however, they must be under constant surveillance, and all classified information should be removed from the drawer with the broken lock. When waiting for a repair to a security container that will not shut properly and has classified information within it, the security container must be under constant surveillance by an individual cleared for the information held within the security container. Alternatively, all information may be removed and stored in a container or vault approved for that same level of information. Classified information cannot be left unattended at any time. Contact a local security official if immediate assistance is needed.

b. Combination Changes. Combinations to security containers, secure rooms, or vaults must be changed when one of the following events occurs:

(1) when placed in use after procurement or moved to a new area of responsibility;

(2) when an individual knowing the combination is transferred, discharged, or reassigned from the organizational element to which the security container is assigned and the individual could gain access to that container, or the individual knowing the combination has a security clearance that is downgraded, suspended, or revoked;

(3) when the combination or record of combination is suspected of possible compromise;

(4) every 3 years, unless more frequent change is dictated by the type of material stored therein (e.g., NATO and COMSEC material is changed every 6 months); or

(5) when a container is taken out of service. The combination will be reset to the factory standard of 50-25-50.

c. Recording and Storing Combinations. A record must be maintained using an SF 700, Security Container Information, for each vault, storage area, or container used for storing classified material. The SF 700 is then stored in another security container approved for storage with an equal or higher classification level. Place a piece of tape over the sealed back of the SF 700, and sign across the tape prior to storing it in another security container. That provides proof that the combination has not been tampered with prior to a new person's requiring the combination. Instructions for using an SF 700 are as follows:

(1) Part 1 must be completed in its entirety and attached to the inside of the control drawer, vault door, or storage area door. If a security container is equipped with separate locking mechanisms for individual drawers, each drawer is considered a separate container, and a separate SF 700 should be affixed inside of each drawer. Part 1 includes a list of persons to be notified in the event the container, vault, or area is found open and unattended. Although disclosure of the personal information requested on the form is voluntary, employees who refuse to provide the information requested can neither be designated as custodians for the stored material nor given combinations to security containers.

(2) Parts 2 and 2a of the SF 700 should be stamped with the highest classification of material stored in the container, vault, or area. Part 2a should be sealed inside of Part 2 and stored in an alternate location.

d. Protection of Combinations. The combination of a vault or container used for the storage of classified material will be classified at the same level as the highest category of classified material authorized to be stored therein. Therefore, it is imperative to remember:

(1) annotating security container combinations on notepads, calendars, slips of paper in wallets or purses, etc., is PROHIBITED; and

(2) knowledge of, or access to, the combination for a classified storage container, vault, or room will only be given to individuals who have been granted security clearances commensurate with the classification level of the material and who have a need-to-know the information stored. Individuals will not be given access by virtue of grade, rank, or position.

e. Opening and Closing Security Containers. An SF 702, Security Container Check Sheet, must be affixed to the outside of each security container, vault, or area utilized for the storage of classified information. If a security container is equipped with separate locking mechanisms for individual drawers, each drawer is considered a separate container and a separate SF 702 is affixed for each drawer. This form is used to reflect daily entry and locking of each container.

The form is essential to conducting preliminary inquiries into potentially lost or stolen classified information or evidence of tampering. Once the SF 702 is completed, it must be retained for a period of no longer than 90 calendar days. The following procedures are used when opening and closing security containers:

(1) Each time a security container is unlocked, the individual opening the container annotates the date and time opened and initials the OPENED BY column of the SF 702.

(2) At the end of the workday or anytime the office is left unattended, containers are locked. The individual locking the container annotates the time closed and in the CLOSED BY column of the SF 702. All drawers and latches are physically checked to ensure that they are locked.

(3) When possible, at the end of each workday, an individual other than the one who locked the container will double check to ensure that the container is locked. This individual does not have to possess a security clearance. However, the appropriately cleared person who locked the safe should be in attendance. Spinning the combination lock several times and pulling on the draw handle will help ensure that the container is locked. The double-check consists of turning the dial at least four times in the same direction and physically checking each drawer and latch. The individual accomplishing the double-check annotates the date, time and initials the CHECKED BY column of the SF 702.

(4) Containers that are used infrequently should be checked daily to ensure they are properly secured and to ensure the integrity of the containers. This includes the containers of individuals on travel or a leave of absence. The individual accomplishing the check annotates the date, draws a line through the OPENED BY and CLOSED BY columns and intials and annotates the time in the CHECKED column of the SF 702.

4. INTELLECTUAL PROPERTY

Once individuals are granted their security clearances and sign nondisclosure agreements (SF 312), they have made a lifelong agreement that they will protect classified information from unauthorized disclosure. Classified information retained within an individual's memory may be considered "Intellectual Property" and also requires protection from individuals who do not have a proper U.S. Government security clearance and a need-to-know. As an example, if a person retires after working on a classified project, he or she cannot share that information with anyone just because he or she is now retired. The information must still be protected from disclosure (i.e., not discussed or written).

5. NATO INFORMATION

The receipt, shipment, and storage of unclassified and classified NATO information is mandated by the U.S. Security Authority for NATO (USSAN) Instruction I-69 and I-70. The USDA NATO Control Office is PDSD. If assistance is required for storage of NATO material, contact PDSD.

CHAPTER 6

DISTRIBUTION OF CLASSIFIED INFORMATION

Classified information shall be transmitted and received in an authorized manner that ensures that evidence of tampering can be detected and that inadvertent access can be precluded. It must also involve a method that assures timely delivery to the intended recipient. Classified information shall be covered by the cover sheets SF 703 (TS), SF 704 (S), or SF 705 (C). Persons transmitting classified information are responsible for ensuring that intended recipients have a security clearance at the appropriate level, an official need-to-know, and the capability to store classified information in accordance with this policy. This section provides USDA's policy on approved methods of distributing classified information to authorized persons and organizations.

1. PREPARING CLASSIFIED INFORMATION/MATERIAL FOR DISTRIBUTION

a. Classified Information Removed from a USDA Facility.

(1) All classified information physically transported outside the facility shall be enclosed in two layers, both of which can provide reasonable evidence of tampering and which conceal the contents. If hand delivering, the outer wrapping can be an envelope, a locked briefcase, or courier bag.

(a) The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices.

(b) The outer enclosure shall be the same except that no markings to indicate that the contents are classified shall be visible and the intended recipients shall be identified by name only as part of the attention line.

(2) Exceptions to packaging involve bulky items or inaccessible classified information such as an internal component. Contact the local security office or PDSD for additional guidance.

b. Document Accountability. Top Secret and Secret classified material/ information must reflect a trail of accountability when leaving the organization. Information originating outside USDA may not be disseminated outside USDA without the consent of the originator. When classified material is being hand carried or mailed outside USDA buildings, an appropriate classified information cover sheet and an AD 471, Classified Document Accountability Record, must accompany the document for the recipient's signature. The procedures for completing an AD 471 are described below.

(1) Ensure that the recipient has the proper security clearance, an official need-to-know, and storage capability for the level of classified information distributed.

(2) Complete the form (typed, or clearly printed). Some titles of documents are classified. In those instances, give the document a number rather than using the title. If a classified title is listed on the form, the AD 471 is classified at the same level as the title.

(3) Once all the documents are listed, space down two lines and put the following label across the bottom of the list:

" ----------NOTHING FOLLOWS ----------."

This is a security measure indicating that nothing has been added or deleted so the recipient knows that he or she has the entire package.

(4) The AD 471 has colored carbon copies. The yellow and pink copies must go with the package. The sender shall retain the remaining copies in his or her office. The receiver is expected to sign for receipt on the yellow copy and return it to the sender, which at that time is matched with the sender's office copy. The receiver keeps the second copy for his or her records.

(5) When using overnight or registered mail, annotate the registration number on the white office copy for tracking purposes.

2. MAILING SERVICES WITHIN AND BETWEEN THE UNITED.STATES, PUERTO RICO, OR A U.S. POSSESSION OR TRUST TERRITORY

Authorized means to mail classified information to a street address are outlined below.

a. TOP SECRET information/material shall be distributed by:

(1) direct contact between authorized persons. This applies to individuals who have been given a courier letter and authorization to physically transport information outside USDA facilities and who understand their responsibilities as a courier of Top Secret information/material;

(2) using the Defense Courier Service or an authorized government agency courier service; or

(3) electronic means over approved, classified communications systems.

b. SECRET information/material shall not be left in a street-side mail collection box or sent to a Post Office Box. It can be distributed by:

(1) any method established for Top Secret information;

(2) U.S. Postal Service Express Mail;

(3) U.S. Postal Service Registered Mail, as long as the Waiver of Signature and Indemnity block, item 11-B on the U.S. Postal Service Express Mail Label, shall not be completed (it cannot be sent to a Post Office Box);

(4) cleared commercial carriers or cleared messenger services; or

(5) commercial express mail, which can be used when an urgent requirement exists. A GSA-contracted carrier for Secret information can be used. When using this option, the package may be addressed to the recipient by name. The release signature block on the receipt label shall not be executed under any circumstances. Communications Security (COMSEC), NATO, or foreign government information (FGI) information cannot be sent by this means.

c. CONFIDENTIAL information/material shall be distributed by:

(1) any method established for Top Secret or Secret information;

(2) U.S. Postal Certified Mail; or

(3) U.S. First Class Mail—if going to a U.S. government facility, not a contractor or overseas location. The outer envelope of the package must have the stamp "DO NOT FORWARD, RETURN TO SENDER."

3. TRANSMISSION METHODS FOR CLASSIFIED INFORMATION TO A U.S. GOVERNMENT FACILITY LOCATED OUTSIDE THE UNITED STATES

"Outside the United States" is defined as outside the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. Possession or Trust territory. Transmission methods are as follows:

a. Top Secret information can be sent using the Department of State Diplomatic Courier Service; and

b. Secret and Confidential information can be sent using U.S. Registered Mail through Military Postal Service facilities, provided that the information does not at any time pass out of U.S. citizen control or pass through a foreign postal

system. The Army Post Office (APO) and Fleet Post Office (FPO) are examples of a Military Postal Service.

4. RELEASING USDA CLASSIFIED INFORMATION TO FOREIGN ENTITIES

USDA classified information can only be released to a foreign government pursuant to an existing treaty, agreement, bilateral exchange, or other obligation. When classified information is transferred to a foreign government or its representative, a signed AD 471 is required. Any proposed release of classified information to a foreign government or individual is handled through the PDSD and USDA Foreign Agricultural Service (FAS), which will coordinate with the Department of State and/or the appropriate U.S. Embassy. Such releases should be kept to a minimum and accomplished only when it can be determined that the release is in the best interest of the U.S. Government. The requests for release and the information proposed for release must be forwarded to PDSD with a justification requesting release approval. Requests originating within the FAS still require coordination with PDSD.

5. ELECTRONIC TRANSMISSION OF CLASSIFIED INFORMATION

Classified information electronically accessed, processed, stored, or transmitted must be protected in accordance with applicable national policy issuances identified in the Index of National Security Telecommunications and Information Systems Security Issuances. SCI requirements are prescribed in the Director of Central Intelligence Directive (DCID) 6/3. COMSEC Custodian and the OCIO are responsible for ensuring that those requirements are met. At a minimum, the following guidelines apply:

a. Voice. Secure voice communications must be made using a Type 1 secure device. One such device is the Secure Terminal Equipment (STE) telephone. It is the user's responsibility to ensure that there are no uncleared individuals or others who do not have a need-to-know who can inadvertently hear the classified conversation. A "KOV-14" card is part of the STE equipment needed to make classified telephone calls. The KOV-14 card is also referred to as a "key" and is unclassified. However, when in the STE phone, the combination of STE phone and key is classified at the level approved for discussion. When the key is removed from the phone, the user must protect a KOV-14 card either by keeping it in the user's personal possession or storing it in a manner that will minimize the possibility of loss, unauthorized use, substitution, tampering, or breakage. A user can send the KOV-14 through X-ray machines or other security devices commonly used at airports without harming the card.

b. Fax. A secure facsimile machine connected to a STE, also called a Secure Facsimile System, is used to transmit and receive classified information. The

system must be accredited by a USDA COMSEC Officer. Once system compatibility verification has been made at each end, the information can be transmitted to the recipient or designated representative. The AD 471 can be used as a receipt if faxed with the document, signed by recipient, and immediately returned to the sender via fax. The fax verification sheet can also be used to prove where the document was sent along with the date and time. The verification sheet must stay with the document.

c. E-mail. Classified e-mail can be sent only on systems that are designed and approved for the level of information involved. USDA currently has access to the Department of Defense (DOD) SIPRNET, the Homeland Security Data Network (HSDN), and the Department of State cable system for electronic transmission of information classified at levels up to and including Secret. Top Secret and SCI information are transmitted using Intelligence Community Electronic Mail (ICEMAIL). Contact PDSD for additional guidance.

6. HAND CARRYING CLASSIFIED INFORMATION

a. Courier Cards or Letters. PDSD issues courier cards or letters to Department employees and USDA contractors who will need to routinely or occasionally hand carry documents within a 200-mile radius of their duty office. Courier cards or letters are valid for no more than 5 years. PDSD will maintain a list of individuals authorized to be couriers, at what level of classification they can carry classified information, and the expiration date of their letter. The requirements for being a courier are listed below. The courier must:

(1) possess a security clearance commensurate with the level of information being couriered;

(2) read and sign Appendix F, Courier Security Agreement, prior to being issued the courier letter or card;

(3) keep a copy of the courier card or letter in their possession while carrying classified documents;

(4) prepare the classified information for transportation as described in Chapter 5 of this Manual; and

(5) carry a valid USDA identification badge for verification.

b. Courier Letter Format. Courier letters must be prepared on USDA letterhead and contain the following:

(1) The full name of the individual, office, title, clearance;

(2) The period of authorization, which is based on when the individual's clearance is due for a periodic reinvestigation; and

(3) The name, title, organizational element telephone number, and original signature of the individual issuing the letter.

c. Aircraft. Airport security is a large and challenging program. Each airport has Federal rules as well as local rules based on location and threats. If possible, it is best to mail classified information to its destination rather than hand carry it on an aircraft. If classified information is carried on an aircraft, the courier must make every attempt to ensure that potential problems are minimized. Hand-carrying classified information on commercial aircraft has specific requirements to ensure that airport security is prepared for the courier's arrival and will not challenge the courier to open the package.

(1) The package must be double wrapped and labeled as described in Chapter 5. If a briefcase or courier bag is used as the outer wrapping, the courier should be prepared to open it for inspection. The material inside should have been prepared to meet inner envelope standards.

(2) The courier must have a letter prepared on official letterhead with the following:

(a) Size of the package and number of packages (i.e., 8 x 11 inches, 1 inch thick, VHS tape, 3 CD ROMS, 1 package). DO NOT describe the contents of the package or the classification level of the information.

(b) Departure and destination location and known transfer points;

(c) An indication of whether the package would be damaged during X-ray and a statement to that effect, and

(d) An office point of contact and phone number in case of problems during transport.

(3) The individual must process through routine airline security ticketing and boarding procedures. The briefcase may be opened for inspection, if requested. Authorized airline screening officials must not permit screening officials to open the envelopes. However, screeners may check the envelopes by X-ray machines, flexing, feel, and weight without opening the envelopes. The material being hand-carried must not contain a metal binding. Airport screening officials will be shown courier authorization documentation in order to avoid having the envelopes opened.

(4) If airline screening officials still insist on opening the envelopes, the individual will ask to see a Federal Aviation Administration (FAA) or Transportation Security Administration (TSA) field office representative. If the FAA or TSA representative insists on opening the envelopes after being shown proper identification and the courier authorization documentation, the individual will not attempt further boarding but will call the security official as identified on the courier authorization letter for assistance with the FAA or TSA representative. If the FAA or TSA representative continues to insist on opening the package, the courier should refuse to board and return directly to his or her office.

(5) Classified material must remain in the personal possession and under the constant surveillance of the courier at all times. The hand carrying of classified information on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage in a U.S. Government installation or a cleared contractor facility. Classified material cannot be stored overnight in an individual's hotel room, private residence, or hotel safe.

7. MEETINGS AND CONFERENCES (CLASSIFIED)

Agencies and individuals can sponsor classified meetings or conferences. The sponsoring USDA point of contact must coordinate closely with his or her security office when coordinating a meeting, conference, or symposium involving classified information.

a. Responsibilities.

(1) The Security Offices of non-USDA attendees and contractors must forward the attendees' clearance information to PDSD. Hand- carried clearance verification forms are not authorized and will not be accepted.

USDA agencies shall not receive attendee security clearance information for classified meetings. All clearance information must be sent directly to PDSD. The individual or agency sponsoring the meeting or conference can request PDSD to verify the clearances of USDA employees planning to attend the classified meeting or conference. These requests must be received by PDSD a minimum of 3 workdays prior to the event taking place.

(2) Sponsors must remind attendees to not bring cell phones, pagers, laptops, Blackberries, and other electronic devices into the meeting room. If such devices are observed, sponsors must request their immediate removal from the meeting room to preclude accidental transmission of classified discussions.

(3) The meeting sponsor must ensure that all notes taken during classified discussions are marked, transmitted, and stored commensurate with the highest classification of information being discussed. If taken off of USDA premises, the notes must be double wrapped. If the notes are to be carried back to a USDA office in the same building where the meeting occurred, and if the individual has an appropriate storage container, the notes can be single wrapped. For USDA employees, no courier card is required for transport between USDA facilities within the Washington, DC and Maryland areas. Non-USDA employees must present a valid courier card or letter to transport notes or other materials back to their offices. If none of the above is possible, the sponsor can also make arrangements to mail the notes to the individual's duty office.

(4) If visual personal recognition of an attendee cannot be made, the Sponsor must authenticate the attendee's identification through visual inspection of the person's Federal, State, or company-issued picture identification card.

(5) For meetings involving collateral Confidential, Secret, or Top Secret information, PDSD can conduct site visits to ensure that adequate measures are in place. The room must be approved for collateral classified discussions. (See Appendix E for requirements.) Meetings where SCI is discussed may only be held in a SCIF. Hotels and leased commercial training areas are not authorized for classified discussions.

b. Procedures and Notification. The sponsor of a classified event must determine whether each attendee has the appropriate security clearance and need-to-know before classified information is presented. Meeting announcements must expressly state the highest level of classified information that will be presented. For example, the announcement might state, "This meeting will be conducted at the SECRET level." During the meeting, the classification level and dissemination controls, if any, of classified information must be verbally announced before it is presented. For example, the sponsor might state: "The following information is classified at the Secret level and must not be disclosed to foreign nationals." In addition, sponsors must coordinate with PDSD, as early as possible, when scheduling the event. Smaller meetings may require little or no coordination. Larger events may require security measures to ensure protection of classified information.

8. CONTRACTORS

a. Visitors. Contractors visiting USDA facilities and requiring access to classified information must have a valid need-to-know and the appropriate security clearance. Need-to-know can be determined in several ways. The most obvious

is the federal agency's actions by allowing a contractor to represent their agency in meetings and working groups. USDA can request a copy of the contractor's DD Form 254, Department of Defense Contract Security Classification Specification which reflects the contractor's general description of their mission. The contract company's facility security office must forward a visit request with clearance verification to PDSD before its employees may participate in classified meetings or events.

b. USDA-Contracted Services. USDA agencies that contract for work involving access to classified information are required to provide security requirements to the contractor through a DD Form 254. The DD Form 254 is prepared by the Contracting Officer's Representative (COR) or project/program manager. When required, the Contracting Officer and the COR must ensure that the appropriate security clause and a completed DD Form 254 are incorporated into the solicitation and resultant contract.

c. Contract Clause. Federal Acquisition Regulation (FAR) 2.101 defines a classified contract as "any contract in which the contractor or its employees must have access to classified information during contract performance. A contract may be a classified contract even though the contract document itself is unclassified." USDA must adhere to the requirements outlined in the National Industrial Security Program Operating Manual (NISPOM). At a minimum, all classified contracts must contain FAR clause 52.204-2 (Security Requirements). This clause requires contractors to meet the security requirements identified in the NISPOM. The clause was published in Agriculture Acquisition Regulation Advisory # 61, dated March 2, 2004.

d. Contractor Responsibilities. USDA contractors are responsible for protecting classified information in accordance with the NISPOM and this Manual.

CHAPTER 7

DISPOSAL, DESTRUCTION AND REPRODUCTION

1. GENERAL

This chapter provides USDA's policy on the disposal, destruction and reproduction of classified information. Classified documents, media, and hardware that are no longer needed to meet mission requirements should be disposed of in accordance with the requirements outlined.

2. DESTRUCTION POLICY

Official records that are considered the "record copy" must be kept in accordance with the requirements set forth by NARA and Departmental Regulation 3080-001. If the material is considered the record copy, USDA records manager can provide further guidance. Non-record classified material will be destroyed as soon as it has served its intended purpose.

3. METHODS OF DESTRUCTION

a. Equipment. Classified material must be destroyed by burning, melting, chemical decomposition, pulping, pulverizing, shredding, disintegration, or mutilation sufficient to preclude recognition or reconstitution of the classified information. The NSA maintains a list of approved destruction devices for classified materials. A copy of this list can be obtained from PDSD. These devices also appear on the GSA Federal Supply Schedule. Purchase requests for High Security Crosscut Shredders or other destruction equipment, as well as questions regarding destruction devices or their use, should be directed to PDSD. Destruction capabilities available to USDA include shredding, burning, and pulverizing. Offices wishing to purchase a destruction device must contact their agency ISC, who will:

(1) forward a request to PDSD for certification of the destruction device. The request can be done over e-mail, but must include the make/model of the device, the year purchased, the purchase price, and the location of the device;

(2) request revalidation of PDSD every 3 years. This will ensure that PDSD maintains a current list of approved destruction equipment within USDA; and

(3) maintain documented approvals (by the office responsible for the device).

b. Procedures for Destruction. Destruction procedures and device use instructions must be posted in close proximity to the device. These procedures must be sufficient to ensure that:

(1) machines are clearly labeled with the highest level of classified information that can be shredded, such as Secret;

(2) classified material being destroyed is protected from casual visual observance during the destruction process; and

(3) users are aware they must inspect the device and immediate surrounding area to ensure that classified material is completely destroyed and that material is not inadvertently left in the destruction area. Note: Complete destruction is defined as destruction of material to equipment specifications. Strips of residue larger than these standards will be reported to security officials who will initiate action for repair.

c. Requirements for Each Classified Level. Top Secret, Secret, and Confidential information must be destroyed by individuals holding a security clearance equal to or higher than the level of information being destroyed. See below for document accountability of the destruction.

4. RECORD OF DESTRUCTION FOR ACCOUNTABLE MATERIAL

Form AD 471, Document Accountability, is the form that can be used for transmitting a document and documenting its destruction. Although this form is not mandatory for Confidential, Secret, and Top Secret information, it does not preclude local security offices from enforcing certification of destruction. To record the destruction of a document from outside of USDA, the agency's document accountability form should be used in lieu of the AD 471.

If the AD 471 is not available, a list of documents being destroyed can be generated and initialed by the person conducting the destruction and one witness. The list should include the document title or number, the date of the document, the originating organization, the highest level of classified information contained within the document, and the date of destruction.

5. DESTRUCTION OF CLASSIFIED MEDIA

Diskettes, film, CDs, memory sticks, USB devices, microfiche, slides, and hard drives can be sent, brought, or mailed to PDSD for destruction. When requesting

that PDSD destroy such items, they must be delivered or mailed with a copy of the form AD 471 to ensure that there is a record of what was transferred between offices.

6. BULK DESTRUCTION

Burn bags can be acquired through USDA supply channels. They are used for destruction of all levels of classified information. Within the Washington, D.C., National Capital Area, PDSD will provide guidance to offices on bulk destruction of classified information. If an office is not within the National Capital Region, then a local security office or agency ISC may be able to locate a nearby Federal facility that has an incinerator approved for destroying classified information. Most military installations can provide assistance in finding an approved local facility for destruction. Individuals or agencies unable to locate an approved incinerator may mail the information to PDSD for destruction. You must contact PDSD prior to sending classified documents for destruction and follow proper mailing procedures as discussed in Chapter 6 of this Manual. The following procedures apply when transporting classified material to the destruction facility:

a. Transportation of bulk classified material. Transportation of bulk classified material for destruction is accomplished in a closed vehicle continuously occupied by at least two individuals with security clearances and accesses commensurate with the level of classified material to be destroyed.

b. Burn Bags. Place no more than 10 pounds in each bag, fold the top, and staple it shut. Care must be taken to ensure that all burn bags are stapled across the top to prevent them from opening during transit. Each bag should be marked with the highest classification level of the information contained inside and with the organization’s name and phone number. It may be necessary for the individuals transporting the material to witness the actual destruction. Classified material will be left at an approved facility only after clearance verification is made.

7. REPRODUCTION OF CLASSIFIED MATERIAL

a. Documents and other material containing classified information shall be reproduced only when necessary for accomplishment of the organization's mission or for compliance with applicable statutes or directives. Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification. Copies of classified information shall be subject to the same controls as the original information.

b. Procedures for reproduction. Reproduction procedures and device use instructions must be posted in close proximity to the device. These procedures must be sufficient to ensure that:

(1) machines are clearly labeled with the highest level of classified information that can be copied, such as Secret;

(2) users are aware they must inspect the device and immediate surrounding area to ensure that no classified material is left on or in the machine.

8. DISPOSAL OF EQUIPMENT

Many offices within USDA lease their equipment from the Department. A machine previously used to reproduce classified information could be returned to the Office of Operations and later leased to another agency. If you are using equipment for classified reproduction, you must take precaution to avoid inadvertently disclosing classified information left on this equipment. Secure fax machines and secure printers and copiers used to reproduce classified material must be properly cleared to ensure there are no latent images on the equipment before turning it in or disposing of the equipment by running a blank sheet of paper through the copier or fax machine at least three times. Contact PDSD to coordinate the disposal of equipment used for classified reproduction and processing.

CHAPTER 8

SELF-INSPECTIONS

1. GENERAL

Self-inspections are the internal review and evaluation of individual USDA offices and agencies concerning their protection and handling of classified information. These inspections can be accomplished by PDSD, local security offices, or agency ISCs. Copies of the inspection report created by the ISC or local security offices must be sent within 5 calendar days to PDSD for record purposes. The report should also be forwarded to senior agency management for their overall program security awareness and to assist them in planning for future security upgrades or expenses.

2. FREQUENCY

Self-inspections should be completed a minimum of every 2 years by agencies that receive, generate, and store classified information. PDSD will schedule random inspections throughout USDA in order to meet the requirements of E.O. 12958. Self-inspections will also be completed when a pattern of security violations or infractions reveal a security weakness.

3. INSPECTION COVERAGE

E.O. 12958 defines the coverage of a self-inspection. Appendix G, Self-Inspection Checklist, can be used as a guide for agencies to conduct a self-inspection. Self-inspections can be expanded if necessary.

CHAPTER 9

LOSS, POSSIBLE COMPROMISE, OR UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

1. GENERAL

Any employee, contractor, or affiliate who has knowledge that classified information has been or may have been lost, or possibly disclosed to an unauthorized person(s), must immediately report the circumstances to PDSD, the local security office, or the agency ISC. PDSD will notify the ISOO when a compromise of classified information has occurred.

2. DISCOVERY

Any employee, contractor, or affiliate who discovers classified information improperly secured or unprotected is responsible for immediately taking custody of the information, safeguarding it in an appropriate manner, and reporting the incident to the local security official, agency ISC, and PDSD.

3. INVESTIGATION OF THE DISCOVERY

The local security official or ISC is responsible for determining circumstances surrounding any possible loss or compromise of classified information. A preliminary inquiry must be initiated immediately. It is the responsibility of the local security office or information security coordinator to conduct the inquiry or appoint a neutral party to conduct a preliminary inquiry of the events involving the discovery. The neutral party must be selected with care. It must be able to conduct the inquiry with impartiality. Appendix H provides guidance and a timeframe within which the report must be completed.

4. REPORT CONCLUSIONS

The preliminary inquiry conclusion will determine USDA's actions.

a. If no loss or unauthorized disclosure of classified information is established, then that part of the inquiry will be concluded. Other corrective action should be taken if security infractions or violations were found. See Section 5 below for security infractions and violations.

b. If there is evidence that classified information was possibly compromised, then further reporting is required. (See Appendix I.)

5. SECURITY INFRACTIONS AND VIOLATIONS

a. An infraction is any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that does not comprise a "violation" as defined below. An example would be an individual's opening a security container and failing to sign the SF 702, Security Container Check sheet. Infractions are more administrative in nature, but are required to be documented by the supervisor to deter patterns of neglect or disregard for security procedures.

b. A violation is a more serious disregard for security procedures and responsibilities. Violations must be documented and reported to PDSD. Agency personnel misconduct investigators may conduct investigations of alleged violations. Violations are defined as any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that include:

(1) disclosure to unauthorized persons of information properly classified under E.O. 12958 or its implementing directives;

(2) classifying or continuing to classify information in violation of E.O. 12958 or other implementing directives; or

(3) creating or continuing to conduct any SAP contrary to the requirements of E.O. 12958.

c. Disciplinary action for minor security infractions will generally not be imposed by management unless there are three or more of the same types of infractions, by the same individual, within a year. Disciplinary action, however, will be considered for security violations, and the following progressive discipline may be applied:

(1) A reprimand or warning after one or two security violations within a 1-year period.

(2) Suspension without pay or loss or denial of access to classified information for continued or serious security violations.

(3) Security clearance revocation and/or removal from employment when the above fails to impress upon an individual the seriousness of security violations.

6. CORRECTIVE ACTIONS

Inquiries and investigations often reveal gaps in security procedures, processes, or facilities. When corrective actions are required by an agency or office, the agency or office must report to PDSD the actions taken and a timeline for further actions. Corrective actions and the subsequent report should be completed within 30 calendar days of a preliminary inquiry or security violation investigation.

CHAPTER 10

SECURITY EDUCATION AND TRAINING

1. GENERAL

This chapter establishes the policy and requirements for the Department's Security Education and Training Program. All individuals responsible for creating, processing, or handling classified information for USDA must have a satisfactory knowledge and understanding of classification and declassification policies and procedures. Security infractions and violations reported each year to PDSD may result in additional training requirements.

2. SECURITY EDUCATION PROGRAM REQUIREMENTS

E.O. 12958 and its implementing directives mandate that agencies conduct initial indoctrination training, mandatory annual refresher training, and termination debriefings. All training must be documented and forwarded to PDSD.

Specialized training can be created to focus on program or agency security weaknesses and concerns. PDSD creates and conducts specialized training, or it can assist agencies in creating their own specialized training.

3. RESPONSIBILITIES

a. PDSD is responsible for ensuring that all individuals receive initial indoctrination training at the time they are authorized to have access to classified information.

b. Annual refresher training may be accomplished in several ways:

(1) PDSD can conduct training for an agency, or an agency ISC may conduct the training. The training given must meet the requirements of E.O. 12958 and ISOO Directive 1. Guest speakers may be invited to conduct the training as long as the training covers all required topics.

(2) Computer-based training may be used if a certification process is programmed within the training to create a record of who has successfully completed the training, or a certificate can be printed to reflect successful completion of the training. The certificate must be faxed to PDSD or ISC as proof that the training was completed.

(3) Video training is acceptable provided that each person watching the video initials or signs a form certifying that he or she received the training.

CHAPTER 11

EMERGENCY RELEASE OF CLASSIFIED INFORMATION AND PROTECTION OF CLASSIFIED INFORMATION

1. EMERGENCY RELEASE OF CLASSIFIED INFORMATION

a. Authority. The Secretary or his or her designees shall prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations in which there is an imminent threat to life or in defense of the homeland. The Department's special provisions are as follows: Classified information can be released to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

(1) The amount of classified information disclosed must be kept to the to the minimum needed to achieve the intended purpose;

(2) The number of individuals who receive it must be limited to the absolute minimum required to achieve the purpose;

(3) The classified information must be transmitted via approved Federal Government channels by the most secure and expeditious method to include those required in this Manual, or by other means deemed necessary when time is of the essence;

(4) Appropriate briefings must be provided to the recipients on their responsibilities not to disclose the information, and a signed SF 312, Nondisclosure Agreement must be obtained;

(5) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but not later than 30 calendar days after the release, the disclosing authority must provide the following information to the Executive Department that originally classified the information:

(a) a description of the disclosed information;

(b) to whom the information was disclosed;

(c) how the information was disclosed and transmitted;

(d) how the information is being safeguarded; and

(e) a description of the briefings provided and a copy of the nondisclosure agreements signed.

b. USDA Classified Information. If the classified information only involves information originally classified by USDA, then PDSD should be notified as soon as possible.

2. PROTECTING CLASSIFIED INFORMATION DURING AN EMERGENCY

a. Procedures. Agency security officials and ISCs or their designees are responsible for developing emergency plans for their areas of responsibility. These plans shall include procedures and responsibilities for the removal or destruction of classified material in case of fire, natural disaster, civil disturbance, or attack. The plan shall specifically include procedures for:

(1) Securing classified material when notification is received to evacuate a building;

(2) Providing building access to emergency personnel (police, fire, rescue squads, etc.);

(3) Relocating classified material when sufficient advance notice of an emergency situation is given;

(4) Recovering lost or missing classified material;

(5) Debriefing personnel involved in an inadvertent exposure to classified material resulting from an emergency situation; and

(6) Creating and maintaining emergency destruction procedures.

b. COMSEC. The OCIO, in conjunction with the COMSEC Custodian, is responsible for planning for the emergency protection of classified COMSEC material.

APPENDIX A

REFERENCES

1. E.O. 12958, Classified National Security Information, as amended by E.O. 13292, dated March 25, 2003.

2. ISOO Directive 1, Classified National Security Information, dated September 22, 2003.

3. Federal Register Notice 67 FR 189, September 30, 2002, Secretary of Agriculture Original Classification Authority.

4. Department of Defense 5200.1-R, Information Security Program, dated January 17, 1997.

5. Department of Defense 5220.22-M, National Industrial Security Program Operating Manual, 2/28/06.

6. Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information, dated June 30, 1998.

7. DCID 1/19, Security Policy for Sensitive Compartmented Information and Security Policy Manual, dated March 1, 1995.

8. DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, dated November 18, 2002.

9. U.S. Security Authority for NATO (USSAN), 1-69, North Atlantic Treaty Organization (NATO) Security program, dated April 21, 1982.

10. National Telecommunications and Information Systems Security Instruction (NTISSI) 4001, Controlled Cryptographic Items (U), March 25, 1985.

11. National Telecommunications and Information Systems Security Instruction (NTISSI) 0-4003, Reporting Communications Security (COMSEC) Insecurities, December 2, 1991.

12. Title 5, U.S.C., Section 552, as amended (Public Law 104-231, 110 Stat. 2422), The Freedom of Information Act.

13. Title 5, U.S.C., Section 552a, Privacy Act of 1974.

14. Title 10, U.S.C., Sections 119 and 128, Special Access Programs

APPENDIX B

DEFINITIONS

Access. The ability and opportunity to obtain knowledge of classified information.

Agency. A component within USDA such as the Foreign Agriculture Service, the Food and Nutrition Service, and the Office of the Inspector General.

Applicable Associated Markings. Markings, other than those which designate classification level, that are required to be placed on classified documents. These include the "classified by" line, downgrading and declassification instructions, special control notices, and related markings.

Automated Information System. An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Automatic declassification. The declassification of information based upon: (a) the occurrence of a specific date or event as determined by the original classification authority or (b) the expiration of a maximum timeframe for the duration of classification established under E.O. 12958.

Classification. The act or process by which information is determined to be classified information.

Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified, and establishes the level and duration of classification for each such element.

Classified National Security Information (or "Classified Information"). Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Classifier. An individual who makes a classification determination and applies a security classification to information, material, or a work area. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a properly classified source or a classification guide.

Collateral Information. Information identified as National Security Information under the provisions of E.O. 12958 but which is not subject to the enhanced security protection required for Sensitive Compartmented Information (SCI) under DCID 1/17. "Collateral" is a coined word that has been adopted by the SCI community to distinguish it from SCI

material. It merely means material that is Confidential, Secret, or Top Secret that is non-compartmented.

Communications Security (COMSEC). Measures employed and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emissions security, and physical security of COMSEC material.

Compromise. An unauthorized disclosure of classified information.

Continental United States (CONUS). United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

Controlled Cryptographic Item (CCI). A secure telecommunications or information handling equipment or ancillary device, or associated cryptographic component, that is unclassified but controlled. (Equipment and components so designated bear the designator "Controlled Cryptographic Item or CCI").

Critical Nuclear Weapon Design Information (CNWDI). Top Secret Restricted Data or Secret Restricted Data revealing the theory of the operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and highly explosive materials by type.

Damage to the National Security. Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of classified information.

Declassification. The authorized change in the status of information from classified information to unclassified information.

Declassification Authority. Refers to (a) the official who authorized the original classification, if that official is still serving in the same position, (b) the originator's current successor in that function; (c) a supervisory official of either, or (d) officials delegated declassification authority in writing by the agency head or the senior agency official.

Declassification Guide. Written instructions issued by a declassification authority that describe the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

Derivative Classification. The process of determining whether information has already been originally classified and, if it has been classified, ensuring that it continues to be

identified as classified by marking or similar means when included in newly created material.

Document. Any physical medium in or on which information is recorded or stored, to include written or printed matter, audiovisual materials, and electromagnetic storage media.

Downgrading. A determination that information classified at a specified level shall be classified at a lower level.

Event. An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.

File series. Documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Foreign Government Information. Refers to (a) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence, (b) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence, or (c) information received and treated as "Foreign Government Information" under the terms of a predecessor order to E.O. 12958.

Formerly Restricted Data. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, this information is treated in the same manner as Restricted Data.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

Information Security. The term "Information Security" means either (1) the system of policies, procedures, and requirements established under the authority of E.O. 12958 and the Information Security Oversight Office to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security or (2) the security controls over an Automated Information System required by the Federal Information Security Management Act of 2002.

Information Security Coordinator (ISC). Individuals designated by their agency or office to act as liaisons between their agency and the Personnel and Document Security Division, Information Security Staff relative to USDA Information Security Program. Responsibilities are identified in Chapter 1 of this Manual.

Infraction. Any knowing, willful, or negligent action contrary to the requirements of E.O. 12958 or its implementing directives that does not comprise a "violation." (See definition of "violation.")

Integrity. The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

Intelligence Activity. An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333.

Mandatory Declassification Review. Review for declassification of classified information in response to a request for declassification that meets the requirements of E.O. 12958.

Material. Any product or substance on or in which information is embodied.

Multiple Sources. Two or more source documents, classification guides, or a combination of both.

National Security. The national defense or foreign relations of the United States.

Need-to-know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Open Storage Area. A room or area constructed and operated within defined standards when the volume, bulk, or functions of the room/area make it impractical to store classified information in individual security containers.

Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

Original Classification Authority (OCA). An individual authorized in writing, either by the President or by an Executive Department head or other official designated by the President, to originally classify information.

Permanent Historical Value. Those records that have been identified in an agency records schedule as being permanently valuable.

Regrade. To raise or lower the classification assigned to an item of information.

Restricted Data. All data concerning (a) the design, manufacture, or utilization of atomic weapons, (b) the production of special nuclear material, or (c) the use of special nuclear material in the production of energy, but not including data declassified or removed from the Restricted Data category under Section 142 of the Atomic Energy Act of 1954, as amended.

Safeguarding. Measures taken and controls employed that are prescribed to protect classified information.

Secure Room. A room and/or areas built for the purpose of protecting classified national security information. Secure rooms are used for open storage of collateral classified information, processing classified information, and classified meetings and conferences.

Security Clearance. A determination that a person is eligible under the standards of E.O. 12968 for access to classified information.

Security In-Depth. A security program has security in-depth when the program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within a facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System, random guard patrols throughout the facility during non-working hours, closed-circuit video monitoring, or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during non-working hours.

Self-Inspection. The internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the information security program established under E.O. 12958 and its implementing directives.

Senior Agency Official (SAO). An official appointed by the Secretary of Agriculture under the provisions of Section 5.4(d) of E.O. 12958.

Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems established by the Director of Central Intelligence. Compartmentalization helps prevent the disclosure of how the U.S. Government obtains intelligence information.

Special Access Program (SAP). Any Federal program or activity (as authorized in E.O. 12958), employing enhanced security measures (stricter safeguarding and access requirements, code words, and similar measures) exceeding those normally required for collateral information at the same level of classification that is established, approved, and managed as a SAP. Unless otherwise authorized by the President, only the Secretaries of State, Defense, and Energy and the Director of Central Intelligence, or the principal

deputy of each, may create a special access program. USDA is not authorized to create a SAP.

Special Activity. An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media and does not include diplomatic activities or the collection and production of intelligence or related support functions.

Subject Matter Expert (SME). An individual with in-depth knowledge of a business area, science, or technology.

Systematic Declassification Review. The review for declassification of classified information contained in records that have been determined by the Archivist of the United States to have permanent historical value in accordance with Chapter 33, Title 44, United States Code, and is exempted from the automatic declassification provisions of E.O. 12958.

Unauthorized disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

Upgrade. To raise the classification of an item of information from one level to a higher one.

Vault. An approved area that is designed and constructed of masonry units or steel-lined construction to provide protection against forced entry. A modular vault approved by the GSA may be used in lieu of a vault as prescribed in Appendix E.

Violation. Refers to (a) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information, (b) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directives, or (c) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of E.O. 12958.

APPENDIX C

MANDATORY DECLASSIFICATION REVIEW PROCESS

1. Mandatory Declassification Review. USDA may be required to review classified information for potential release to the public. Requests are accepted for review if:

   a. the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

   b. the information is not exempted from search and review under Sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431); and

   c. the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

2. Exemption. Classified information that is exempt from mandatory review is information originated by:

   a. the incumbent President or, in the performance of executive duties, the incumbent Vice President;

   b. the incumbent President's White House Staff or, in the performance of executive duties, the incumbent Vice President's staff;

   c. committees, commissions, or boards appointed by the incumbent President; or

   d. other entities within the Executive Office of the President that solely advise and assist the incumbent President. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents under the control of the Archivist pursuant to Sections 2107, 2111, 2111 note, or 2203 of Title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly

of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or by an agency on the Panel. The information shall remain classified pending a prompt decision on the appeal.

3. Requests for classified records in the custody of USDA as the originating agency. A valid mandatory declassification review request need not identify the requested information by date or title of the records, but must be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. All requests must be forwarded to USDA, Office of Security Services, Personnel and Document Security Division, 14th and Independence Avenue, S.W., Mail Stop 5050, Washington, DC 20250-5050. In responding to mandatory declassification review requests, PDSD will:

   a. coordinate with subject matter experts to determine the information's current level of damage to national security;

   b. make a prompt declassification determination, if possible, and notify the requester accordingly;

   c. inform the requester of the additional time needed to process the request. A final determination must be coordinated within 180 calendar days from the date of receipt;

   d. ensure that, if information cannot be declassified in its entirety, subject matter experts and security professionals will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Any release of information must be coordinated with the agency's Privacy Act/FOIA Officer.

   e. notify the requester of their right for an administrative appeal if a denial is delivered on an initial request. Appeals must be filed within 60 calendar days of receipt of the denial.

4. Requests for classified records which USDA did not originally classify. If USDA receives a mandatory declassification review request for records in its possession that were originated by another agency, USDA shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that USDA may review its records, then USDA shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency.

   USDA will respond to the requester and provide a copy of the response to the originating agency.

5. Appeals of denials of mandatory declassification review requests. USDA appellate authority shall normally make a determination within 60 workdays following the receipt of an appeal. If additional time is required to make a determination, then USDA appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

6. Appeals to the ISOO Interagency Security Classification Appeals Panel (ISCAP). In accordance with E.O. 12958, the Interagency Security Classification Appeals Panel shall publish, in the Federal Register, the rules and procedures for bringing mandatory declassification appeals before it.

7. Foreign government information. When foreign government information is being considered for declassification, USDA will:

   a. determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time;

   b. determine if another exemption under section 1.6(d) of the E.O. 12958 (other than section 1.6(b)(5)), such as the exemption that pertains to United States foreign relations, may apply to the information;

   c. consult with any other concerned agencies in making its declassification determination; and

   d. consult with the Department of State and the foreign government prior to declassification.

8. Cryptologic and intelligence information. Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

9. Fees. In responding to mandatory declassification review requests for classified records, USDA may charge fees in accordance with section 9701 of title 31, United States Code. The schedules of fees published in the Federal Register by agencies in implementation of E.O. 12356 shall remain in effect until revised.

10. Assistance to the Department of State. USDA shall assist the Department of State in its preparation of the Foreign Relations of the United States (FRUS) series by facilitating access to appropriate classified materials in its custody and by expediting any declassification reviews of documents proposed for inclusion in the FRUS.

11. Requests filed under mandatory declassification review and the Freedom of Information Act (FOIA). When a requester submits a request both under mandatory review and FOIA, the USDA FOIA office or agency FOIA office will coordinate the request with PDSD. USDA will coordinate with subject matter experts, FOIA experts, the Office of the General Counsel, and security professionals to process requests for declassification that are submitted under the provisions of FOIA, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

12. Redaction Standard. USDA shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction.

13. Mandatory Review. When conducting a mandatory review for declassification, USDA shall declassify information that no longer meets the standards for classification under this Manual. USDA shall release this information unless withholding is otherwise authorized and warranted under applicable law.

APPENDIX D

EQUIVALENT FOREIGN SECURITY CLASSIFICATION

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Albania	TEPER SEKRET	SEKRET	IMIREBESUESHEM	I KUFIZUAR
Argentina	ESTRICTAMENTE SECRETO	SECRETO SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Balkans	STROGO PROVERLJIVO	TAJNO (Military Secret – VOJNA TAJNA) (State Secret – DRZAVA TAJNA)	PROVERLJIVO	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTS
Belgium(Flemish)	ZEER GEHEIM	GEHIEM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Bulgaria	STROGO SEKRENTO	SEKRETEN/ SEKRENTO	PROVERITELEN/ PROVERITELNO	ORINCHE (Limited) NAPROZOLEN (Illicit) or ZAPRANEN (Forbiden)
Cambodia	TRES SECRET	SECRET	SECRET/CONFIDENTIAL	
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	SECRETO	RESERVADO	RESERVADO
Colombia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENCIAL RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Croatia	NAJVECI	TAJNI	POVERLJIV	OGRANCIEN

	TAJNITAJNI			
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Guatemala	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN			
France	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL	DIFFUSION RESTREINTE
Germany	STRENGGEHEIM	GEHEIM	VS-VERTRAULICH	
Greece	ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ	ΑΠΟΡΡΗΤΟΝ	ΕΜΠΙΣΤΕΥΤΙΚΟΝ	ΠΕΡΙΩΡΙΣΜΕΝΗΣ ΧΡΗΣΕΩΣ
Guatemala	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Haiti		SECRET	CONFIDENTIAL	
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Hong Kong	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Hungary	SZIGOR'UAN TITKOS	TITKOS	BIZALMAS	
Iceland	ALGJORTI	TRUNADARMAL		
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Iraq (English Translation)	ABSOLUTELY SECRET	SECRET		LIMITED
Ireland (Gaelic)	AN-SICREIDEACH	SICREIDEACH	RUNDA	SRIANTA
Israel	SODI BEYOTER	SODI	SHAMUR	MUGBAL
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	KIMITSU	GOKUHI	HI	TORIATSUKAICHUI

Jordan	MAKTUM JIDDAN	MAKTUM	SIRRI	MAHDUD
Kazakstan	Use Russian equivalent			
Korea	I KUP PI MIL	II KUP PI MIL	III KUP PI MIL	
Kyrgyzstan	Use Russian equivalent			
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Moldovan (May also use Russian Equivalent)	ULTRASECRET	SECRET	CONFIDENTIAL	RESTRINS
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Netherlands	ZEER GEHEIM	GEHEIM	CONFIDENTIEEL or VERTROUWELIJK	DISENSTGEHEIM
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELL	BEGRENSET
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENDCIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	TAIJNY SPECJALNEGO	TAJNY	POUFNY	
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romania	ULTRASECRET	SECRET	CONFIDENTIAL or SECRET	RESTRINS
Russian	COBEOWEHHO	CEKPETHO		

Saudi Arabia	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI RESTRICTED
Spain	MAXIMO SECRETO	SECRETO	CONFIDENCIAL	DIFFUSION LIMITADA
Sweden (Red Borders)	HEMLIG	HEMLIG		
Switzerland	(Three languages. Top Secret has a registered number to distinguish it from Secret and Confidential.)			
French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
German	STRENG GEHEIM	GEHEIM	VERTRAULICH	
Italian	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Taiwan	(No translation in English characters)			
Tajikistan	Use Russian equivalent			
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Turkey	COK GIZLI	GIZLI	OZEL	HIZMET OZEL
Turkmenistan	Use Russian equivalent			
Ukraine	TSILKOM SEKRETNE	SEKRETNE	KONFIDENTSIAL'NO	DLYA
Union of South Africa	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Afrikaans	UITERS GEHEIM	GEHEIM	VERTROULIK	BEPERK
United Arab (Egypt)	TOP SECRET	VERY SECRET	SECRET	OFFICIAL
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Uzbekistan	Use Russian equivalent			
Viet Nam (French)	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE

(Vietnamese)	TOI-MAT	MAT	KIN	TU MAT

Note: The classifications given above represent the nearest comparable designations that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classification. The source of this information is DOD 5200.1-R, Information Security Program.

APPENDIX E

PHYSICAL SECURITY STANDARDS

1. VAULT

It may be necessary to promulgate vault requirements when a room is designed to meet special program requirements. USDA requirements must be equal to those of other Federal agencies to ensure compatibility with USDA customers, as follows:

a. Floor and Walls. Eight inches of reinforced concrete to meet current standards. Walls are to extend to the underside of the roof slab above.

b. Roof. Monolithic reinforced-concrete slab of thickness to be determined by structural requirements, but not less than the floors and walls.

c. Ceiling. The roof or ceiling must be constructed of reinforced concrete (the thickness to be determined by the structural requirements) but not less than the floors and walls.

d. Vault door and frame unit should conform to Federal Specifications AA-D-2757 Class 8 vault door or Federal Specifications AA-D-600 Class 5 vault door.

2. SECURE ROOM OR OPEN STORAGE

Secure rooms and rooms approved for open storage of classified material are terms used congruently. These rooms or areas are constructed and operated within defined standards when the volume, bulk, or functions of the room/area make it impractical to store Top Secret, Secret, or Confidential information in individual security containers. The following are the minimum standards:

a. Walls, Ceiling, Floor, and Roof. Construction must be of permanent construction materials, such as plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, glass, wire mesh, expanded metal, or other materials offering resistance to, and evidence of, unauthorized entry into the area. Walls will be extended to the true ceiling and attached with permanent construction materials, with mesh, or with 18-gauge expanded steel screen. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering, such as liquid nails. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction.

b. Doors. The access door to the room shall be substantially constructed of wood, metal, or other solid material. The hinge pins of outswing doors will be penned, brazed, or spot welded to prevent removal. Entrance doors should be equipped

with a built-in GSA three-position combination lock meeting Federal Specifications FF-L-2740. Under special circumstances, other locking devices for Secret and Confidential material can be approved. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar that extends across the width of the door, or by other means approved by USDA.

c. Windows. It is preferred that secure rooms be placed in an inner room without windows. If a window is necessary, however, the bottom of the window must be at least 18 feet above the exterior ground, thus precluding easy access. The windows should be opaque or covered with a window covering such as blinds that cannot be opened and closed. Windows must be covered with an 18-gauge steel screen or bars if there is a manmade or natural object near the window allowing easy access to the window or if the window is at ground level. Examples would be exterior stairs, trees, fences, or poles. Requirements can be reduced for the secure room if it is located within a controlled compound with roving guards. PDSD can approve secure rooms on a case-by-case basis.

d. Openings. Utility openings, such as ducts and vents, should measure 96 square inches or less in its smallest dimension. Openings larger than 96 square inches require the installation of 18-gauge wire mesh, expanded metal grills, commercial metal sound baffles, or an IDS to preclude entrance or alert attention to unauthorized entry.

3. INTRUSION DETECTION SYSTEM (IDS) STANDARDS

The purpose of an IDS is to detect an unauthorized penetration in a secured area. An IDS compliments other physical security measures and consists of the Intrusion Detection Equipment (IDE), operating procedures, and the response unit or guard force.

a. Alarm Process

(1) Premise Control Unit. The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors which comprise a “zone” at a monitor station. This shall be used as the definition of an alarmed zone for the purposes of this Appendix.

(2) PCU Signal. The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communication scheme. This prevents tampering or

injection of false information by an intruder. The supervised signal is sent by the PCU through the transmission link to the monitor station. Inside the monitor station either a dedicated panel or central processor monitors information from the PCU signals. When an alarm occurs, an enunciator generates an audible and visible alert to security personnel. Alarms, normally, result from intrusion, tampering, component failure, or systems power failure.

(3) Assessment. The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches a response force or guard.

(4) Response. The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response force must also determine the precise nature of the alarm and take all measures necessary to secure the area. The response must be within 15 minutes to meet the requirements for open storage or a secure room.

(5) Action. When encountering an open door to the secure area, a response force or guard member should immediately call for backup before entering the room. If the room is occupied and the responder verifies that the occupant is authorized, then the report is annotated appropriately. If it is determined that the room is unattended or that a possible theft may have occurred, the point of contact for the secure room must be called immediately. The security force must remain at the scene until the shift supervisor and room point of contact have completed an incident report. Safety before security must always be considered if there is risk of danger.

b. Alarm Features

(1) Transmission. When the transmission line leaves the facility and traverses an uncontrolled area, a Class I or Class II line must be used.

(a) Class I. Class I line security is achieved through the use of DES or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by the National Institute of Standards (NIST) or another independent testing laboratory is required.

(b) Class II. Class II line supervision refers to systems in which the transmission is based on pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication or UL Class II line supervision. The signal shall not repeat itself within a 6 month period. Class II security shall

be impervious to compromise using resistance voltage, current, or signal substitution techniques.

(2) Internal Cabling. Cabling between the sensors and the PCU should be dedicated to IDE and must comply with national and local code standards.

(3) Entry Control Systems. If an entry control system is integrated into an IDS, reports from the automated entry control system should be subordinate in priority to reports from intrusion alarms.

(4) Maintenance Mode. When an alarm zone is in the maintenance mode, its condition must automatically signal the monitor station. The signal must also appear as an alarm or maintenance message at the monitor station, and the IDS shall not be securable while in the maintenance mode. The alarm or message must be continually visible at the monitoring station throughout the maintenance period. A standard operating procedure must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods shall be achieved in the system. A self-test feature shall be limited to one second per occurrence.

(5) Annunciation of Shunting or Masking Condition. Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period if the condition exists whenever there is a survey of zones or sensors. Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the secure area.

(6) Power Supplies. Primary power for all IDE shall be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment shall change power sources without causing an alarm indication. Emergency power shall consist of a protected independent backup power source that provides a minimum of 4 hours operating power battery and/or generator power. When batteries are used for emergency power, they shall be maintained at full charge by automatic charging circuits. The manufacturer’s periodic maintenance schedule will be followed and the results documented.

(7) Component Tampering Protection. IDS components located inside or outside the secure area should be evaluated for a tamper protection requirement. If access to a junction box or controller will enable an unauthorized modification, tamper protection will be installed.

c. System Requirements.

(1) Independent Equipment. For areas protected by multiple alarms that have one monitor station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

(2) PCU Access and Secure Switch. No capability should exist to allow changing the access status of the IDS from a location outside the protected area. All PCUs must be located inside the secure area and should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU may be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

(3) Motion Detection Protection. Secure areas that afford reasonable access to the container, or where classified data is stored, should be protected with motion detection sensors (e.g., ultrasonic and passive infrared). In advanced PCUs, dual technology may also be authorized when one technology transmits an alarm condition independently from another technology. A failed detector shall cause an immediate and continuous alarm condition.

(4) Protection of Perimeter Doors. Each perimeter door shall be protected by a balanced magnetic switch that meets the standards of UL 634.

(5) Windows. All readily accessible windows (within 18 feet of ground level) shall be protected by an IDS, either independently or by motion detection sensors in the space.

(6) IDS Requirements for Continuous Operations Facilities. A continuous operations facility may not require an IDS. This type of secure area should be equipped with an alerting system when the occupants cannot observe all potential entrances into the room. Duress devices may also be required.

(7) False and Nuisance Alarm. Any alarm signal transmitted in the absence of detected intrusions or identified as a nuisance alarm is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designated but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The IDS maintenance program should ensure that incidents of false alarms should not exceed one in a period of 30 calendar days per zone.

(8) IDS Installation and Maintenance Staffing. Alarm installation and maintenance should be accomplished by employees who have a favorable suitability determination. PDSD and local personnel security representatives can coordinate the public trust evaluation.

(9) Monitoring Station Staffing. The monitoring station should be supervised continuously by employees who have a favorable suitability determination. PDSD and local personnel security representatives can coordinate the public trust evaluation.

APPENDIX F

COURIER SECURITY AGREEMENT

GENERAL INSTRUCTIONS: As a designated courier of classified material, you are authorized to hand carry or escort material while in a travel status between your duty and temporary travel duty (TDY) stations. In some situations, you may not have actual access to or specific knowledge of the information you are carrying. However, when you receive material in a sealed envelope or other container, you become the custodian of that information.

All USDA employees are subject to various sections of Title 18, United States Code, which makes criminal the unauthorized release of national security information. However, as a courier, you are solely and legally responsible for protection of the information in your possession. This responsibility lasts from the time you receive the information until it is properly delivered to the intended recipient.

This Appendix is provided to help you become familiar with your responsibilities as a courier and duties as a custodian as well as with the security and administrative procedures governing the safeguarding and protection of classified information.

ACCESS: Dissemination of classified material is restricted to those persons who are properly cleared and have a need-to-know the information. No person has the right to or is entitled to access to classified information solely by virtue of rank or position. To help prevent unauthorized access and possible compromise of material entrusted to you, it must be retained in your possession or properly guarded at all times. You cannot read, study, display, or use classified material while in public places or conveyances.

STORAGE: Whenever classified information is not under your personal control, it will be guarded or stored in a GSA-approved security container. You cannot leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, or storage compartments in the passenger section of commercial airlines, or while aboard trains or buses. You cannot store the material in detachable storage compartments such as trailers, luggage racks, or aircraft travel pods. You cannot pack classified items in regular checked baggage. Retention of classified material in hotel or motel rooms, or personal residences, is specifically prohibited. Safety deposit boxes provided by motels or hotels do not meet the standards for storage of classified material.

Advance arrangements for proper overnight storage at a U.S. Government facility or, if in the United States, a cleared contractor facility, is required prior to departure. Arrangements are the responsibility of the office authorizing the transmission of classified material.

PREPARATION: Whenever you transport classified information, it must be enclosed in two opaque sealed envelopes, or in similar opaque wrappings, or in two opaque sealed

containers such as boxes or other heavy wrappings without metal bindings. A briefcase, when used, can serve as an outer wrapping or container. The inner envelope or container shall be addressed to a Federal office (as if for mailing), stamped with the highest classification and placed inside the second envelope or container. When the outer covering is an envelope or box, it will be sealed and addressed for mailing (in the event of emergency) to the government activity and the person who is to receive the document. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission. Receipts will be exchanged when and if required.

HAND CARRY: A courier card or letter authorizing you to courier classified information should ordinarily permit you to pass through passenger control points within the United States without the need for subjecting classified material to inspection. Except for customs inspection, airports have established screening points to inspect all hand-carried items. If you are carrying classified material in envelopes you should process through the ticketing and boarding procedures in the same manner as other passengers. When carrying a sealed envelope in a briefcase (as carry-on luggage), it shall be routinely offered for inspection. The screening official may check an envelope by X-ray machine, flexing, feel, or weight without actually opening it. If the screening official is not satisfied with your identification, authorization statement, or letter, you will not be permitted to board the aircraft and are no longer subject to further screening for boarding purposes. Do not permit the screening official to open envelopes or read any portion of the classified document as a condition for boarding.

Your primary concern must be the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations can neither guarantee the protection of classified information nor be written to cover all conceivable situations. They must be augmented by basic security principles and a common-sense approach to protection of official national security information.

You are reminded that you are not to discuss classified information in public or discuss the fact that you are hand-carrying classified material.

APPENDIX G

SELF-INSPECTION CHECKLIST

PROGRAM MANAGEMENT

Does the activity hold a copy of DM 3440-001?

Does the activity hold a copy of E.O. 12958 and its implementing directives?

Is there a named mission area, agency, or office Information Security Coordinator (hereafter referred to as the ISC)?

Does the ISC have the necessary training to perform the job?

Does the ISC have direct and ready access to his or her agency head?

Are adequate inspections of the agencies that handle classified information made to determine the effectiveness of the Information Security Program? Who conducts the inspections? How often are reports rendered, and what corrective actions are taken?

Are data collected and reported to satisfy reporting requirements of the Information Security Oversight Office?

CLASSIFICATION, DECLASSIFICATION, AND DOWNGRADING

Is (original) security classification applied only to protect the national security and only as long as required by national security considerations?

Is information safeguarded as appropriate pending a determination by an original classification authority when there is reasonable doubt about the need to classify information?

Are measures taken to ensure that unnecessary classification and higher than necessary classifications are avoided?

Do persons who have derivative classification responsibility verify the information's current level of classification as far as practicable before applying the markings?

Are documents classified on the basis of the information they contain or reveal?

In unusual circumstances, is classification by compilation of unclassified items of information fully supported by a written explanation with the material so classified?

Is information extracted from a classified source derivatively classified or not classified in accordance with the classification markings shown in the source?

If holders of classified information have substantial reason to believe that information is classified improperly or unnecessarily, are they required to communicate that belief to their security representative or the classifier of the information for necessary correction?

Are disagreements on classification, declassification, or regarding actions referred to the next higher echelon if not resolved within 30 calendar days?

MARKING

Does your activity hold copies of the latest edition of ISOO Guide to Marking Classified Documents?

Are documents properly marked with the overall classification including page marking, and, except for blank pages, are interior pages marked according to their individual content including "unclassified" when no classified information is contained on such a page?

Is the classification authority properly identified on classified documents?

Is the original classification authority identified on the "classified by" line if all of the document's information is classified as an act of original classification?

Is "multiple sources" listed on the "classified by" line if the classification is derived from more than one original classification authority, or an original classification authority and another source, or from more than one source document, classification guide, or combination thereof?

When "multiple sources" are listed on the "classified by" line, are these sources identified and maintained with the file or record copy of the document?

Are major components (e.g., annexes and appendices) of complex documents properly marked?

Are illustrations, photographs, figures, graphs, drawings, charts, and similar portions of classified documents, as well as captions of such portions, properly marked?

Are documents containing compilations of unclassified information warranting classification and compilations of unclassified portions within documents marked properly with the overall classification and an explanation of the basis for the assigned classification?

Are transmittal documents properly marked?

Are electronically transmitted messages properly marked, and are adequate records maintained to show the source of the assigned classifications?

Are markings properly applied on special categories of material?

Are portions of classified documents properly marked?

Are all subjects or titles unclassified or only unclassified short titles used?

Are files, file folders, or groups of classified documents removed from secure storage marked conspicuously with the highest classification of any of the contents or an appropriate classified document cover sheet affixed?

Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded, is the material properly remarked by the holding office upon notification from the original classification authority?

Are derivative declassification dates or events properly applied?

Is each classified document marked on its face with one or more of the standard markings?

Have additional warning notices been applied as appropriate?

SAFEKEEPING AND STORAGE

Is information and material afforded protection commensurate with the level of classification assigned?

Is classified information that is not under the personal control and observation of an authorized person guarded or stored in a locked security container as prescribed for the various levels of classification?

Are classified containers marked showing an assigned container number or symbol in lieu of an external mark as to the level of classified information authorized to be stored therein?

Are combinations to security containers changed only by individuals with the appropriate security clearance and responsibility and at the frequency required?

Are combinations classified at the highest category of the classified information authorized to be stored therein?

Is a properly classified SF 700, Security Container Information, maintained for each container used for storing classified information, showing the location of the container

and the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination?

Is access to combinations limited to those individuals who are authorized access to the classified information stored therein?

When taken out of service, are built-in combination locks reset to a standard combination of 50-25-50 and combination padlocks reset to a standard combination of 10-20-30?

Do procedures provide for escorted persons to neutralize lockouts or repair damage to a container approved for the storage of classified information?

Are procedures established to prohibit the removal of classified material from an agency or office to do work at home or for other reasons?

When classified documents are removed from storage, are they kept under constant surveillance, face down, and covered when not in use with cover sheets (i.e., SF 703, 704, and 705 for Top Secret, Secret, and Confidential documents, respectively)?

Are preliminary drafts protected according to their content and destroyed as classified waste after they have served their purpose?

Has a system of security checks at the close of each workday been established for each area where classified information is handled or stored to ensure that the area is secure? Are the SF 701, Activity Security Checklist, and the SF 702, Security Container Checklist, used as part of this system?

Are cleared personnel aware of the prohibition against discussing classified information over an unsecure telephone?

Do individuals comply with security requirements and procedures governing disclosure of classified information at conferences, symposia, conventions, and similar meetings as well as those governing the sponsorship and attendance of U.S. and foreign personnel at such meetings?

Except for classified information that has been released to the custody of a foreign country, is the retention of U.S. classified material in foreign countries authorized only when that material is necessary to satisfy specific U.S. Government requirements, and is the material stored under U.S. Government control?

COMPROMISE OF CLASSIFIED INFORMATION

Are persons aware of their responsibilities in the event of an actual or possible loss or compromise?

Are investigations conducted?

ACCESS, DISSEMINATION, AND ACCOUNTABILITY

Before access to classified information is granted, have you determined that the individual possesses the appropriate security clearance and a need-to-know? Have you determined that an initial security briefing, which includes the requirement to execute a SF 312, Classified Information Nondisclosure Agreement, has been completed?

Is a demonstrated, foreseeable need for access to classified information established before a request for a personnel security clearance is initiated?

Have procedures been established to control access to classified information by visitors?

Do classified visit notifications meet the minimum requirements?

Have procedures consistent with DM 3440-1 been established for the proper dissemination of classified material?

Is classified information originating outside USDA not disseminated outside USDA without the consent of the originator?

Are dissemination requirements for other types of classified information met?

Are standing distribution requirements for classified information and materials, such as distribution lists, reviewed at least annually to verify the recipients' need-to-know?

Have administrative procedures been established by each office for controlling classified information and material to include providing a means to ensure that classified material sent outside an agency or office has been delivered to the intended recipient by use of a receipt?

Have procedures been developed to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is enclosed?

Are classified working papers marked, protected, and destroyed in accordance with the classification level of the material? Further, are they marked with a declassification or review date when placed in permanent files?

Are working papers accounted for and controlled in the same manner as final classified documents prior to being released by the originator outside the agency or transmitted through electronic channels, filed permanently, or retained more than 90 calendar days from date of origin?

Has specific reproduction equipment been designated for the reproduction of classified information, and have reproduction rules been posted on or near the designated equipment?

Are notices prohibiting reproduction of classified information posted on equipment used for the reproduction of unclassified information?

Are all copies of classified documents reproduced for any purpose, including those incorporated in a working paper, subject to the same controls prescribed for the original document?

COMPROMISE OF CLASSIFIED INFORMATION

Are persons aware of their responsibilities in the event of an actual or possible loss or compromise?

Are persons aware of the sanctions of releasing classified information in an unauthorized manner?

TRANSMISSION/HAND CARRYING

Is classified information transmitted or transported in accordance with the requirements for each security classification?

Does the preparation of classified information for transmission, shipment, or conveyance meet minimum requirements?

Are appropriately cleared personnel who are authorized to escort or hand-carry classified material complying with the minimum storage requirements?

Are the general restrictions concerning escort or hand carrying classified material adhered to, including not leaving material, under any circumstances, unattended while being carried in a private, public, or government conveyance?

Do individuals authorized to hand-carry classified material receive an appropriate briefing, and are they required to sign a statement acknowledging receipt of such briefing?

Is classified material authorized to be hand-carried aboard a commercial passenger aircraft only when there is neither time nor means available to transport the information?

DISPOSAL AND DESTRUCTION

Is documentary information disposed of or destroyed in accordance with USDA record management regulations?

Is non-record classified information destroyed when no longer needed, in accordance with proper procedures?

Do destruction procedures incorporate a means to verify the destruction of classified information?

Are approved methods of destruction used?

Have procedures been instituted that ensure that all classified information intended for destruction is actually destroyed?

Are appropriate destruction procedures followed for each level of classified material destroyed?

Are burn bags and their contents controlled and safeguarded in a manner designed to minimize the possibility of their unauthorized removal?

Is other classified waste (such as handwritten notes and working papers) destroyed properly when no longer needed?

SECURITY EDUCATION

Have security education programs been established to meet basic objectives?

At a minimum, have all personnel authorized or expected to have access to classified information received indoctrination training on all of the essential principles, practices, and procedures relating to the protection of classified information?

Are personnel advised of the adverse effects to the national security that could result from unauthorized disclosure and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control?

Are personnel informed of the techniques employed by foreign intelligence activities in attempting to obtain classified information and of their responsibility to report any and all such attempts?

Have all cleared personnel been advised of the penalties for engaging in espionage activities?

Are USDA employees denied access to classified information until they have received an initial security briefing and have signed an SF 312?

Have programs been established to provide, at minimum, annual security training for personnel having continued access to classified information?

Are personnel who have had access to classified information within the past year given a foreign travel briefing, before foreign travel, to alert them to their possible exploitation?

SECURITY CONTAINER MANAGEMENT

Classified documents in a security container filed in folders. Are classified markings, e.g., Confidential, Secret, etc., placed on the top and bottom on front and back of each folder?

The folder labeled with the subject of the classified information. Is an SF 702 annotated each time the container is opened or closed? Is an SF 700 updated and posted inside the drawer? Is the combination stored in an SF 700 and secured in another security container capable of an equal level of classified storage? Are visible Open-Closed signs, or similar signs, on the front of the container? Have combinations been changed within the last 3 years? Is there material between, behind, or underneath any drawers?

FOREIGN GOVERNMENT INFORMATION

Are the classification, declassification, marking, and protective requirements for foreign government information being met?

Is foreign government information contained in USDA documents controlled in a way that ensures that the information is not prematurely declassified?

ADMINISTRATIVE SANCTIONS

Are USDA personnel subject to administrative sanctions for knowingly, willfully, or negligently committing security violations?

Is appropriate and prompt corrective action taken whenever a knowing, willful, or negligent security violation occurs, or in the event of repeated administrative discrepancies or repeated disregard of the requirements of DR 3440-001.

APPENDIX H

PRELIMINARY INQUIRY QUESTION SHEET FOR THE POSSIBLE LOSS OR COMPROMISE OF CLASSIFED MATERIAL

After notifying PDSD of suspected loss or compromise of classified material, the individual responsible for completing the report of preliminary inquiry should make every effort to provide the information listed below. The individual must summarize the facts and make a determination as to whether classified material has been possibly lost or compromised. The report must be forwarded, within 72 hours of notice of the possible violation, to USDA, Office of Security Services, Personnel and Document Security Division, 14th and Independence Ave., S.W., Mail Stop 5050, Washington, DC, 20250-9305; (202) 720-7373. If that timeframe cannot be met, notify PDSD to negotiate an alternate timeframe.

The requested information includes the following:

1. The exact location of where the discovery took place.

2. The exact date and time discovered.

3. Name of individual(s) involved, Agency/Division/Branch/Office, and their respective phone number(s).

4. A summary of the discovery and circumstances, including the identification of the material lost or discovered and its classification level. USDA must notify the originating organization when there is a possible loss or compromise of their information.

5. Information gained from an interview of witnesses or individuals that may have had access to the material. Witnesses must prepare a statement and sign it for official record purposes. A signed and dated copy of an e-mail message from the witness qualifies as a signed statement. The statement should be detailed, providing information such as the approximate time they entered a room, what they saw, what their actions were, whether they noticed anything unusual, the last time they may have seen the material, etc.

6. Information gained from a review office time sheets, automated records from badge access systems, security container and room sign in/out sheets, computer records, and any other evidence that may be pertinent to the inquiry.

7. A determination of whether or not there has been a possible compromise or loss of classified material. One of the following statements should be used in the conclusion;

a. Compromise of classified material did occur;

b. Compromise of classified material did not occur;

c. Probability of classified material compromise is remote; or

d. Probability of classified material compromise is not remote.

8. A determination must also be made as to whether a security violation or infraction was committed, the name of who is the thought to be responsible, and the reason(s) why that individual may be responsible.

APPENDIX I

RESPONSIBILITY WHEN THERE IS A POSSIBLE COMPROMISE OF CLASSIFIED INFORMATION

PDSD must be notified within one calendar day of a suspected loss or compromise of classified material. PDSD is responsible for reporting to other Federal departments or foreign governments, through appropriate channels, when a loss or possible unauthorized disclosure of their classified information is suspected.

Incidents involving SCI and/or COMSEC information shall be reported and investigated within the specific channels established for these types of information. PDSD must be notified immediately.

Incidents involving contractors, grantees, licensees, and other personnel falling under the purview of the National Industrial Security Program (NISP) shall be handled in accordance with this Manual and the NISPOM. PDSD must be notified immediately.

If information originally classified by USDA is involved, an evaluation must be made to determine the impact and to make an estimate of damage to the national security. PDSD will either complete an evaluation or will designate a Special Investigation Officer who will determine the following:

1. Loss or possible compromise of the information; whether the information should still be considered classified and, if so, the damage to the national security.

2. Whether the information can be declassified. If so, a statement from an SME must explain why it can be declassified.

3. Whether the classification should be upgraded, requiring additional protection.

4. Whether the investigation disclosed a weakness in USDA security procedures and, if so, recommendations for corrective actions to be taken. The recommendations must identify the activity responsible for completing each corrective action.

All compromises involving computer systems, terminals, or equipment shall be reported to OCIO.

If espionage is suspected at any time, notify the Office of Inspector General immediately.