



**DM 3440-001**

**United States  
Department of  
Agriculture**

Office of Homeland Security  
and Emergency Coordination

**USDA Classified National Security Information  
Program Manual  
DM 3440-001**

**USDA CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM MANUAL**

**TABLE OF CONTENTS**

**Chapter 1: General Information .....5**  
    Purpose .....5  
    Scope .....5  
    Authority .....5  
    Special Instructions/Cancellations .....6  
    Positions and Responsibilities .....6

**Chapter 2: Security Clearances .....13**  
    Requirements for Access .....13  
    Interim Clearances .....13  
    NDA .....13

**Chapter 3: Security Training and Briefing .....15**  
    General .....15  
    ISC Training .....15  
    SSC Training .....15  
    Initial Security Briefings .....16  
    Site Specific Training .....16  
    Refresher Training .....16  
    Generic Travel Briefing .....17  
    High Risk Travel Briefing .....17  
    Foreign Travel Debriefing .....17  
    Original Classification Training .....17  
    SCG Training .....17  
    Derivative Marking Training .....18  
    Courier Training .....18  
    SCI Indoctrinations .....18  
    SCI Refresher Training .....18  
    Classified on Approved Systems .....18  
    Request for Waiver .....18

Debriefings .....	19
<b>Chapter 4: Classification and Marking .....</b>	<b>20</b>
Classification .....	20
Marking Requirements .....	25
RD/FRD .....	33
Intelligence Information .....	36
NATO Information Security Requirements .....	39
<b>Chapter 5: Safeguarding CNSI .....</b>	<b>44</b>
General Safeguarding Requirements .....	44
Waivers .....	44
Control and Accountability .....	44
Receiving Classified Materials .....	46
Classified Discussions .....	46
Unclassified Sensitive Security information .....	46
Storage and Storage Equipment .....	46
Construction Requirements .....	49
Transmission .....	66
Reproduction .....	71
Disposition .....	71
Retention .....	72
Destruction .....	72
COMSEC .....	73
Information Security Systems .....	73
<b>Chapter 6: Visits and Meetings .....</b>	<b>77</b>
Sending Clearance for a Classified Visit .....	77
Receiving Clearance for a Classified Visit .....	78
Meetings .....	79
Disclosure .....	81
<b>Chapter 7: Contracting .....</b>	<b>83</b>
Contractor Requirements .....	83
<b>Chapter 8: Reporting .....</b>	<b>85</b>

Required Reporting .....	85
SF-312 NDA .....	85
Change in Employee Status.....	86
Foreign Travel .....	86
Arms Control Treaty Visits .....	87
Litigation .....	87
Security Incidents, Infractions and Violations .....	87
Inadvertent Disclosure.....	89
FWA Reporting .....	90
Reporting for Travel or Posting in Critical Human Intelligence (HUMINT) Threat Posts .....	90
<b>Chapter 9: Self-Inspection Program .....</b>	<b>92</b>
General .....	92
Frequency .....	92
Inspection Coverage .....	92
Documentation .....	92
Reports .....	93
<b>Appendix A: References .....</b>	<b>94</b>
<b>Appendix B: Definitions .....</b>	<b>96</b>
<b>Appendix C: Acronyms and Abbreviations .....</b>	<b>104</b>
<b>Appendix D: Foreign Equivalent Security Classifications.....</b>	<b>108</b>

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

<b>DEPARTMENTAL MANUAL</b>	Number: DM 3440-001
SUBJECT: USDA Classified National Security Information Program	DATE: June 9, 2016
	OPI: Office of Homeland Security and Emergency Coordination

CHAPTER 1

GENERAL INFORMATION

1. PURPOSE

This Departmental Manual (DM) establishes the policies and procedures that govern the U.S. Department of Agriculture's (USDA) Classified National Security Information (CNSI) Program, including uniform requirements and guidance for classifying, safeguarding, declassifying, and destroying CNSI, whether originated by or released to USDA. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of CNSI, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information.

2. SCOPE

This DM applies to all USDA Mission Areas, Agencies, Offices, employees and contractors who possess, handle, distribute, process, transmit, transport, store, and/or who have been entrusted with CNSI and are required to protect that information according to standards commensurate with those discussed in this DM.

3. AUTHORITY

This DM implements applicable Federal statutes, Executive Orders (E.O.), national directives, international treaties, and certain Government-to-Government agreements. The authority for this guidance is derived from [E.O. 13526](#), *Classified National Security Information*; [E.O. 13587](#), *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*; [32 Code of Federal Regulation \(CFR\) Part 2001](#), *Classified National Security Information, Final Rule*; Office of Management and Budget (OMB) Memorandum [M-11-08](#), *Initial Assessment of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems*; and, Departmental Regulation [\(DR\) 3440-001](#), *USDA Classified National Security Information Program Regulation*.

#### 4. SPECIAL INSTRUCTIONS/CANCELLATIONS

This DM supersedes DM 3440-001, *USDA Classified National Security Information Program Manual*, dated May 1, 2008.

#### 5. POSITIONS AND RESPONSIBILITIES

E.O. 13526 requires each Department that has been given Original Classification Authority (OCA) to establish a CNSI program that ensures the protection of CNSI.

- a. The Secretary of Agriculture is responsible for originally classifying USDA information, up to the Secret level, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. In addition, the Secretary will:
  - (1) Demonstrate a personal commitment and commit senior management to the successful implementation of the CNSI program;
  - (2) Commit necessary resources to the effective implementation of the CNSI program established;
  - (3) Ensure that Departmental record systems are designed and maintained to optimize the appropriate sharing of CNSI, and to facilitate its declassification under the terms of E.O. 13526 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 CNSI program.
- b. The Assistant Secretary for Administration (ASA) is designated by the Secretary as the SAO who oversees the CNSI program and serves as liaison between USDA and the National Archives and Records Administration (NARA), Information Security Oversight Office (ISOO). This designation has been re-delegated to the Director of USDA's Office of Homeland Security and Emergency Coordination (OHSEC). The SAO shall maintain eligibility for access to CNSI commensurate to the level of information held or handled within the agency and will:
  - (1) Oversee USDA's CNSI program;
  - (2) Promulgate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;
  - (3) Ensure that there are Security Education, Training, and Awareness (SETA) programs, and establish the training schedule;
  - (4) Ensure that there is an ongoing self-inspection program, which shall include, but is not limited to, regular reviews of representative samples of the agency's original and

derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by Section 1.7(c) and 1.7(d) of E.O. 13526, and ensure delegate reports annually to the Director of ISOO on the agency's self-inspection program;

- (5) Establish procedures consistent with directives issued pursuant to E.O. 13526 to prevent unnecessary access to CNSI;
    - (a) Require that a need for access to classified information be established before initiating administrative clearance procedures; and
    - (b) Ensure that that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs.
  - (6) Develop special contingency plans for the safeguarding of CNSI used in or near high risk environments;
  - (7) Ensure that the performance evaluation used to rate employee performance includes the designation and management of CNSI as a critical element or item to be evaluated in the rating of:
    - (a) Original classification authorities;
    - (b) Security managers or security specialists; and
    - (c) All other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings.
  - (8) Account for the costs associated with the implementation of this DM, which shall be reported to the Director of ISOO for publication;
  - (9) Assign in a prompt manner agency personnel to any request, appeal, challenge, complaint, or suggestion arising out of this DM that pertains to CNSI that originated in a component of the Department that no longer exists and for which there is no clear successor in function;
  - (10) Report annually to ISOO as required by 32 CFR Part 2001, and have the SAO sign and review all outgoing reports; and
  - (11) Establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.
- c. USDA Mission Areas, Agencies, and Staff Offices are responsible for:

- (1) Collaborating with OHSEC to incorporate language defining security duties and responsibilities and qualifications for position descriptions and performance elements;
  - (2) Identifying to OHSEC an Information Security Coordinator (ISC); and
  - (3) Identifying to OHSEC a Top Secret Control Officer (TSCO). The TSCO can also serve as the ISC. The TSCO will be approved and appointed in writing by the Agency Head.
- d. The Personnel and Document Security Division (PDSO) of OHSEC, is responsible for revisions, additions, or deletions to this document. In addition, PDSO will:
- (1) Serve as the Special Security Office (SSO) for the department. The SSO is responsible for the day-to-day security management and implementation of the department's CNSI program. This includes, but is not limited to:
    - (a) Establish and maintain SETA programs to include training the OCA;
    - (b) Collaborate with USDA Mission Areas, Agencies, and Staff Offices to incorporate language defining security duties and responsibilities and qualifications for position descriptions and performance elements for the ISC, Site Security Coordinator (SSC) and TSCO;
    - (c) Establish and maintain a self-inspection program, which shall include the periodic review and assessment of USDA's classified products;
    - (d) Establish procedures to prevent unnecessary access to CNSI, including procedures that:
      - 1 Require a justification for access to CNSI before initiating security clearance procedures; and
      - 2 Ensure that the number of persons granted access to CNSI is limited to the minimum consistent with operational and security requirements and needs.
    - (e) Approve and inspect special contingency plans for the safeguarding of CNSI used in or near a high risk area;
    - (f) Through the Assistant Secretary of Administration (ASA) and the Director, Office of Human Resource Management (OHRM), ensure that applicable employee performance standards include language requiring the proper protection of CNSI for all employees who routinely handle such information. For example, standards may include the statement, "Maintains classified national security information In Accordance With (IAW) E.O. 13526, Classified National Security Information and DM 3440-001." At a minimum, positions requiring this standard are:

- 1 Derivative classifiers;
  - 2 Security specialists or ISCs, SSCs, TSCOs, SSOs; and
  - 3 All other personnel whose duties significantly involve the creation or handling of CNSI.
- (g) Account for the costs associated with the implementation of E.O. 13526, which shall be reported annually to the Director of ISOO for publication;
  - (h) Handle referrals for any request, appeal, challenge, complaint, or suggestion that pertains to CNSI that originated in a component of the Department that no longer exists, and for which there is no clear successor function;
  - (i) Assist the OCA with the preparation of a Security Classification Guide (SCG) 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. 13526);
  - (j) Assist in establishing and implementing a program for systematic declassification reviews;
  - (k) 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;
  - (l) Ensure that USDA does not disclose information originally classified by another agency without its authorization;
  - (m) Implement ISOO's established classification and marking requirements for all CNSI handled, stored, and processed within USDA;
  - (n) Ensure that North Atlantic Treaty Organization (NATO) information is controlled and accounted for and all NATO security procedures are followed; and
  - (o) Report to the SAO on the status of self-inspections and reporting yearly concurrent with the ISOO reporting requirements.
- e. The ISC is the trusted agent representing OHSEC, PDSD and USDA to the Mission Areas, Agencies, and Staff Offices on matters relating to this DM. The ISC is the primary point of contact for security matters for their respective Agency and/or Staff Office. The ISC is appointed in writing by their Agency Head that outlines their responsibilities and duties. Duties include, but are not limited to:
- (1) Serve as the respective Mission Area, Agency, and Staff Office liaison for day-to-day security related activities and provide support for annual data calls, annual

security refresher training, annual inspection of accredited spaces and equipment, and provide security assistance to their Agency, Mission Area, Staff Office on matters pertaining to accessing and/or handling CNSI;

- (2) Possess a national security clearance commensurate to the level of information handled by the Mission Areas, Agency(s), and Staff Office(s) they represent as well as possess access to all approved facility(s) for which they are responsible;
  - (3) Have thorough knowledge of their Mission Areas, Agency(s), and Staff Office(s) functions to include their classified missions or classified program support;
  - (4) Have the ability to apply adequate resources to protect CNSI;
  - (5) Initiate a preliminary inquiry when there is a failure to follow establish policy and procedures or there is suspicion of a possible compromise or loss of CNSI;
  - (6) Immediately report security incidents, infractions and violations to the SSO;
  - (7) Provide to the SSO all requested information to meet requirements for annual reporting to ISOO;
  - (8) Conduct inventories of classified assets and evaluating agency security needs, at a minimum on an annual basis;
  - (9) Coordinate document reviews with the SSO for possible classification or declassification;
  - (10) Maintain a record management system in accordance with [DR 3080-001](#), *Records Management* and the retention guide identified within this DM;
  - (11) Review, comment on, and provide recommendations on draft security policy documents when requested by PDSD or OHSEC; and
  - (12) ISCs are responsible for designating an SSC. ISCs shall collaborate with OHSEC to incorporate language defining security duties and responsibilities and qualifications for position descriptions and performance elements. The SSC is responsible for assisting in many of the duties of the ISC as delegated by the ISC.
- f. The SSC is the trusted agent representing PDSD and the ISC to the Secure Work Area (SWA). The SSC is the responsible person for all classified facilities that they have been appointed to oversee. They are the day-to-day manager of those facilities to include the activities in those facilities. The SSC is appointed in writing by either their Agency Head or their ISC and report to the ISC for SWA matters. Duties include, but are not limited to:
- (1) Serve as the official liaison between the ISC and the assigned SWA(s) for day-to-day security related activities and provide support for annual data calls, annual security

- refresher training, annual inspection of the accredited space(s) and equipment, and provide security assistance to all individuals with access to the SWA;
- (2) Possess a national security clearance commensurate to the level of information stored, processed or handled in their assigned SWAs;
  - (3) Conduct and record site specific training for all individuals on the access roster for their SWA, to include a review of the SWA Standard Operating Procedures (SOP);
  - (4) Ensure that all visitors not on the access roster are signed in and have the appropriate clearance and identification before entering the space;
  - (5) Have thorough knowledge of their Mission Areas, Agency(s), and Staff Office(s) functions to include their classified missions or classified program support;
  - (6) Initiate a preliminary report when there is a failure to follow establish policy and procedures or there is suspicion of a possible compromise or loss of CNSI;
  - (7) Immediately report security violations and infractions to the ISC;
  - (8) Provide to the SSO and/or ISC all requested information to meet requirements for annual reporting to ISOO;
  - (9) Conduct periodic inventories of classified assets and holdings;
  - (10) Coordinate document reviews with the ISC for consideration by SSO for possible classification or declassification;
  - (11) Maintain a record management system in accordance with DR 3080-001 and the retention guide identified within this DM; and
  - (12) Ensure that all special or additional site specific measures, as identified in the SOP, are followed and documented as required.
- g. The TSCO is the trusted agent representing OHSEC, PDSO and USDA in ensuring all that measures taken in matters relating to this DM to, track, record and store Top Secret material in their assigned Mission Areas, Agency(s), and Staff Office(s). They will assist with inventories of classified holdings and be able to report on status and disposition of Top Secret material. They are also responsible for making sure that Top Secret classified material is kept to the minimum amount necessary and marked appropriately. The TSCO reports directly to the Agency Head, or the ISC as prescribed on appointment.
- h. The Office of the Chief Information Officer (OCIO) has the responsibility to:
- (1) Certify and accredit USDA computer systems for processing collateral CNSI;

- (2) Coordinate with PDSD, requests for processing collateral CNSI on USDA computers and establishing secure networks;
  - (3) Incorporate, where appropriate, applicable USDA information security policies and procedures into USDA policies and standards for Information Technology (IT) system protection. System protection functions include communications security, encryption, network security products, and system reliability; and
  - (4) Identify cleared system administrators.
- i. USDA employees holding security clearances are required to:
- (1) Familiarize themselves with and adhering to the provisions of this DM;
  - (2) Protect CNSI from individuals who do not have the appropriate clearance level as well as a need-to-know;
  - (3) Maintain the proper security clearance;
  - (4) Meet the accountability requirements identified within this DM;
  - (5) Complete required security awareness and education training; and
  - (6) Report any security incidents immediately upon discovery to their respective SSC, ISC, or PDSD.

## CHAPTER 2

### SECURITY CLEARANCES

#### 1. REQUIREMENTS FOR ACCESS

Persons shall be allowed access to CNSI only if they:

- a. Possess a valid and appropriate security investigation as stated in [DR 4600-001](#), *USDA Personnel Security Clearance Program*;
- b. Have signed an accepted Non-Disclosure Agreement (NDA); and
- c. Have a valid need-to-know for the information in order to perform a lawful and authorized government function. Special projects require program manager to authenticate material contribution for need-to-know.

#### 2. INTERIM CLEARANCES

In accordance with DR 4600-001, applicants for Top Secret, Secret and Confidential clearances may be granted an interim clearance provided there is no evidence of adverse information of material significance. The interim clearance status will become a final clearance if results are favorable following completion of full investigative requirements. Non United States (U.S.) citizens are not eligible for access to CNSI on an interim basis.

An interim Secret or Confidential clearance is valid for access to CNSI at the level of the eligibility granted, except for RD, Communication Security (COMSEC) Information, and NATO information. An interim Top Secret clearance is valid for access to Top Secret information, RD, NATO Information, and COMSEC information at the Secret and Confidential level.

When an interim clearance has been granted and derogatory information is subsequently discovered or reported, the SSO will suspend access pending completion of the adjudication of the completed, final investigation.

Suspension of access is not a denial or revocation of the clearance and may not be appealed.

#### 3. NDA

Before being granted access to Confidential, Secret, or Top Secret information, employees must sign Standard Form [\(SF\)-312](#), *Classified Information Nondisclosure Agreement*, or other NDA approved by the Office of the Director of National Intelligence (ODNI). The SF-312 (or its predecessor, SF-189), or a legally enforceable facsimile retained in lieu of the original, shall be maintained for 50 years from the date of signature. The original SF-312 will be maintained with the employee's government Official Personnel File. PDSD shall maintain a copy of the SF-312 for the duration of their access and a period of one (1) year from the date of their debriefing. Electronic signatures shall not be used to execute the SF-312.

Before being granted additional accesses, individuals adjudicated and approved will be required to sign any additional NDAs at the behest of the Cognizant Security Authority (CSA) and will be subject to any requirements therein. Individuals approved for access to SCI must sign Form 4414, *Sensitive Compartmented Information Nondisclosure Agreement*, and may be subject to a Counter Intelligence (CI) polygraph at the behest of the CSA.

## CHAPTER 3

### SECURITY TRAINING AND BRIEFING

#### 1. GENERAL

This chapter establishes the policy and requirements for the Department's SETA Program. All individuals responsible for creating, processing, or handling CNSI for USDA must have a satisfactory knowledge of security policies, procedures, responsibilities, reporting, and classification management.

[E.O. 12968](#), *Access to Classified Information*, E.O. 13526, and E.O. 13587, and its implementing directives mandate that agencies conduct initial indoctrination training, mandatory annual refresher training, termination debriefings, and original and derivative classification training. All training must be documented, recorded and maintained in a central records management system for the duration of an individual's access.

The SAO will ensure that all cleared employees receive accurate and relevant security training and briefings commensurate with their involvement with CNSI. Specific and unique additional trainings will be identified by the SSO or the program manager relevant to the mission needs and environment. The SAO will suspend classification authority of individuals who fail to complete mandatory training for original classification to include declassification or derivative classification in the required time and have not received a waiver. PDSO will conduct all security training via Aglearn. Security training completed outside of Aglearn will be documented and updated in webSETS and or SIMS.

#### 2. ISC TRAINING

The SSO shall be responsible for ensuring that the ISCs complete all prescribed security training as outlined by PDSO and approved by the SAO. Training requirements shall be based on the agency's or mission area's involvement with CNSI. Designated ISCs must display at a minimum; a general understanding of physical security, technical security, classification management, reporting, self-inspection, and personnel security disciplines that are applied in a CNSI program. Acceptable training curriculums from ODNI, Office of the National Counterintelligence Executive or the Defense Security Service Academy are recommended.

#### 3. SSC TRAINING

ISCs shall be responsible for ensuring that designated SSCs have been appropriately trained. Training requirements shall be based on the facility's involvement with CNSI and will include delegated authority, area familiarization, SOP, and self-inspection requirements/techniques. All training will be documented by the ISC and forwarded to PDSO.

#### 4. INITIAL SECURITY BRIEFING

Initial briefings will be conducted either by the SSO or by a delegated ISC. Prior to being granted access to CNSI, every employee shall receive an initial security briefing that includes, at a minimum, the following:

- a. Insider Threat awareness;
- b. Operational security;
- c. An overview of the security classification system (OCA and derivative);
- d. Basic security policies, principles, practices;
- e. Criminal, civil, and administrative penalties;
- f. Employee reporting obligations and requirements;
- g. Requirements for access and continued access;
- h. Fraud Waste and Abuse (FWA) and whistleblower protection; and
- i. Security procedures and duties applicable to USDA.

#### 5. SITE SPECIFIC TRAINING

The SSC, in coordination with the ISC, shall prepare site specific training that details the procedures for the operational environment of their SWA. Site specific training shall be conducted either by the ISC or SSC managing a facility. The SSO shall provide site specific training for facilities under their direct control. Site specific training will be completed and documented by the SSC's on an annual basis.

#### 6. REFRESHER TRAINING

The ISC will support the SAO's requirement to ensure that all cleared employees receive security education and training at least annually. At a minimum, the ISC will ensure their cleared employees complete the Departmental annual training, but may also provide supplemental training. Refresher training will reinforce the information provided during the initial security briefing and will keep cleared employees informed of appropriate changes in security regulations. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. All refresher training must be approved by PDSD. The SSO will ensure that the SETA program meets the specific and unique requirements of the individual USDA programs. ISCs shall maintain records about the programs offered and employee participation in them and forward all records to the SSOs or record them in a central database as specified by the SSO.

## 7. GENERIC TRAVEL BRIEFING

The SSO or delegated ISC shall provide all cleared employees who are required to report their foreign travel, with security education and training regarding traveling Outside the Contiguous United States (OCONUS). This training can be given on a case by case basis or to all cleared individuals at the discretion of the SSO or delegated ISC. This training will include details about official or personal foreign travel and the risks to cleared individuals. The training briefing will be approved by the SSO. Once the briefing has been completed a cleared employee may travel to any low risk country (as determined by the SSO) with only a travel notification (using the Agriculture Department [\[AD\]-1196](#), approved Foreign Travel Reporting Form). This training will include a signed acknowledgement of responsibilities. Upon return from the foreign travel, the individual must fill out and turn in the debriefing portion of the AD-1196 form within 10 business days.

## 8. HIGH RISK TRAVEL BRIEFING

The SSO will coordinate with the ISC to provide all cleared employees with some form of security education and training regarding traveling OCONUS to high risk countries/areas. PDSD will maintain a current list of high risk countries. This training will include specific details about the risks of the intended destination to cleared individuals, to include current events, threats and risks. The briefing will be conducted by the SSO or designee. This training will include a signed acknowledgement of responsibilities. Upon return from the foreign travel the individual must fill out and turn in the debriefing portion of the AD-1196 form within 10 business days.

## 9. FOREIGN TRAVEL DEBRIEFING

The SSO or delegated ISC shall provide all cleared employees with a written foreign travel debriefing template or an in-person debriefing at the discretion of the SSO. All debriefings will be documented, recorded, maintained by the SSO, and forwarded to other agencies as required.

## 10. ORIGINAL CLASSIFICATION TRAINING

The SSO will ensure that the OCA at USDA has been adequately trained to perform their duties and is knowledgeable about the rules and regulations regarding the classification of new material and the creation of SCGs. Individuals who fail to complete the annual training in proper classification and declassification will have their classification authority suspended until training is completed unless a waiver has been approved. If waiver is approved, the employee will complete the training as soon as practicable.

## 11. SCG TRAINING

Upon the creation of an SCG all employees approved to use it for classification will be trained by the SSO or ISC in the proper use of SCGs and the proper creation of classified material. This training will be completed yearly and include a signed acknowledgement of responsibilities. Each classified activity shall have an SCG to identify Critical Program Information (CPI).

## 12. DERIVATIVE MARKING TRAINING

The SSO or delegated ISC shall provide designated cleared employees with a documented need to create derivatively classified material with training on the creation, marking, tracking and storage of derivative material. This training will be approved by the SSO, will be completed biennially and include a signed acknowledgement of responsibilities. Employees who fail to complete derivative training will have their authority to apply derivative classification marking suspended until training is completed unless a waiver has been approved. If waiver is approved, the employee will complete the training as soon as practicable.

## 13. COURIER TRAINING

The SSO shall provide courier training to individuals who demonstrate a requirement to courier information. There will be a generic briefing to qualify as a courier as well as specific training for couriers traveling OCONUS. All instances of courier training will be documented by the SSO. This training will be completed yearly and include a signed acknowledgement of responsibilities.

## 14. SCI INDOCTRINATIONS

Prior to being granted access to classified SCI information, an employee shall receive an initial SCI security briefing that includes an overview of the security classification system of SCI material from the SSO as approved by the sponsor.

## 15. SCI REFERSHER TRAINING

After being granted access to classified SCI information, an employee shall receive an annual SCI security refresher training that includes an overview of the security classification system of SCI material from the SSO as approved by the sponsor.

## 16. CLASSIFIED ON APPROVED SYSTEMS

Prior to being granted access to an approved system for CNSI, an employee shall receive an initial training that includes an overview of the approved system, its requirements and extra training on marking electronic copies of CNSI as well as sending CNSI email and CNSI chats. This training must be approved by the SSO and recorded and documented by the ISCs and forwarded to the SSOs.

## 17. REQUEST FOR WAVIVER

Employees who are unable to receive mandatory training in original classification, declassification or derivative classification marking in the required time due to an unavoidable circumstance will request in writing a waiver from the SAO. The request will contain the following information:

- a. Justification for the request; and

- b. An expected time to complete the training.

## 18. DEBRIEFINGS

A formal debriefing program must be developed and approved by the SSO and ISC. SSOs or delegated ISCs shall formally debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement), or when an employee's clearance is terminated, suspended, or revoked. A formal debriefing should include at a minimum:

- a. How to obtain a release before publishing;
- b. What can and cannot be discussed or placed in resumes and applications for security clearances;
- c. Turning in all holdings of CNSI;
- d. Applicability of penalties for engaging in espionage;
- e. Where to report suspected Foreign Intelligence Service (FIS) contacts or any attempted by unauthorized persons to solicit program data;
- f. Appropriate espionage laws and codes; and
- g. A NDA signed after the debriefing has taken place and forwarded to PDSD within two (2) business days.

In the event that an individual cannot be contacted, and the whereabouts of the individual cannot be determined within 30 days, the individual shall be administratively debriefed. This process is to include the update of any applicable databases, as well as the signing of the SF-312 (using “administratively withdrawn” in place of the subject’s signature).

## CHAPTER 4

### CLASSIFICATION AND MARKING

#### 1. 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 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 ISC should be contacted for assistance. A cleared subject matter expert must review the material and make an initial classification determination. If an agency ISC is not available, the SSO should be contacted for assistance.

In some situations, an aggregation of CNSI may warrant a higher classification than its component parts. For example, two (2) 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.

The SSC, in coordination with their ISC, is responsible for maintaining a control system to account for the disposition of all USDA original and derivative materials, regardless of the classification level.

##### a. Levels of Classification

There are three (3) 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 OCA 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 OCA is able to identify or describe; and
- (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 OCA is able to identify or describe.

##### b. 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. An original classification decision can be made only by a U.S. Government official who has been designated or delegated the authority in writing. The only USDA official with this authorization is the

Secretary of Agriculture and may not be delegated. A determination to originally classify information may be made only when:

- (1) An original classification authority is classifying the information;
- (2) The information falls into one or more of the categories set forth in Section 1.4 of E.O. 13526, as identified below:
  - (a) Military plans, weapons systems, or operations;
  - (b) Foreign government information;
  - (c) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
  - (d) Foreign relations or foreign activities of the U.S., including confidential sources;
  - (e) Scientific, technological, or economic matters relating to the national security;
  - (f) U.S. Government programs for safeguarding nuclear materials or facilities;
  - (g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
  - (h) The development, production, or use of weapons of mass destruction.
- (3) The unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to national security, which includes defense against transnational terrorism, that can be identified or described by the original classifier; and
- (4) The information is owned by, produced by or for, or is under the control of the U. S. Government.

The Secretary of Agriculture must state the concise “reason” for classification on the front of the document. The original classifier must also indicate a date or event for the duration of classification up to 10 years from the date of the original classification unless the date is further extended due to information sensitivities for up to 25 years. The date of origin of a classified document must be applied to OCA documents.

c. 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.

As such, when classified information is incorporated, paraphrased, restated, or generated in new form, it will be marked with the classification markings that apply to the source information.

Derivative classification includes the classification of information based on guidance, which may be either a source document or classification guide. The duplication or reproduction of existing CNSI is not derivative classification.

CNSI in email messages is subject to all requirements of E.O. 13526 and 32 CFR Part 2001, current editions. If an email is transmitted on a classified system, or includes a classified attachment and contains no CNSI within the body of the email itself, then the email is not a derivative classification decision. The email overall classification must reflect the highest level present in the attachment.

The Agency ISC shall ensure that all employees authorized to make derivative classification decisions:

- (1) Are identified by name and position, or by personal identifier, on documents they derivatively classify;
- (2) Observe and respect original classification decisions;
- (3) Carry forward the pertinent classification markings to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:
  - (a) Both the date or event for declassification that corresponds to the longest period of classification among the sources;
  - (b) A listing of the source materials.
- (4) Are trained, in accordance with SSO direction, in the proper application of the derivative classification principles, with an emphasis on avoiding over classification, at least once every two (2) years. Training will cover classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. The training will be approved by the SSO;
- (5) Are given ready access to the pertinent classification guides and/or guidance necessary to fulfill these important actions; and
- (6) Whenever practicable, derivative classifiers shall use a classified addendum if CNSI constitutes a small portion of an otherwise unclassified document.

d. Classification Challenge

PDSD will establish a system for processing, tracking and recording formal classification challenges made by authorized holders. Classification challenges shall be

considered separately from Freedom of Information Act (FOIA) or other access requests, and shall not process such challenges in turn with pending access requests.

If an employee believes:

- (1) That information is classified improperly or unnecessarily;
- (2) That current security considerations justifies downgrading to a lower classification or upgrading to a higher classification; or
- (3) That the security classification guidance is improper or inadequate, the employee shall discuss such issues with the pertinent ISC or SSO for remedy.

If a solution is not forthcoming, and the employee believes that corrective action is still required, a formal written challenge shall be made to the ISC or SSO. All challenges to classified information and/or material classifications shall be forwarded through the PDSO to the appropriate OCA. Such challenges shall include a description sufficient to identify the issue, the reasons why the employee believes that corrective action is required, and any recommendations for appropriate corrective action. Challengers and agencies shall attempt to keep all challenges, appeals and responses unclassified in any case; the information in question shall be safeguarded as required by this DM for its assigned or proposed level of classification, whichever is higher, until action is completed.

PDSO will provide a written response to the employee within 60 days. If no written answer is received within 60 days from an external OCA, the SAO should be requested to provide assistance in obtaining a response or a date in which the response will be received. If no response is received within 120 days, PDSO will notify the employee in writing of their right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP). The employee may also forward the challenge to the ISCAP if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. The fact that an employee has initiated such a challenge will not, in any way, serve as a basis for adverse action by the Government. If an employee believes that adverse action did result from a classification challenge, full details should be furnished promptly to the ISOO for resolution.

e. Proposal for Classification

Whenever an employee originates information they believe should be classified the following rules shall apply:

- (1) If the information was previously identified as classified, it shall be classified according to an appropriate SCG or source document, and marked as required by this DM.
- (2) If the information was not previously classified, but the employee believes the information may or should be classified, the employee should protect the information as though classified at the appropriate level and submit it to the agency that has an

interest in the subject matter for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used:

**CLASSIFICATION DETERMINATION PENDING**

**Protect as though classified (Top Secret, Secret, or Confidential)**

- (3) This marking shall appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received. In addition, employees are not precluded from marking such material as SSI, or any other information control structure enacted at USDA for the protection of unclassified information. Pending a final classification determination by the OCA, the employee should protect the information. It should be noted however, that E.O. 13526 prohibits classification of information over which the Government has no jurisdiction.

f. CNSI Appearing in Public Media

The fact that CNSI has been made public does not mean that it is automatically declassified. Employees shall continue the classification until formally advised to the contrary. Questions about the propriety of continued classification in these cases should be brought to the immediate attention of the SSC, ISC or SSO.

g. Downgrading or Declassifying CNSI

Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Only an SSO or delegated ISC can downgrade or declassify information based on formal notification from the OCA. If material is marked for automatic declassification, the employee shall seek guidance from the SSO or ISC prior to taking any action. The SSO will coordinate with the subject matter expert a justification for an exemption from the automatic declassification requirement. The SSO will prepare the notification from the SAO to the Director of ISOO with specific information being proposed for exemption from automatic declassification. The notification will be submitted to the Director of ISOO at least one (1) year before the information is subject to automatic declassification and the notification will include:

- (1) A detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;
- (2) An explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and
- (3) A specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

After a review of specific series of records as defined in section 6.1(r) of E.O. 13526, it is determined that the series of records almost invariably contain information that falls

within one (1) of more of the exemption categories under section 3.3(b) of E.O. 13526, the SAO will submit the request for exemption to the Director of ISOO at least one (1) year prior to the onset of automatic declassification. Copies of records within the specific file series or records of a similar topic to the specific files series located elsewhere may be exempted in accordance with exemptions approved by the ISCAP.

Downgrading or declassifying actions constitute implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of the classification. At the time the material is actually downgraded or declassified, the action to update records and change the classification markings shall be initiated and performed by the SSO or ISC.

Declassification is not an automatic approval for public disclosure.

## 2. MARKING REQUIREMENTS

Physically marking CNSI with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all CNSI be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal CNSI, the period of time protection is required, the identity (by name and position or personal identifier) of the classifier, the source(s) for derivative classification, and any other notations required for protection of the information. All classified material shall be marked and controlled in accordance with the ISOO marking guide, the program SCG, and other program guidance.

### a. Marking Requirements for Information and Material

As a general rule, the markings specified in paragraphs c through h below are required for all CNSI regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, Information Systems media, and slides may be more difficult due to size or other physical characteristics. Since the primary purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding.

### b. Identification Markings

All classified material shall be marked to show the name and address of the employee responsible for its preparation, the identity of the person (by name and position or personal identifier) responsible for each derivative classification action, and the date of preparation. These markings are required on the face of all classified documents.

### c. Overall Markings

The highest level of CNSI contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside

of the front cover, on the title page, on the first page, and on the outside of the back. All copies of classified documents shall also bear the required markings. Overall markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.

- (1) Top Secret notebooks are to be permanently bound documents with each page numbered consecutively, front and back.

d. Page Markings

Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the information on the particular page is UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which classification is assigned is adequately identified by portion markings according to subsection f below.

e. Component Markings

The major components of complex documents are likely to be used separately. In such cases, each major component shall be marked as a separate document. Examples include:

- (1) Each annex, appendix, or similar component of a plan, program, or project description;
- (2) Attachments and appendices to a letter; and
- (3) Each major part of a report.

If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included, such as: **All portions of this (annex, appendix, etc.) are UNCLASSIFIED.** When this method of marking is used, no further markings are required on the unclassified major component.

f. Portion Markings

Each section, part, paragraph, or similar portion of a document containing CNSI shall be marked to show the highest level of its classification, or that the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal CNSI. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately before the portion to which it applies. For paragraphs or subparagraphs beginning with numbers, letters or

symbols such as bullets, place the portion marking after the number, letter or bullet and before the text. In marking portions, the parenthetical symbols (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified shall be used.

Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.

g. Subject and Title Markings

Unclassified subjects and titles shall be selected for classified documents, if possible. A subject or title shall be marked with the appropriate symbol placed immediately before the item, which shall reflect the classification of the title, not the content of the document.

h. Markings for Derivatively Classified Documents

All CNSI shall be marked to reflect the source of the classification and declassification instructions. Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

(1) "CLASSIFIED BY" Line

The purpose of the "Classified By" line is to identify the person who applies derivative classification markings for the document. If not otherwise evident, the agency and office of origin will be identified and follow the name and position or personal identifier of the derivative classifier.

(2) "DERIVED FROM" Line

The purpose of the "Derived From" line is to link the derivative classification applied to the material by the employee and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the employee shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a SCG listed on a source document. When identifying an SCG on the "Derived From" line, the guide title or number, issuing agency, and date shall be included. Many times an employee is extracting information from more than one classified source document, in these cases; the employee may use the phrase "multiple sources". When the phrase "multiple sources" is used, the employee shall include a listing of the source materials in, or attached to, each derivatively classified document. This listing may take the form of a bibliography identifying the applicable classification sources. The markings used to show this are:

Single source document:

Derived by: Name and position or personal identifier  
Derived from: Source and date of source document.  
Declassify on: Repeat declassification date/event from source.

Multiple sources document:

Derived by: Name and position or personal identifier.  
Derived from: Identify sources.  
Declassify on: Use declassification date/event furthest into future from among source.

(3) "DECLASSIFY ON" Line

The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the employee shall carry forward the duration instruction from the source document or classification guide (e.g., date or event). When the source is marked "Original Agency's Determination Required" (OADR), "X1 through X8", Manual Review (MR), "Director of National Intelligence (DNI) Only," "Director of Central Intelligence (DCI) Only," or contains any other no longer valid declassification instruction, the "Declassify On" line shall be marked with a date that is 25 years from the date of the source document, unless other guidance has been provided by the OCA in accordance with E.O. 13526. 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. Material containing RD or FRD shall not have a "Declassify On" line unless co-mingled with CNSI subject to E.O. 13526.

(4) "DOWNGRADE TO" Line

When downgrading instructions are contained in the SCG or source document a "Downgrade To" line will be included. When completing this line, the employee shall insert Secret or Confidential and an effective date or event. The markings used to show this information are:

**CLASSIFIED BY** \_\_\_\_\_  
**DERIVED FROM** \_\_\_\_\_  
**DOWNGRADE TO** \_\_\_\_\_ **ON** \_\_\_\_\_  
**DECLASSIFY ON** \_\_\_\_\_

(5) "REASON CLASSIFIED" Line

As a general rule, a "Reason Classified" line will be shown only on originally classified documents.

i. Documents Generated under Previous E.O.'s

Documents classified under previous E.O.'s need not be re-marked to comply with the marking requirements of E.O. 13526.

CNSI originated under recent E.O.s contains overall, portion, paragraph, and appropriate downgrading and declassification markings that will provide sufficient guidance for the classification of extracted information. However, CNSI originated under previous E.O.s may not have these markings. If the source document does not contain portion markings, the overall classification of the source document shall be used for the extracted information in the new document.

The classification markings for a source document are the responsibility of the originator. Employees are encouraged to contact the SSO or ISC to avoid improper or unnecessary classification of material.

j. Marking Special Types of Material

The following procedures are for marking special types of material, but are not all inclusive. The intent of the markings is to ensure that the classification of the item, regardless of its form, is clear to the holder.

(1) Files, Folders, or Groups of Documents

Files, folders, binders, envelopes, and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included in the group. Cover sheets may be used for this purpose.

(2) Email and other Electronic Messages

Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text and shall be displayed at the top and bottom of each message. A "Classified By" line, a "Derived From" line, a "Declassify On" line, and portion markings are required on messages. Certain agencies may also require that messages contain a "Reason Classified" line in order to identify the specific reason for classification, which is carried over from the source document(s) or SCG. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. Email transmitted on or prepared for transmission on classified systems or networks shall be configured to display:

(a) The overall classification at the top and bottom of the body of each message;

(b) The overall classification marking string for the email will reflect the classification of the header and body of the message, including the subject line,

the text of the email, a classified signature block, attachments, included messages, and any other information conveyed in the body of the email; and

(c) Classified email will be portion marked.

When forwarding or replying to an email, employees or contractors shall ensure that the classification markings reflect the overall classification and declassification instructions for the entire string of emails and attachments. This includes any newly drafted material, material received from previous senders, and any attachments.

When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The markings required shall be included after the signature block, but before the overall classification marking at the end of the email. The last line of the message shall be the overall classification of the email.

Further training and approval will be given to all employees at USDA with access to classified systems.

(3) Microforms

Microforms contain images or text in sizes too small to be read by the unaided eye. The applicable markings shall be conspicuously marked on the microform medium or its container to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further markings and handling shall be as appropriate for the particular microform involved.

(4) Translations

Translations of U.S. CNSI into a language other than English shall be marked to show the U.S. as the country of origin, with the appropriate U.S. markings and the foreign language equivalent. No CNSI will be released to a foreign national or foreign nation without approval from the SSO coordinated through the SAO or relevant OCA.

k. Marking Transmittal Documents

A transmittal document shall be marked with the highest level of CNSI contained in the document and with an appropriate notation to indicate its classification when the enclosures are removed. An unclassified document that transmits a classified document as an attachment shall bear a notation substantially as follows: "Unclassified when Separated from Classified Enclosures". A classified transmittal that transmits higher CNSI shall be marked with a notation substantially as follows: "Confidential (or Secret) when Separated from Enclosures". In addition, a classified transmittal itself must bear all the classification markings required for a classified document.

l. Marking Wholly Unclassified Material

Normally, wholly unclassified material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient of such material that:

- (1) The material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or
- (2) The material has been reviewed and has been determined to no longer require classification and it is declassified.

m. Marking Compilations

In some instances, certain information that would otherwise be unclassified when standing alone may require classification or may warrant a higher classification than its component parts. When classification is required to protect a compilation of such information, the overall classification assigned to the compilation shall be conspicuously affixed. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the compilation. Any unclassified portions will be portion marked (U), while the overall markings will reflect the classification of the compiled information, even if all the portions are marked (U).

n. Working Papers

Working papers containing CNSI shall be dated when created; marked with the highest classification of any information contained in them; protected at that level or destroyed when no longer needed. Working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level if they are released outside of the facility, filed permanently, or retained for more than 180 days from the date of the origin. All working papers must have a cover sheet marked with the date of origin, the originator's name and the annotation "Working Paper".

o. Marking Miscellaneous Material

Material developed in connection with the handling, processing, production, storage and utilization of CNSI shall be handled in a manner that ensures adequate protection of the CNSI involved and shall be destroyed at the earliest practical time, unless a requirement exists to retain such material. There is no requirement to mark such material.

p. Marking Training Material

Unclassified documents or materials that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual unclassified status of the information. For example: **SECRET FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED** or **UNCLASSIFIED SAMPLE** or a similar marking may be used.

q. Downgrading or Declassification Actions

When documents or materials that have been downgraded or declassified are removed from storage for use or for transmittal outside the facility, they shall be re-marked according to paragraph 1 or 2 below. If the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, a downgrading and declassification notice may be attached to the inside of the file drawers or other storage container instead of the re-marking otherwise required. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. This authority is held only by the OCA or delegate that originated the document. When documents or other material subject to downgrading or declassification are withdrawn from the container solely for transfer to another, or when the container is transferred from one place to another, the transfer may be made without re-marking if the notice is attached to the new container or remains with each shipment.

- (1) Prior to taking any action to downgrade or declassify information, the employee shall seek guidance from the SSO. If such action is approved, all old classification markings shall be canceled and the new markings substituted, whenever practical. In the case of documents, as a minimum the outside of the front cover, the title page, the first page, and the outside of the back shall reflect the new classification markings, or the designation **UNCLASSIFIED**. Other material shall be re-marked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material.
- (2) When employees are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be re-marked to indicate the change. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or employee or contractor taking the action. Other holders shall be notified if further dissemination has been made by the employee.

r. Upgrading Action

When a notice is received to upgrade material to a higher level, for example from Confidential to Secret, the new markings shall be immediately entered on the material according to the notice to upgrade, and all the superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the material. Other holders shall be notified as appropriate if further dissemination of the material has been made by the employee or contractor. The notice shall not be classified unless the notice contains additional information warranting classification.

s. Inadvertent Release

If CNSI is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified or if control of the material has been lost, if all copies cannot be accounted for, or if unauthorized

personnel have had access to it, the employee shall immediately report the incident to either an SSC, ISC, SSO or PDS and help them:

- (1) Determine whether all holders of the material are cleared and authorized access to it;
- (2) Determine whether control of the material has been lost; and
- (3) If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned.

### 3. RD/FRD

This section is provided for information purposes only. It describes the requirements for classifying and safeguarding nuclear-related information that is designated RD or FRD. Such information is classified under [42 U.S.C. § 2011 \*et seq.\*](#), *Atomic Energy Act of 1954*, as amended, as opposed to other government information that is classified by E.O. 13526.

#### a. Unauthorized Disclosures

Employees shall report all unauthorized disclosures involving RD and FRD information to the SSO.

#### b. International Requirements

42 U.S.C. § 2011 *et seq.* as amended provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. The disclosure by a USDA employee of RD and FRD shall not be permitted until an agreement is signed by the U.S. and participating governments and disclosure guidance and security arrangements are established. RD and FRD shall not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the U.S. and the cooperating entity and supporting statutory determinations as prescribed 42 U.S.C. § 2011 *et seq.* as amended.

#### c. Personnel Security Clearances

Only the Department of Energy (DOE), Nuclear Regulatory Commission (NRC), Department of Defense (DOD), and the National Aeronautics and Space Administration (NASA) can grant access to RD and FRD. The minimum investigative requirements and standards for access to RD and FRD for contractors under the security cognizance of DOE are set forth below:

- (1) Top Secret RD – A favorable Single Scope Background Investigation (SSBI) or equivalent;
- (2) Secret RD – A favorable SSBI or equivalent;

- (3) Confidential RD – A favorable National Agency Check with Law and Credit (NACLC) or equivalent;
- (4) Top Secret FRD – A favorable SSBI or equivalent;
- (5) Secret FRD – A favorable NACLC or equivalent; and
- (6) Confidential FRD – A favorable NACLC or equivalent.

d. Classification

The Director, DOE, Office of Classification and Information Control, determines whether nuclear-related information is classified as RD under [10 CFR Part 1045](#), Subparts A, B, and C, Nuclear Classification and Declassification. The DOE and the DOD jointly determine what CNSI is removed from the RD category to become FRD under 10 CFR §1045.14 (a). These decisions are promulgated in classification guides issued under 10 CFR §1045.37 (a).

Only those employees designated as RD classifiers by the SAO may classify RD and FRD documents according to 10 CFR §1045.37 (a) (2). Such employees must be trained on the procedures for classifying, declassifying, marking, and handling for RD and FRD information and documents according to 10 CFR §1045.35 (a). RD classifiers shall use classification guides as the primary basis for classifying and declassifying documents containing RD and FRD information 10 CFR §1045.37 (c). If such classification guidance is not available and the information in the document appears to meet the definition of RD, then the RD classifier shall, as an interim measure, mark the document as Confidential RD (or as Secret RD if the sensitivity of the information in the document so warrants) and promptly forward the document to the SSO. The SSO shall provide the employee with the final determination based upon official published classification guidance. If the SSO cannot make such a determination, the SSO shall forward the document to DOE for a classification determination.

e. Declassification

DOE determines whether RD and Transclassified Foreign Nuclear Information (TFNI) information may be declassified under 10 CFR §1045.14 (b). The DOE, jointly with the DOD, determines whether FRD information may be declassified under 10 CFR §1045.14 (d).

Documents marked as containing RD, FRD and TFNI information remain classified until a positive action by an authorized Government official is taken to declassify them; no date or event for automatic declassification ever applies to RD, FRD, and TFNI documents.

f. Challenges to RD/FRD Classification

Any employee who believes that an RD, FRD, or TFNI document is classified improperly or unnecessarily may challenge that classification following the procedures established by the SSO.

g. Marking

Documents containing RD, FRD, and TFNI information shall be marked as indicated below:

- (1) Front of the document. In addition to the overall classification level of the document at the top and bottom of the page, the following notices must appear on the front of the document, as appropriate:

- (a) If the document contains RD information:

**RESTRICTED DATA**

This document contains RESTRICTED DATA as defined in the Atomic Energy Act (AEA) of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

- (b) If the document contains FRD information:

**FORMERLY RESTRICTED DATA**

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144(b), AEA 1954.

- (2) A document containing RD or FRD information also must be marked to identify:

- (a) The classification guide or source document (by title and date) used to classify the document; and
- (b) The identity of the RD classifier unless the classifier is the same as the document originator or signer:

Derived from: (Classification guide or source document – title and date)  
RD Classifier: (Name and position or title)

- (3) Interior Page

Each RD or FRD document must also be clearly marked at the top and bottom of each interior page with the overall classification level and category of the document or the classification level and category of the page, whichever is preferred. The abbreviations RD and FRD may be used in conjunction with the classification level (e.g., Secret RD or Secret FRD).

(4) Other Caveats

Any other caveats indicated on the source document shall be carried forward.

(5) TFNI

Documents containing TFNI must be marked in accordance with 32 CFR Part 2001, current edition, and [ISOO Notice 2011-02](#), *Further Guidance and Clarification on Commingling Atomic Energy Information and Classified National Security Information*.

(6) Comingling

To the greatest degree possible, do not comingle RD and FRD in the same document with information classified pursuant to E.O. 13526.

4. INTELLIGENCE INFORMATION

This section provides general guidance on the intended purpose of several security tenets that form a critical baseline for the protection of intelligence information.

a. Apply Need-to-Know

Authorized holders (individuals or information systems) of classified intelligence information shall determine if prospective recipients (individuals or information systems) have the requisite clearances and accesses, and require knowledge of specific classified intelligence information in order to perform or assist in a lawful and authorized governmental function. To effectively implement this concept, Intelligence Community (IC) departments, agencies, and bureaus must work cooperatively with customers to understand their requirements and ensure that they receive all applicable classified intelligence information while minimizing the risk of unauthorized disclosure. IC organizations shall provide intelligence at multiple security levels appropriate to the security authorizations of intended customers. Customers, in turn, shall be responsible for verifying need-to-know for this information for individuals of information systems within their organizations.

b. Protect SCI

In order to protect information regarding particularly fragile intelligence sources and methods, SCI has been established as the SAP for the ODNI. SCI must be protected in specific SCI control systems and shall be clearly defined and identified. ODNI has the sole authority to create or to discontinue SAPs, including SCI access control systems pertaining to intelligence sources and methods and classified intelligence activities (including special activities, but not including military operational, strategic, and tactical programs).

c. Educate the Work Force

The SSO shall establish formal security awareness training and education programs to ensure complete, common, and consistent understanding and application of security principles. Individuals shall be advised of their security responsibilities before receiving access to classified intelligence information and information systems. Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.

d. Promote Security Reciprocity

To facilitate security reciprocity across the IC and industry, the SSO shall accept from other IC departments, agencies, and bureaus access eligibility determinations and accreditations of information systems and facilities except when an agency has documented information indicating that an employee, contractor, information system, or a facility does not meet Director of Central Intelligence Directive (DCID) standards. Any exceptions to access eligibility determinations and accreditations of information systems and facilities must be noted in certifications to other agencies.

e. Manage Risk

Agencies shall employ a risk management/risk analysis process to cost-effectively minimize the potential for loss of classified intelligence information or assets and the consequences should such loss occur. This methodology shall involve techniques to counter threats, reduce vulnerabilities, and implement security countermeasures.

f. Minimize Insider Threat

All personnel who have access to classified intelligence information shall be thoroughly vetted, fully trained in their security responsibilities, appropriately supervised, and provided a secure work environment. Counter Intelligence (CI) and security management shall maintain aggressive programs to deter, detect, and support the apprehension and prosecution of those cleared personnel who endanger national security interests.

g. Control Markings Authorized for Intelligence Information

(1) "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)

Information bearing this marking may be disseminated within the headquarters and specified Mission Areas, Staff Offices, or Agencies of the recipient organizations, including their contractors within government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or product is presented or distributed only to original recipients of the information and marked accordingly. Dissemination beyond headquarters or to agencies other than the original recipients requires advanced permission from the originator.

(2) “CAUTION-PROPRIETARY INFORMATION INVOLVED” (PROPIN)

Marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This information may not be disseminated outside the Federal Government in any form without the express permission of the originator of the proprietary information. Dissemination to contractors is precluded irrespective of their status to, or within, the U.S. Government without the authorization of the originator of the information.

(3) “NOT RELEASABLE TO FOREIGN NATIONALS” (NOFORN)

NOFORN is CNSI that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator. It cannot be used with AUTHORIZED FOR RELEASE TO (REL TO) [country codes] or EYES ONLY on page markings. When a document contains both NOFORN and REL TO (see below) or NOFORN and EYES ONLY portions, NOFORN takes precedence for markings at the top and bottom of the page.

(4) “AUTHORIZED FOR RELEASE TO (REL TO) (name of countries /international organization)”

This marking is used to identify intelligence information that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign/international organization indicated.

h. Limitation on Dissemination of Intelligence Information

A USDA employee is not authorized to further disclose or release classified intelligence information without prior written authorization of the releasing agency, coordinated with the SSO.

i. Safeguarding Intelligence Information

All intelligence information in USDA’s possession shall be safeguarded and controlled according to the provisions of this DM for CNSI of the same classification level, with any additional requirements and instructions received from the SSO, and with any specific restrictive markings or limitations that appear on the documents themselves.

j. Inquiries

All inquiries concerning source, acquisition, use, control, or restrictions pertaining to intelligence information shall be directed to the SSO who will coordinate with the providing agency.

## 5. NATO INFORMATION SECURITY REQUIREMENTS

This section provides the minimum standards for the protection of classified NATO information. All personnel employed by or sponsored by USDA are responsible for protecting classified information under their custody and control in accordance with the instructions provided in this DM. These security requirements have been established by the U.S. Security Authority for NATO (USSAN) for safeguarding NATO information provided to U.S. industry.

### a. Access

- (1) Access to NATO information is based on a demonstrated need-to-know, possession of the appropriate level security clearance, and receipt of a NATO security briefing.
- (2) Access to classified NATO information above the NATO Restricted level requires a NATO clearance of at least the level of the information accessed. Access to NATO Restricted or NATO Unclassified information does not require a clearance, but a need-to know still exists.
- (3) Access to ATOMAL information requires a final Top Secret U.S. clearance regardless of the actual level of classification.
- (4) Anyone accessing classified NATO information has a NATO security briefing before the initial access, and an annual refresher thereafter.
- (5) When access to classified NATO information is no longer required, individuals are debriefed and the record of debriefing is maintained by the SSO.

### b. NATO Clearances

- (1) Requests for NATO clearances, with justification, are processed through the SSO and approved by OHSEC.
- (2) A NATO Secret or Confidential clearance requires a valid U.S. Secret Clearance.
- (3) Interim U.S. Secret clearances are acceptable for access to non-ATOMAL NATO Secret information and below.
- (4) A Cosmic Top Secret clearance requires a final U.S. Top Secret Clearance.
- (5) Requirements for U.S. Clearances are in accordance with DR 4600-001.

### c. NATO Clearance Levels

- (1) NATO has the following levels of security classification:
  - (a) COSMIC TOP SECRET (CTS);
  - (b) NATO SECRET (NS);

- (c) NATO CONFIDENTIAL (NC); and
  - (d) NATO RESTRICTED (NR).
- (2) Another marking, ATOMAL, is applied to U.S. RD or FRD and United Kingdom (UK) Atomic information that has been released to NATO. ATOMAL information is marked:
- (a) COSMIC TOP SECRET ATOMAL (CTSA),
  - (b) NATO SECRET ATOMAL (NSA), or
  - (c) NATO CONFIDENTIAL ATOMAL (NCA).
- d. Briefings and Training
- Before having access to NATO CNSI, employees shall be given a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO CNSI. The initial briefing will be conducted by the designated NATO SSO. Annual refresher briefings shall also be conducted. When access to NATO CNSI is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Certificates shall be maintained for two (2) years for NATO Secret and NATO Confidential, and three (3) years for Cosmic Top Secret and all ATOMAL information. The NATO SSO shall maintain a record of all NATO briefings and debriefings in a designated database. All requests for access to NATO information are approved by OHSEC.
- e. Protection and Storage
- (1) NATO Cosmic Top Secret, NATO Secret, and NATO Confidential information is afforded the same level of protection given its U.S. equivalent U.S. classified information.
  - (2) Protection and storage requirements are outlined in Chapter 5.
  - (3) In addition to the storage requirements outlined in Chapter 5, NATO information is stored separately from other classified non- NATO information. A separate drawer or a partition within a drawer is sufficient to meet this requirement.
  - (4) NATO ATOMAL information is subject to the same protections as RD and FRD as outlined in Chapter 4 of this DM.
  - (5) NATO ATOMAL information is further separated from other classified NATO information within storage containers. A separate drawer or a partition within a drawer is sufficient to meet this requirement.

- (6) NATO Restricted information is afforded the same protection as U.S. Confidential information when possible. However, storage in a locked drawer or file cabinet is acceptable when other storage is not practical.
- (7) NATO Restricted information is processed or stored only on systems approved for the processing of classified U.S. information.
- (8) NATO UNCLASSIFIED information is afforded the same protections as information categorized as For Official Use Only (FOUO).
- (9) The use of coversheets with classified NATO materials is required.

f. Transmission and Transportation

- (1) Transmission and transportation of NATO Confidential, NATO Secret, and Cosmic Top Secret information is afforded the same protections as its U.S. equivalent classification with the exception of commercial overnight delivery, which is prohibited. These protections are outlined in Chapter 5.
- (2) When issued, courier cards indicate that the holder has a NATO clearance should they need to transport classified NATO information.
- (3) Except for mail, NATO Restricted materials are transmitted or transported in a manner approved for NATO Confidential or higher information.
- (4) Transmittal of NATO Restricted information requires the use of secure phone, fax, or an email system approved for the transmission of classified U.S. information.
- (5) NATO Restricted information may be sent using U.S. first class mail. The information is double wrapped. The outer envelope may count as one of the wrappings. The contents or the fact that the information is NATO classified is not discernable from the outside.

g. Accountability and Control

- (1) NATO information flows down from the Central U.S. Registry (CUSR) to USDA users through a system of sub-registries, control points, and user offices. Sub-registries are those offices that receive materials directly from the CUSR, and are formerly established by the CUSR. Control points are established through a sub-registry. User offices can be established through a sub-registry or a control point. Control points and user offices receive materials and operational guidance from the established sub-registry.
- (2) The SSO maintains the prime USDA NATO sub-registry.
- (3) Sub-registries are authorized to establish control points, up to the level of the sub-registry, wherever required.

- (4) Sub-registries and control points maintain a current Department of the Army Adjutant General (DAAG) Form 29. Control points should forward the original to the cognizant sub-registry, and the sub-registry shall ensure that the CUSR has the most recent original copy for all sub-registries and control points.

h. Destruction

- (1) Classified NATO information is destroyed in the same manner approved for classified U.S. information. For approved methods, refer to Chapter 5.
- (2) NATO Unclassified information may be destroyed in any manner prescribed for FOUO.
- (3) Destruction certificates, signed by two (2) properly cleared persons, are required for NATO Secret, Cosmic Top Secret, and all ATOMAL. NATO Secret certificates are maintained for five (5) years; Cosmic Top Secret certificates are maintained for 10 years. ATOMAL certificates are maintained for 10 years for Cosmic Top Secret ATOMAL, five (5) years for NATO Secret ATOMAL, or five (5) years for NATO Confidential ATOMAL.
- (4) NATO Secret, Cosmic Top Secret, and all ATOMAL documents are destroyed at the sub-registry, unless specifically approved for destruction at the control point level. Destruction of these documents may not be further delegated to the user office level.

i. Incident Reporting

Security incidents involving classified NATO information are reported to the sub-registry.

For additional guidance for security violations and infractions refer to Chapter 8.

j. Further Information

Further information about NATO can be obtained from the SSO.

k. Security Classification Guide:

The security classification guides will be updated a minimum of once every five (5) year or upon regulatory changes. The guide will be coordinated at a minimum the guides shall have:

- (1) Identify the subject matter of the classification guide;
- (2) Identify the original classification authority by name and positions, or personal identifier;
- (3) Identify an agency point-of-contact or points-of-contacts for questions regarding the classification guide;

- (4) Provide the date of issuance or last review;
- (5) State precisely the elements of information to be protected;
- (6) State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;
- (7) State, when applicable, special handling caveats;
- (8) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.4 of E.O. 13526; and,
- (9) Prescribe a specific date or event for declassification.

PDSD will consult with the users of the guide and other Subject Matter Experts (SMEs) within USDA when reviewing and updating the guide. PDSD will provide users and subject matter experts 90 days to review and provide input to update the guide. To review a minimum of nine (9) months prior to the five (5) year updates by users and SMEs.

## CHAPTER 5

### SAFEGUARDING CNSI

#### 1. GENERAL SAFEGUARDING REQUIREMENTS

Employees shall be responsible for safeguarding CNSI in their custody or under their control. The extent of protection afforded CNSI shall be sufficient to reasonably prevent the possibility of its loss or compromise. All spaces where CNSI will be stored, processed, or discussed shall be accredited by the SSO, or delegated ISC, and must have an approved SOP, approved by the SSO or delegated ISC. Each accredited facility will have an on-site designated SSC that will be trained and appointed by the SSO in writing. It is preferred that the SSC be separate from the ISC whenever possible to ensure proper oversight and inspection processes. In each case a written delegation from the SSO will name the SSC for the site.

#### 2. WAIVERS

Waivers to the requirements of this DM may be approved only by the SAO, within the guidelines of E.O. 13526. Waivers may be approved for up to three (3) years. Requests to waive requirements cited in this directive will be submitted, in writing, through the agency security office to the SSO for approval from the SAO. Waiver requests shall include sufficient justification to support the request and identification of compensatory measure that will be implemented to mitigate deficiencies. Requests for a waiver must be submitted in writing to the Chief, PDSD 90 days prior to implementing commensurate protective measures 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;
- g. Point of contact, including the person's name, address, telephone number; and
- h. Email address.

#### 3. CONTROL AND ACCOUNTABILITY

##### a. Policy

The SSO, ISC's, and SSC's shall establish an information control system to protect and control the CNSI in their cognizance. The information control system employed shall be

capable of facilitating inspection, auditing, retrieval and disposition with a high degree of accuracy.

b. Cover Sheets

Coversheets are used to protect the need-to-know of CNSI. Their purpose is to shield from inadvertent disclosure and alert observers that there is classified information attached to it. Cover sheets shall be used:

- (1) Top Secret – Must have a cover sheet permanently affixed at all times.
- (2) Secret and Confidential – Must have a cover sheet affixed:
  - (a) Whenever being transmitted via mail or courier; and
  - (b) Whenever being moved in a public or common area within a SWA.
- (3) As a Record of Disclosure – Must include the identity of all persons given access to the information and the date of the disclosure.

c. Accountability for Top Secret

- (1) TSCOs shall be designated by their Agency Head and are responsible for the area to receive, transmit, and maintain access and accountability records for Top Secret information. All Top Secret information shall be entered into a PDSD approved document control accountability system whenever it is received, generated, or dispatched either internally or externally to other approved areas. A 100% inventory shall be conducted at least annually as guided by the SSO or PDSD.
- (2) The transmittal of Top Secret information shall be tracked by a continuous receipt and dispatch process both within and outside the facility.
- (3) Each item of Top Secret material shall be numbered in series. The copy number shall be placed on all copies of Top Secret documents and on all associated transaction documents.

d. Control and Accountability for USDA Generated Products

- (1) Employees must maintain a record of disposition over all USDA generated, either originally or derivatively classified materials.
- (2) The SSC, on behalf of their ISC, or ISC shall maintain a record with shows the disposition of all USDA generated, either originally or derivatively, classified products. There shall be a 100% disposition record for all items at any given time.
- (3) The SSC, or ISC, shall maintain a current list of all derivative classifiers in their respective agency.

- (4) All USDA generated classified products will be tracked by a continuous receipt and dispatch system both within and outside the facility.
- (5) Each USDA generated classified product shall be numbered in series. The copy number shall be placed on all copies and on all associated transaction documents.

#### 4. RECEIVING CLASSIFIED MATERIALS

Procedures shall be established to ensure that CNSI, regardless of delivery method, is received directly by authorized personnel. CNSI should be received by authorized personnel in an accredited SWA. Materials not received electronically shall be examined for evidence of tampering and the classified contents shall be checked against the receipt. If there is no evidence of tampering and no discrepancies and a receipt is included with CNSI it shall be signed and returned to the sender. Discrepancies in the contents of a package or absence of a receipt for CNSI material shall be reported promptly to the sender and to the SSO, ISC or SSC in accordance with Security Incident reporting guidelines (See Chapter 8).

#### 5. CLASSIFIED DISCUSSIONS

All classified discussions must be conducted in an accredited SWA. In such areas all countermeasures and actions prescribed by the approved SOP must be followed before, during, and after classified discussion. There will be no classified discussions over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

#### 6. UNCLASSIFIED SENSITIVE SECURITY INFORMATION

All unclassified sensitive security information (SSI) shall be safeguarded IAW DR 3440-002 on SSI. The information systems that are approved for processing unclassified information shall be physically separated from any classified information systems.

#### 7. STORAGE AND STORAGE EQUIPMENT

This section describes the uniform requirements for the physical protection of CNSI. Where these requirements are not appropriate for protecting specific types or forms of CNSI, compensatory provisions shall be developed by the SSO, ISC or SSC and approved by the SAO. Nothing in this DM shall be construed to contradict or inhibit compliance with any safety or American Disabilities Act (ADA) requirements. The SSO, ISC or SSC shall try to meet appropriate security needs according to the intent of this DM and at an acceptable cost.

##### a. General Services Administration (GSA) Storage Equipment

All CNSI will be stored in a GSA approved security container within an approved SWA.

##### b. Protection of Combinations to Security Containers and SWAs

Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the

level of CNSI authorized for storage. A record must be maintained using an SF-700, Security Container Information form, for each SWA or security container used for storing CNSI.

The SF-700 is then stored in another security container approved for storage with an equal or higher classification level. The SF-700 must be maintained by an ISC or SSO. The combination of a SWA or security container used for the storage of CNSI will be classified at the same level as the highest category of CNSI 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 or SWA 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.

c. SF-700 Instructions

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 or SWA 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 or SWA 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 2(a) of the SF-700 should be stamped with the highest classification of material stored in the container, vault, or area. Part 2(a) should be sealed inside of Part 2 and stored in another security container in a SWA.

d. Changing Combinations

Combinations shall be changed by a person authorized access to the contents of the container or SWA, in coordination with, or by the SSC, ISC, or SSO who maintains the records for access. Combinations shall be changed as follows:

- (1) The initial use of an approved container or SWA for the protection of CNSI;
- (2) Reassignment of personnel to other duties where access is no longer required;

- (3) The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked;
- (4) The compromise or suspected compromise of a container, SWA, or its combination, or discovery of a container or SWA left unlocked and unattended;
- (5) At other times when considered necessary by the ISC or SSO, not to exceed three (3) years; and
- (6) When a combination has been changed, a new SF-700 will be created, stored, and maintained by the ISC or SSO.

e. Opening and Closing of GSA Approved Security Containers and SWAs

An [SF-702](#), *Security Container Check Sheet*, must be affixed to the outside of each security container or SWA utilized for the storage of CNSI. 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 CNSI 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 and SWAs:

- (1) Each time a security container or SWA is unlocked, the individual opening the security container or SWA 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 SWA is left unattended, security containers are locked. The individual locking the security 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 security container or SWA will double check to ensure that the security container or SWA is locked. This individual does not have to possess a security clearance. Preferably, the appropriately cleared person who locked the security container or SWA should be in attendance. Spinning the combination lock several times and pulling on the draw handle or doorknob will help ensure that the security container or SWA is locked. The double check consists of turning the dial one full turn counter-clockwise followed by one full turn clockwise and physically checking each drawer and latch or doorknob. The individual accomplishing the double check annotates the date, time and initials the "CHECKED BY" column of the SF-702.
- (4) Security containers that are used infrequently must be checked daily to ensure they are properly secured and to ensure the integrity of the security container. This includes the security 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 initials and annotates the time in the “CHECKED BY” column of the SF-702.

- (5) A security container should be opened and inspected at least once a month to ensure the proper function of the lock as well as the integrity and contents of the security container has not been altered or compromised.

f. Repair of GSA Approved Security Containers

Repairs, maintenance, or other actions that affect the physical integrity of a GSA approved security container used for storage of CNSI shall be accomplished in accordance with [Federal Standard \(FED-STD\) 809A](#), *Neutralization and Repair of GSA Approved Containers*. Maintenance or repairs are to be accomplished by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers. Repair procedures may be obtained from the SSO.

An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer’s replacement or identical cannibalized parts. A signed and dated certification for each repaired security container, provided by the repairer, shall be on file setting forth the method of repair used.

g. Movement of GSA Approved Security Containers

A GSA approved security container inspected and certified as empty by an SSC, ISC or SSO can be moved like any other item. If the security container must be moved with CNSI inside, or it cannot be verified that there is no CNSI inside then it will only be moved outside of its approved SWA accompanied by a cleared escort and with approval from an ISC or SSO.

## 8. CONSTRUCTION REQUIREMENT

Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, or SWA. SWAs will be constructed and accredited as collateral-level closed storage facilities. Construction and accreditation of a collateral-level, open-storage facility shall be considered only when the volume or bulk of classified material, or the functions associated with processing the classified material, make the use of GSA approved security containers impractical, not for convenience. These criteria and standards apply to all new construction, reconstruction, alterations, modifications, and repairs of existing areas. They will also be used in evaluating existing areas.

Any Agency or Staff Office that desires an open-storage facility must submit a request in writing, through the SSO, to the SAO for approval prior to any construction. The request must identify the need and justification for an open-storage facility and a description of why a closed-storage facility will not provide sufficient protection of CNSI materials. Each request will be reviewed and considered on a case-by-case basis.

All requests for an accredited facility, either open-storage or closed-storage will be reviewed using a risk management analysis. Risk management factors considered will include sensitivity, value and crucial nature of the information, analysis and known and anticipated threats, vulnerabilities, and countermeasures benefits versus cost. Each facility is unique and all operational requirements and the associated risks the facility will play an integral role into the physical security construction requirements for the facility. Agencies or Staff Offices may exceed the standards cited in this directive, but may not lessen them. If an Agency or Staff Office chooses to exceed the standards cited herein, sufficient justification must exist to warrant any increased expenditures. The three (3) core principles will always be considered when evaluating a room for accreditation as a SWA. These three (3) principles are acoustical protection (discussion), physical security (access), technical control and management (electronic devices and computers).

Accredited SWAs that have been approved and are on record at PDSO prior to the publication of this DM will not need to be recertified unless a change has been made that affects the structure and measures in place at the time of the original accreditation, or the standards used for approval of the area are less than those required by this directive. In the latter instance the ISC shall bring the area(s) up to the standards cited herein within one (1) year of the publication of this DM, and the area will be recertified in accordance with this directive. Accreditations will be for a period not to exceed three (3) years. All security inspections taking place will use this standard.

a. Request for SWA Accreditation

When an Agency or Staff Office requires an accredited SWA:

- (1) They will submit a request in writing to their ISC. If there is no ISC assigned, then the request will be submitted to the SSO. The request will include the classification level of the SWA and the operational capabilities (i.e., storage, discussion, processing). Also a Concept of Operations (CONOPS) will need to accompany the request. The CONOPS will contain specific details on the operational needs of the SWA.
- (2) If the SWA is for open-storage, they will submit a request and justification for an open-storage SWA also with a description of why a closed-storage SWA is not appropriate. Open storage areas shall only be approved for operating reasons, not for convenience. Where open storage is requested to satisfy the installation of a CNSI system, unless otherwise justified and approved, the open storage authorization shall be limited to the system only. All documents and removable media will require closed storage in an appropriate GSA-approved security container. All COMSEC/Transient Electromagnetic Pulse Surveillance Technology (TEMPEST) issues should be covered by the OCIO. Also a CONOPS will need to accompany the request. The CONOPS will contain specific details on the operational needs of the SWA.

- (3) For Agencies or Staff Offices with no existing ISC, requests will be submitted to the SSO. Once the facility has been approved, an SSC will be identified and appointed in writing.
- (4) The SSO, in coordination with the ISC, will conduct a site survey of the facility to determine the construction requirements for the SWA based on the request for accreditation and the CONOPS.
- (5) Once the site survey has been completed, and all requested information has been provided, the construction requirements to achieve accreditation will be presented to the ISC.
- (6) An accreditation checklist will be completed and approved by PDSD.

b. Approval Authority

- (1) The SAO is the approval authority for all open-storage SWAs at USDA. The SSO is responsible for coordinating the execution and implementation of the approval.
- (2) The SSO is the approval authority for all Top Secret SWAs. Secret and Confidential closed-storage facilities may be approved by a delegated ISC.
- (3) Upon accreditation of a SWA, the approval authority shall issue a memorandum to the requesting Agency or Staff Office, citing the specific location, building, room number, etc., level of CNSI authorized, any restrictions, and any other information recommended by the SSO.
- (4) A copy of the approval memorandum, Survey Checklist, and SOP shall be maintained by the SSO and within the area by the ISC and/or SSC.

c. SOP

All accredited SWAs will have an approved SOP for the space prior to accreditation. The SOP must be unique to the space and should be created by the ISC and SSC and submitted to the SSO, or delegated ISC, for concurrence. At a minimum, the SOP shall cover the topics identified below, as applicable to the proposed SWA:

- (1) Access control;
- (2) List of authorized unescorted access;
- (3) List of authorized to open/close SWA;
- (4) Day-to-day operations of the SWA;
- (5) Receipt/dispatch of CNSI;
- (6) Storage of CNSI;

- (7) Approved equipment list (i.e., reproduction, destruction);
- (8) Automatic Identification System (AIS) usage;
- (9) Medial control;
- (10) Movement of CNSI;
- (11) Classification management (i.e., cover sheets);
- (12) Top Secret Control Officer procedures;
- (13) Escorting procedures;
- (14) Self-inspection procedures;
- (15) Co-utilization agreements;
- (16) Security incidents;
- (17) Emergency destruction procedures; and
- (18) Modifications/changes to the SWA.

Proposed SOP changes shall be forwarded to the ISC for approval; approved copies will be forwarded to PDSO.

d. Closed Storage Construction Standards

Classified information is secured under conditions adequate to prevent access by unauthorized persons. The requirements specified in this DM represent acceptable security standards. Weapons or sensitive items such as funds, jewels, and precious metals are not to be stored in the same container used to safeguard CNSI. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the ODNI through various Intelligence Community Directives (ICDs).

(1) Standards for storage equipment

Consult GSA supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of CNSI.

(2) Standards for combination locks

New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms shall conform to Federal Specification [\(FF-L\)-2740B](#), *Locks, Combination, Electromechanical*. If the existing non-FF-L-2740B lock fails, the locks are to be replaced with locks meeting FF-L-2740B standards.

(3) Top Secret

Top Secret information is to be stored in a GSA approved security container located in a modular vault, a SWA constructed with [FED-STD 832](#), *Construction Methods and Materials for Vaults*, or in accordance with other construction criteria established by the SSO, and equipped with an Intrusion Detection System (IDS), with personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by Security-In-Depth, or a five (5) minute response time if no Security-In-Depth is in place. Within the U.S. at a closed storage facility, a response force is capable of responding to an alarm within 15 minutes after annunciation and a reserve response force is available to assist the responding force. Response personnel must be appropriately trained and equipped according to SOPs to accomplish initial or follow-up response to situations that may threaten the facility's security.

- (a) Other construction criteria may be established when the intended capabilities of a room or the potential risks do not justify construction of a vault or building to FED-STD 832. Examples of these types of construction include, but are not limited to:
  - 1 Identification of rooms to be used to support Continuity of Operations (COOP) exercises or real-life situations; and
  - 2 Identification of rooms to be used as temporary SWAs which are not utilized for classified purposes on a permanent or regularly occurring basis.
- (b) In these situations, counter-measures to ensure the protection of CNSI must be identified and implemented prior to approval of the facility.
- (c) One (1) or more of the following supplemental controls are in place when Top Secret information is stored in a GSA approved container:
  - 1 Guard or duty personnel possessing a minimum of a final adjudicated secret clearance inspect the security container once every two (2) hours;
  - 2 An Intrusion Detection System (IDS) is in place with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or
  - 3 Security-In-Depth or compensatory measures as determined by the SSO.

(4) Secret

Secret information is stored by one (1) of the following methods:

- (a) In the same manner as prescribed for Top Secret information; or,
- (b) In a GSA-approved security container located in a vault or other approved facility without supplemental controls;

- (c) In a SWA that is approved for the open storage of Secret information; or
  - (d) Security-In-Depth or compensatory measures as determined by the SSO.
- (5) Confidential

Confidential information shall be stored:

- (a) In a GSA-approved security container located in an accredited room; and
  - (b) Have compensatory measures that prevent access to prevent access by unauthorized persons as approved by the ISC or SSO.
- e. Open Storage Construction Standards

Construction and accreditation of a collateral-level, open-storage facility is considered only when the volume or bulk of classified material, or the functions associated with processing the classified material, make the use of GSA approved security containers impractical.

(1) Approvals

Open storage areas are approved based on:

(a) Operational justification

Open storage areas are only approved for operational reasons, not for convenience. Where open storage is requested to satisfy the installation of a classified information system, unless otherwise justified and approved, the open storage authorization is limited to the system only. All documents and removable media still require closed storage in an appropriate security container.

(b) Compliance with construction standards cited in this Manual

An Open Storage Survey Checklist is used to verify that the open storage area meets required standards.

(c) Completion of a SOP Guide for operating the area

An SOP is modified and tailored to suit the specific open storage area.

(d) Receipt of a Facility Approval Memo

The memo is signed by the SAO for the area being approved, specifies the facility being approved, and specifies the maximum level of material authorized for open storage.

## (2) Level of Storage

### (a) Top Secret Storage

An open storage area for Top Secret material meets the construction standards and IDS requirements cited in Section 5. Arrival on-scene to unannounced alarm activations is within 15 minutes from the time the alarm is received at the monitoring station.

### (b) Secret Storage

An open storage area for Secret material meets the construction standards cited in Section 7. In addition, IDS is installed that meets the standards cited in Section 7. Arrival on-scene to unannounced alarm activations is within 30 minutes from the time the alarm is received at the monitoring station.

## (3) General Construction Requirements

These criteria and standards apply to all new construction, reconstruction, alterations, modifications, and repairs of existing areas. These criteria and standards are also used in evaluating existing areas.

All vents, ducts, and similar openings in excess of 96 square inches (11" diameter for circular ducts) that enter a SWA are protected with either bars, or grills, or commercial metal duct sound baffles that meet the appropriate sound attenuation class. If one (1) dimension of the duct measures less than six (6) inches, or the duct is less than 96 square inches, bars are not required; however, all ducts are treated to provide sufficient sound attenuation.

If bars are used, the bars are a minimum of ½" diameter steel welded vertically and horizontally six (6) inches on center; if grills are used, the grills are a minimum of 13-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms are permanently installed metal and no farther apart than six (6) inches in one (1) dimension. A deviation of ½" in vertical and/or horizontal spacing is permissible. An access port to allow visual inspection of the protection in the vent or duct may be installed inside the secure perimeter of the SWA. If the inspection port is installed outside the perimeter of the SWA, it is locked.

## (4) Doors

Routine entrance/exit doors are kept to an absolute minimum. Where possible, only a single door is used for routine entry/exit.

Doors are constructed substantially of wood or metal. When doors are used in pairs, or a gap exposes the latching mechanism, an astragal (overlapping molding) is installed where the doors meet or exposure occurs. It is preferred that hinges be on the secure side of the door. Hinge pins that are exposed to the outer perimeter of the area are pinned, brazed, or spot-welded to preclude removal.

(a) All doors shall meet the following criteria:

- 1 Solid core wood, minimum 1¾” thick, natural wood veneer, installed in welded steel frame assembly mounted to 14-gauge metal studs. Knock-down (collapsible jam and header) frame or aluminum frame is not acceptable.
- 2 Doors and frames meet or exceed a Sound Transmission Class (STC) 45 equivalent rating in processing areas. Doors and frames meet or exceed an STC 50 equivalent rating in areas where there will be amplified sound. Doors have adjustable acoustical gasket around the door with an automatic threshold seal installed in these instances.
- 3 Doors with windows, louvers, baffle plates, or similar openings are only authorized to be used in areas with no processing or discussion. These items are secured with 13-gauge expanded metal securely fastened on the inside. If visual access is a factor, any windows are covered.

(b) Doors are equipped with an industrial Grade 1 automatic door closer.

(c) For new construction or renovation, entrance doors are secured with a GSA approved, built-in combination lock meeting Federal Specification FF-L-2740B. Other high security locks may be used on a case-by-case basis with the approval of the SSO. Other doors are secured from the inside with a panic bolt (which can be actuated by an alarmed panic bar); a dead bolt; a rigid wood or metal bar (that precludes “springing”), which extend across the width of the door and is held in position by solid clamps, preferably on the door casing; or by other means approved by the SSO, consistent with relevant fire and safety codes.

(d) Routine entrance doors are additionally equipped with a supplemental access control device (e.g., key lock, lever set, card reader, cipher lock, etc.), to control access into the area during working hours. Supplemental access control devices are for access control purposes only and do not provide sufficient security for an unattended open storage area.

(e) All door hardware meets Grade 1 standards.

(f) All key locks meet Underwriters Laboratories (UL) 437 standards.

(5) Windows

Every effort should be made to construct open storage areas without windows. Where the presence of windows is unavoidable, windows are covered by opaque window film, or by blinds turned to no more than a 45 degree angle, permanently fastened at top and bottom, and not adjustable by the user. The ability to open the window is eliminated by either permanently sealing it or installing a locking mechanism on the inside. Windows that open and are less than 18 feet from grade or adjacent roofs, less than 14 feet from other structures, trees, or horizontal openings,

or less than three (3) feet from openings on the same wall that are not part of the open storage space require one (1) of the following:

- (a) Vertical round iron or steel bars, a minimum of ½” diameter spaced six (6) inches on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support.
- (b) Vertical flat iron or steel bars, a minimum of 1½” x 3/8” spaced six (6) inches on center. The bars may be mortised into the masonry, built into the frame, or equipped with horizontal crossbars for added strength and support

Note: All fasteners are welded or specially manufactured to prevent removal.

#### (6) Walls

Walls, true floor, and true ceiling are permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, is done in such a manner as to provide visual evidence of unauthorized penetration. Walls, true floors, and true ceilings are uniformly painted to show evidence of unauthorized penetration.

Construction is of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method is devised to prevent the removal of such panels without leaving visual evidence of tampering.

The perimeter walls of the open storage area are true floor to ceiling or, sufficiently modified to represent a secure enclosure. When wall barriers do not extend to the true ceiling and a false ceiling is created, walls are permanently constructed to extend above the false ceiling to the true ceiling using the same building materials as the existing walls.

If there is a threat of forced entry (to include high crime areas) as determined by the physical security representative, walls are reinforced, slab-to-slab, with 13-gauge expanded metal. The expanded metal is spot welded, or fastened by every six (6) inches to vertical and horizontal metal supports of 14-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling, approved by the SSO.

#### f. Acoustic Controls

Acoustic controls are designed to protect conversations from being overheard outside the SWA. Acoustic controls are not intended to prevent a positive audio attack. SWA perimeter walls, doors, windows, floors, and ceilings, as well as all openings such as vents and ducts, provide sufficient acoustic control measures to preclude inadvertent disclosure of conversation. This can be achieved through structural enhancements or sound masking if construction or budget restraints prevent structural enhancements from being feasible.

The ability of a SWA to retain sound within the perimeter is rated using a descriptive value, the STC. All SWAs meet the equivalent of Sound Group III – STC 45 or better. STC Group IV – STC 50 or better is required for amplified sound (e.g., secure video teleconferencing, speaker phone).

- (1) Sound Group III STC 45 or better. Loud speech from inside the room can be faintly heard but not understood from outside the room. Normal speech is unintelligible.
- (2) Sound Group IV STC 50 or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume can be heard only faintly or not all.

In certain cases there may be a sufficient stand-off distance between a perimeter wall and the operational area, to prevent sound from carrying beyond the perimeter wall. The SSO may waive the STC construction requirement if the STC 45 equivalent rating can be achieved through stand-off distance. The stand-off distance is subject to inspection, and the area designated as a no discussion area. Areas containing amplified sound are built out to an STC 50 equivalent sound rating.

Examples of sound masking include installation of a Compact Disk (CD) or audio tape player with separate speakers; white noise generators; or other vibrating or noise generating systems that can be installed along the inside perimeter of the area. Where sound traverses through vents, ducts, and other similar openings, install music speakers in or near the opening, or white noise generators in or near the opening. When planning a retrofit, sound masking may be the most cost effective option to meet the acoustic control requirements.

Examples of structural enhancements include the use of sound deadening high-density materials in wall construction; use of extra layers of drywall for wall construction; and use of door gaskets for doorframes. Where sound traverses through vents, ducts, and other similar openings, consider installing commercial sound baffles or waveforms. The installation of Z ducts is an effective method of protecting Heating, Ventilation, and Air Conditioning (HVAC) systems. When planning new construction, structural enhancements should be used to meet the acoustic control requirements.

Testing is performed at the completion of construction to ensure that the required STC level's equivalent has been met. The test is designed to ensure that classified national security information is protected from inadvertent disclosure and compromise. It is important that the test reflects the operational context of the area, the equipment to be deployed and the facilities' security-in-depth.

g. Radio Frequency (RF) Shielding

RF shielding is not normally required in SWAs unless otherwise required by the SSO.

h. IDS

The IDS and related components complies with this DM, the UL 2050 and UL 681 Extent 3 standards. Facilities maintain a current National Industrial Security Systems (CRZH) UL certificate of installation and services. The UL listed Alarm Service Company is responsible for completing the National Industrial Security Alarm Description Worksheet.

(1) Certificate of Compliance

Evidence of compliance with the requirements of this DM consists of a valid UL certificate for the appropriate category of service. This certificate is issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company is:

- (a) Listed as furnishing security systems of the category indicated;
- (b) Authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the category of service; and
- (c) Subject to the UL Field Counter Check Program, whereby periodic inspections are made of representative alarm installations by UL certified personnel to verify the correctness of installation practices.

(2) UL certificate (CRZH) exemptions

If the component constructs and operates its own non UL listed monitoring station, the component Monitoring Station meets the construction and operational standards of a Government Contractor Monitoring Station as outlined in UL 2050. The IDS installation is accomplished by an alarm installation company that is certified by UL 2050 for compliance and the dedicated staff of trained physical security technicians that provide everyday maintenance and repair of the IDS system.

The IDS is connected to, and monitored by, a UL listed monitoring station unless approved otherwise by the SSO. The approval authority approves contingency protection procedures in the event of IDS malfunction.

(3) IDS Requirements

(a) Independent Equipment

When many alarmed SWAs are protected by one (1) monitoring station, SWA zones are clearly distinguishable from the other zones to facilitate a priority response. All sensors are installed within the protected area.

(b) Premise Control Unit (PCU)

No capability should exist to allow changing the access status of the IDS from a location outside the protected area without prior approval of the SSO. All PCUs (alarm panel) are located inside the SWA. Assigned personnel initiate all changes in access and secure status. Operation of the PCU is restricted by use of a keypad and/or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space causes an alarm to be transmitted to the monitor station.

(c) Backup Power

Emergency backup electrical power is provided by battery, generator or both. If batteries are used, the batteries provide a minimum of 24 hours of backup power.

(d) Keypads

All alarm keypads are located inside the SWA next to the primary entry/exit door.

(e) Motion Detection Protection

Motion detectors are a UL 639 listed device. SWAs that reasonably afford access to the container or area where classified data is stored are protected with motion detection sensors (i.e., ultrasonic, passive infrared, etc.). Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector causes an immediate and continuous alarm condition.

(f) Protection of Perimeter Doors

Each perimeter door is protected by a UL 634 listed Level 2, High Security Switch (HSS). The HSS removal tamper is monitored 24 hours a day regardless if the system is in the access or secure mode of operation.

(g) Protection of Emergency Exit-Doors

Each perimeter emergency exit-door is protected by a UL 634 listed Level 2, HSS and monitored 24 hours a day regardless if the system is in the access or secure mode of operation.

(h) Entrance Door Delay

Entrance door sensors have an initial time delay to allow for change in alarm status, but not to exceed 30 seconds.

(i) Windows

All readily accessible windows below 18 feet are protected by an appropriate intrusion detection unit installed to signal breakage or penetration of the window

or movement of an intruder in the vicinity of the window. Additionally an HSS is used on windows that are movable.

(j) Duress

A minimum of one (1) continuously alarmed duress button is recommended in all SWAs.

(k) False and/or Nuisance Alarm

Any alarm signal transmitted in the absence of a detected intrusion, 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 designed but which is not related to an intrusion attempt. All alarms are investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms do not exceed one (1) in a period of 30 days per zone.

(l) IDS Testing

The IDS is tested annually to provide assurance that the IDS system is in conformance with this Instruction. U.S. citizens shall accomplish all IDS testing. Testing shall be coordinated with the Office of Operations (OO), Physical Operations Division (POD), by the ISC and/or SSC. Results shall be stored for a minimum of two (2) years after the date of testing.

(m)IDS Personal Identification Number (PIN) codes

IDS PIN codes are FOUO, and require additional protection from disclosure. The codes are not transmitted over unsecure phone lines or unencrypted/non-password protected email. Individual PIN codes are assigned to each user. Shared PIN codes are not authorized.

(n) Central Monitoring Station

- 1 The central monitoring station may be located at the facility of a UL listed:
  - a Government contractor monitoring station, formerly called a proprietary central station;
  - b National industrial monitoring station;
  - c Central station that complies with the UL 827, Standard for Central-Station Alarm Services;
  - d Cleared commercial central station;

NOTE: For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

- e Secret-cleared U.S. citizens who are trained alarm monitors are in continuous attendance in sufficient numbers to supervise and operate each alarmed area;
- f Trained alarm monitors are in attendance at the alarm monitoring station at all times when IDS is in operation;
- g The central monitoring station is required to indicate whether or not the system is in working order and to indicate tampering with any element of the systems. Necessary repairs are made as soon as practical. Until repairs are completed, periodic patrols are conducted at four (4) hour intervals for Secret areas and two (2) hour intervals for Top Secret areas during non-working hours, unless an appropriately cleared employee is stationed at the alarmed site;
- h When IDS is used, it is activated immediately at the close of business at the alarmed area or container. A record is maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate is reviewed by the central monitoring station and, upon appropriate determination, referred to the appropriate security official for investigation. Such records are maintained in accordance with the General Records Schedule; and
- i Records are maintained for one (1) year indicating time of receipt of alarm; name(s) of security force personnel responding; time dispatched to facility area; time security force personnel arrived; nature of alarm; and what follow-up actions are accomplished.

(o) Response to Alarms

- 1 The following resources may be used to investigate alarms:
  - a Proprietary security force personnel;
  - b Central station guards; or
  - c Subcontracted guard services.
- 2 When the IDS is in operation, a sufficient number of properly trained proprietary security force personnel, cleared to the appropriate level of the area, are available at all times to be immediately dispatched to investigate each alarm.
- 3 Response personnel are cleared only if they have the ability and responsibility to access the area or container(s) housing the classified material (i.e., combinations to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material).

- 4 Uncleared guards may be dispatched by a signaling service station, or residential monitoring station to an alarm. However, agency-developed response plans include notification to a cleared representative of the affected facility for each alarm annunciation. If alarm activation resets in a reasonable amount of time and no physical penetrations of the SWA or container are visible, then entrance into the area or container is not required. The uncleared guards remain on the premises until a designated, cleared representative of the facility arrives, or as instructed by the cleared facility representative.
- 5 If the alarm activation does not reset or physical penetration is observed, then a cleared response team is dispatched. The initial uncleared response team stays on station until relieved by the cleared response team.
- 6 Subcontracted guards are under contract with either the central monitoring station or the cleared facility.
- 7 The agency requires a 15 minute response time for Top Secret level open-storage areas, and a 30 minute response time for Secret level open-storage areas. Arrangements are made with the monitoring station to immediately notify a cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.
- 8 The items listed below are some examples of security in-depth features. Security in-depth features are evaluated by the SSO on a case-by-case basis:
  - a Military installations, embassy compounds, or contractor compounds with a dedicated response force of U.S. personnel. A Memorandum of Agreement is executed outlining response requirements for these facilities.
  - b Enclosed vestibule outside of an SWA entrance equipped with an approved high security lock and UL listed alarm equipment installed in accordance with manufacturer's instructions.
  - c Separate building access controls/alarms along with elevator controls (e.g., after hours card reader or PIN with audit capability) are required to gain access to building or elevator.
  - d Fenced, alarmed compound with access controlled vehicle gate and/or pedestrian gate.

(p) Exceptional Cases

- 1 If the requirements set forth above cannot be met due to extenuating circumstances, SSO approval shall be requested for an alarm system that is:

- a Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization; or
  - b Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the component, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization.
- 2 Police department response systems may be requested only when the SWA is located in an area where:
  - a Central control station services are not available with line security and/or proprietary security force personnel, or a contractually dispatched response to an alarm signal cannot be achieved within the time limits required.
  - b It is impractical for the component to establish a proprietary guard force at the location. In these instances, an installation proposal, explaining how the system would operate, is submitted to the SSO. The proposal includes sufficient justification for granting an exception and the full name and address of the police department that will monitor the system and provide the required response. The name and address of the UL listed/UL certified company that is installing the system, and inspecting, maintaining, and repairing the equipment is also furnished. The facility requests a 15 minute response time from the police department for Top Secret level open-storage areas, and a 30 minute response time for Secret level open-storage areas. Arrangements are made with the monitoring station/police to immediately notify a cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material. In exceptional cases where central station monitoring service is available, but no proprietary security force of central station or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of response is available, the SSO may approve cleared employees as the sole means of response.
  - c Continuous operations facilities may not require IDS. This type of secure area should be equipped with an alerting system if occupants cannot observe all potential entrances into the room. Duress devices may also be required.

i. Restricted Areas

When it is necessary to control access to CNSI in an open area during working hours, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect CNSI because of its size, quantity or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All CNSI will be secured during non-working hours in approved repositories or secured using other methods approved by the SSO.

j. Portable Electronic Devices (PEDs)

PEDs shall not be introduced into any SWA without written approval from the SSO. Approvals will be considered only when the risk associated with the use of such equipment are clearly identified and sufficiently mitigated. Restrictions on the introduction of PEDs into SWAs shall be prominently posted and included in the SOP.

A PED is defined as any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition includes but is not limited to, laptops, pocket Personal Computers (PCs), palmtops, media players, memory sticks/thumb drives, cellular telephones, PEDs with cellular phone capabilities, and pagers. To find out if a device is approved or for a more complete and up to date list of prohibited items please contact your ISC.

(1) All PEDs, with the exception of the following, are prohibited within an approved facility:

- (a) Electronic calculators, spell checkers, language translators;
- (b) Receive-only pagers;
- (c) Audio and video playback devices;
- (d) Receive-only radios;
- (e) Infrared (IR) devices that convey no intelligence data (text, audio, video, etc.), such as an IR mouse and/or remote controls; or
- (f) Medical, life and safety portable devices.

k. End of Day Security Checks

SSO's, ISC's, and SSC's responsible for an accredited SWA shall establish a system of security checks to be completed at the close of each working day. Site specific security checks will be identified in the approved SOP. The [SF-701](#), Activity Security Checklist, is the required form for documenting these checks.

SSO's, ISC's, and SSC's that operate "multiple work shift" accredited SWAs shall ensure that employees perform the security checks at the end of the last working shift in which CNSI was removed from storage for use. The checks will be conducted according to the approved SOP. The SF-701 is the required form for documenting these checks.

l. Perimeter Controls

SSO's, ISC's, and or SSC's responsible for accredited SWAs shall establish and maintain a system to deter and detect unauthorized introduction or removal of CNSI from their facility. The objective is to discourage the introduction or removal of CNSI without proper authority.

All persons who enter or exit a SWA shall be subject to an inspection of their personal effects in order to deter the unauthorized removal of classified material and the introduction of prohibited items or contraband, except under circumstances where the possibility of access to CNSI is remote, to be determined by the SSO. Inspections shall be limited to buildings or areas where classified work is being performed. Failure to comply with a request for inspection may result in adverse security actions, to include the suspension of access to CNSI and the loss of a security clearance. Notification of this requirement shall be conspicuously posted at all pertinent entries and exits.

The extent, frequency, and location of entry and exit inspections shall be accomplished in a manner consistent with the approved SOP and operational efficiency.

m. Emergency Procedures

The SSO, ISC's, and SSC's responsible for accredited SWAs shall develop procedures for safeguarding CNSI in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to potential emergencies. ISC's and SSC's responsible for accredited SWAs shall immediately report to the SSO any emergency situation that renders the facility incapable of safeguarding CNSI.

9. TRANSMISSION

a. Transmission and Transportation

Classified material shall be transmitted in a manner that prevents loss or unauthorized access. The preferred method for transmission of CNSI at the USDA is the secure fax or secure email (i.e., Homeland Secure Data Network [HSDN], Joint Worldwide Intelligence Communication System [JWICS]). The secure fax consists of a combination of secure terminal equipment (STE) and a fax machine approved for the transmission of CNSI. The HSDN is a secret collateral system maintained by the Department of Homeland Security (DHS). The JWICS is a Top Secret/SCI system maintained by the ODNI. USDA is a subscriber to both systems. HSDN is owned by OHSEC and managed by the OCIO. JWICS is owned and managed by OHSEC.

b. Preparation and Receipting

- (1) CNSI to be transported outside of a facility shall be enclosed in opaque inner and outer envelope. The inner envelope shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer envelope shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner envelope; except that confidential information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee and the document, but shall contain no CNSI. It shall be signed by the recipient and returned to the sender. Form AD-471 shall be used at the receipt for all CNSI materials.
- (2) A suspense system will be established by the SSC, ISC, and SSO to track transmitted documents until a signed copy of the receipt is returned.
- (3) In the event that a receipt of shipment of material is not returned within 30 days, a tracer action shall be initiated.
- (4) When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit. This method requires review by and ISC or SSO and approval from the SSO.
- (5) All classified material must be prepared, reproduced and packaged by cleared personnel only, and only in approved areas.

c. Top Secret Transmission Outside of a Facility

Written authorization of the SSO or designated ISC is required to transmit Top Secret information outside of the facility. Top Secret material may be transmitted by the following methods within and directly between the U.S. and its Territorial Areas:

- (1) The Defense Courier Service (DCS);
- (2) Department of State Courier System (also known as a diplomatic pouch);
- (3) A two (2) person designated courier or escort cleared for access to Top Secret information as advised by the SSO; and
- (4) By electronic means over National Security Agency approved cryptographic communications systems (i.e., secure phone/fax, approved classified email such as HSDN or JWICS).

d. Secret Transmission Outside of a Facility

Secret material may be transmitted by one (1) of the following methods within and directly between the U. S. and its Territorial Areas:

- (1) By the methods established for Top Secret;

- (2) U.S. Postal Service (USPS) Express Mail and USPS Registered Mail (to be received only by appropriately and accessed personnel);

NOTE: The “Waiver of Signature and Indemnity” block on the USPS Express Mail Label 11-B, may not be executed and the use of the external (street side) express mail collection boxes is prohibited.

- (3) A cleared commercial carrier;
- (4) A cleared commercial messenger service engaged in the intra-city/local area delivery (same day delivery only) of classified material;
- (5) A commercial delivery company approved by the SSO, that provides nation-wide, overnight service with computer tracking and reporting features. Such companies need not be security cleared;
- (6) By electronic means over NSA approved cryptographic communications systems (i.e., secure phone/fax, approved classified email such as HSDN or JWICS); or
- (7) Other methods as directed in writing by the SSO.

e. Confidential Transmission Outside of a Facility

Confidential material shall be transmitted by the methods established for Secret material, except that a commercial carrier does not have to be cleared, or by USPS Certified Mail.

f. Transmission Outside of the U.S. and U.S. Territorial Areas

CNSI may be transmitted to a U.S. Government entity outside the United States or a U.S. Territory only under authorization of the ISC or SSO.

Top Secret material may be transmitted by the DCS, Department of State Courier System, or a courier service authorized by the SSO.

Secret and Confidential material may be transmitted by:

- (1) Registered mail through U.S. Army, Navy, or Air Force postal facilities;
- (2) By an appropriately cleared employee with courier authorization and training; or,
- (3) As authorized by the SSO.

If there information sharing agreements or other agreements that have been signed by both the SAO and the foreign government, which establishes procedures for transmitting CNSI those should be followed. These agreements shall not contain measures that are less than what is identified in E.O. 13526.

g. Addressing Classified Material

Mail or shipments containing CNSI shall be addressed to an approved classified mailing address of the facility. An individual's name shall not appear on the outer cover. This does not prevent the use of office code letters, numbers, or phrases in an attention line to aid in internal routing.

When it is necessary to direct Secret or Confidential material to the attention of a particular individual, other than as prescribed below, the identity of the intended recipient shall be indicated on an attention line placed in the letter of transmittal or on the inner container or wrapper.

When addressing Secret or Confidential material to an individual operating as an independent consultant, or to any facility at which only one (1) employee is assigned, the outer container shall specify: "TO BE OPENED BY ADDRESSEE ONLY" and be annotated: "POSTMASTER-DO NOT FORWARD. IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER."

h. Transporting within a Facility

CNSI may be transmitted within a facility without double-wrapping provided adequate measures are taken to protect the material against unauthorized disclosure. The individual must have training from the SSO, ISC, or SSC to ensure proper documentation and action.

For all hand carrying of Top Secret material, a two (2) person courier team shall be used unless a single-person courier has been approved by PDSO.

i. Use of Couriers, Hand Carriers, and Escorts

Designated cleared employees as couriers, hand carriers, and escorts shall ensure:

- (1) They are approved by an SSO in writing with a yearly recertification;
- (2) They have completed courier training and signed a courier agreement;
- (3) They are briefed on their responsibility to safeguard CNSI;
- (4) They possess an identification card or badge which contains the employee's name;
- (5) The employee retains CNSI in his or her personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability, if needed; and
- (6) If the classified material is being hand-carried to a classified meeting or on a visit, an inventory of the material shall be made prior to departure. A copy of the inventory shall be carried by the employee. On the employee's return to the facility, an

inventory shall be made of the material for which the employee was charged by the SSC, ISC, SSO or other delegated and documented individual.

- (7) If any problems are encountered while in route (i.e., losses or other incidents), they shall immediately be reported to the ISO.

j. Use of Commercial Passenger Aircraft for Transporting Classified Material

Classified material may be hand-carried aboard commercial passenger aircraft by cleared employees with the approval of the SSO. Before any movement of classified assets, a transportation plan shall be developed and approved by PDSD a minimum of 30 days prior to the transport.

The SSO shall provide employees with written authorization to hand carry CNSI on commercial aircraft. The written authorization shall:

- (1) Provide the full name, date of birth, height, weight, and signature of the traveler and state that he or she is authorized to transmit classified material;
- (2) Describe the type of identification the traveler will present on request;
- (3) Describe the material being hand carried and request that it be exempt from opening;
- (4) Identify the points of departure, destination, and known transfer points;
- (5) Include the name, telephone number, and signature of the SSO, and the location and telephone number of the SSO or ISC.

k. Use of Escorts for Classified Shipments

If an escort is necessary to ensure the protection of the CNSI being transported, a sufficient number of escorts shall be assigned to each classified shipment to ensure continuous surveillance and control over the shipment while in transit. Specific written instructions and operating procedures shall be furnished escorts prior to shipping and shall include the following:

- (1) Name and address of persons, including alternates, to whom the classified material is to be delivered;
- (2) Receipting procedures;
- (3) Means of transportation and the route to be used;
- (4) Duties of each escort during movement, during stops while in route, and during loading and unloading operations; and
- (5) Emergency and communication procedures.

## 10. REPRODUCTION

SSOs, ISCs and SSCs shall establish written reproduction procedures; a control system to ensure that reproduction of CNSI is held to the minimum consistent with operational requirements. Classified reproduction shall be accomplished by authorized personnel knowledgeable of the procedures utilizing reproduction equipment approved by the ISC/PDSD. These persons will be given training from the SSO, ISC or SSC that has been approved by the SSO. All persons who are approved for reproduction will sign an acknowledgment that they understand their responsibility and the SSO, ISC or SSC will keep a list of all personnel approved for reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

### a. Protection

Reproduced copies of classified documents shall be subject to the same protection as the original documents.

- (1) Risk managed download procedures shall be in place and followed for copying Unclassified or lower classified information from a classified information system.

### b. Marking reproductions

All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

### c. Records

SSOs, ISCs or SSCs shall maintain a record of the reproduction of all Top Secret material for two (2) years.

### d. Reproduction Equipment

The reproduction equipment shall be positioned to assure immediate and positive monitoring. A notice indicating whether or not equipment can be used for reproduction of classified material shall be posted. All procedures, to include the clearing of equipment, accessing of operators, clearing of media and handling malfunctions, shall be approved in writing by the ISC/PDSD. Reproduction equipment may only be used outside an approved area, such as a temporary secure working area (TSWA), must be approved by the PDSD.

## 11. DISPOSITION

All CNSI is to be properly safeguarded and accounted for at all times. Top Secret materials must be controlled through the Top Secret Control Officer. All USDA generated CNSI must be accounted for at all times. It is recommended that inventories of CNSI be maintained so that an accurate accounting of CNSI holdings is easily attainable. Disposition

recommendations, by categories of information, or document control number, when required, shall be submitted to the SSO and contracting officer for concurrence.

## 12. RETENTION

CNSI that is no longer needed shall be processed for appropriate disposition. CNSI approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the CNSI or material.

The SSO, ISC or SSC shall establish procedures for review of their classified holdings on a recurring basis to reduce these classified inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and classified waste shall be destroyed as soon as practical after they have served their purpose. Any appropriate downgrading and declassification actions shall be taken on a timely basis to reduce the volume and to lower the level of classified material being retained.

Upon contract close-out, all requests for retention of classified information shall be submitted to the government Contracting Officer through the PDS/SSO for review and approval.

## 13. DESTRUCTION

Employees shall destroy classified material in their possession as soon as possible after it has served the purpose for which it was originally retained, developed or prepared. All destruction procedures shall be reviewed and approved by PDS.

### a. Methods of Destruction

The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, chemical decomposition or pulverizing. The preferred method within USDA is shredding for paper, CDs and Digital Versatile Discs (DVDs). The use of any other method must be approved by the SSO prior to being implemented. Any machinery used to destroy CNSI must be listed on the National Security Agency's Evaluated Product List (EPL). If equipment requires replacing or requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for any destruction of CNSI. The EPL may be obtained from the SSO.

Classified material in microform; that is, microfilm, microfiche, or similar high data density material; must be destroyed in an approved method after contacting the SSO and is not to be shredded unless directed by the SSO. No other forms of destruction will be used without written authorization from the SSO prior to the destruction of the media.

Larger items such as equipment, laptops, desktops and internal components such as hard drives that are no longer required, which hold CNSI data, are to be transferred to OCIO/Agriculture Security Operations Center (ASOC) and turned over to Classified Material Conversion (CMC) at the National Security Agency. Custody of these items is to be transferred from the owning agency, through the ISC, to the SSO for destruction,

using form [AD-471](#), Classified Document Accountability Record. The SSO may also provide written guidance for unusually large items, and will assist with the coordination.

b. Witness to Destruction

Accountable classified material shall be destroyed by authorized personnel who have a full understanding of their responsibilities. For destruction of Top Secret material, two persons are required. For destruction of Secret and Confidential material, one (1) person is required.

c. Destruction Records

Destruction records are required for Top Secret material. The records shall indicate the date of destruction, identify the accountable material destroyed, and be signed by both of the individuals designated to destroy and witness the destruction, immediately following the completion of the destruction. At the SSC's or ISC's discretion, the destruction information required may be combined with other required control records. Destruction records shall be maintained for two (2) years.

d. Classified Waste

Classified waste shall be destroyed as soon as practicable. This applies to all waste material containing CNSI. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material. Classified waste residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed.

#### 14. COMSEC

COMSEC information shall be controlled and protected in accordance with applicable national policy, DOD issuances, and USDA/OCIO regulations. Security classification and declassification policies of this DM apply to COMSEC information in the same manner as other CNSI, except only National Security Agency (NSA)/Central Security Service (CSS) is authorized to declassify COMSEC information.

#### 15. INFORMATION SECURITY SYSTEMS

Information systems that are used to capture, create, store, process or distribute CNSI must be properly managed to protect against unauthorized disclosure of CNSI, loss of data integrity to ensure the availability of the data and system.

Protection requires a balanced approach including information system security features that include, but are not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the information system are required.

a. Responsibilities

OCIO is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process CNSI at USDA.

b. Assessment & Authorization

- (1) Assessment is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The assessment process subjects the system to appropriate verification that protection measures have been correctly implemented. The OCIO/DAA shall review and certify to the SAO that all systems have the appropriate protection measures in place and validate that they provide the protection intended. The SAO may conduct an onsite assessment to validate the OCIO/DAA review and certification of the information system.
- (2) The accreditation of an information system is the official management decision to permit operation of an information system in a specified environment at an acceptable level of risk, based on the implementation of an SAO approved set of technical, managerial and procedural safeguards. All information system certifications shall be reviewed and the information system accredited to operate by the SAO.
- (3) The OCIO/DAA may grant interim approval (temporary authority) to operate an information system. Interim approval to operate may be granted for up to 180 days with an option for the OCIO/DAA to extend the interim approval for an additional 180 days. SAO approved protection measures shall be in place and functioning during the period of interim approval.
- (4) Information systems shall be reaccredited whenever security relevant changes are made to the accredited information system. Proposed modifications to an information system shall be reviewed by the OCIO/DAA to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system's environment change, if the applicable information system protection requirements change, or if the protection mechanisms implemented for the system change, the system shall be reaccredited. During the reaccreditation cycle, the OCIO/DAA may grant an interim approval to operate the system.
- (5) All modifications to security relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security relevant changes shall be subject to the provisions of the system configuration management program. The OCIO/DAA shall notify the SAO of requests for changes to the resources that deviate from the requirements of the approved System Security Plan (SSP). The OCIO/DAA shall determine if system reaccreditation is required.

- (6) Each information system shall be re-evaluated for reaccreditation every three (3) years. Such review involves a determination by the OCIO/DAA that the conditions under which the original accreditation was granted still apply. If the accreditation remains valid, the accreditation originally furnished by the OCIO/DAA need only be annotated that the re-evaluation was conducted and the date of the re-evaluation.
- (7) The OCIO/DAA shall evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change:
  - (a) Levels of concern;
  - (b) Protection level;
  - (c) Technical or nontechnical protection measures;
  - (d) Vulnerabilities;
  - (e) Operational environment;
  - (f) Operational concept; or
  - (g) Interconnections.
- (8) The OCIO/DAA shall withdraw system accreditation and ensure proper sanitization when the system is no longer required to process CNSI, or if the operational need for the system no longer outweighs the risk of operating the system.
- (9) The SAO will be notified and an accreditation will become invalid immediately whenever detrimental, security significant changes occur to any of the following:
  - (a) The required protection level;
  - (b) The operational environment; or
  - (c) The interconnections.
- (10) If two (2) or more similar information systems are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the information system, the information system configurations are essentially the same, and the physical security requirements are similar), a Master System Security Plan (MSSP) may be written by the OCIO/DAA, certified by the OCIO/DAA to cover all such information systems. The information system covered by an MSSP may range from stand-alone workstations up to and including multi-user information system and local networks that meet the criteria for a MSSP approach. This type of approval applies only to systems operating at protection Levels 1 and 2.

c. MSSP

The MSSP shall specify the information required for each certification for an information system to be accredited under the plan.

d. Information System Certification Report (ISCR)

An ISCR shall contain the information system identification and location and a statement signed by the OCIO/DAA certifying that the information system implements the requirements in the MSSP.

e. System Accreditation

The OCIO/DAA shall accredit the first information system under the MSSP. All other information systems to be operated under the MSSP shall be certified by the OCIO/DAA as meeting the conditions of the approved MSSP. This certification, in effect, accredits the individual information system to operate under the MSSP. A copy of each certification report shall be retained with the approved copy of the MSSP.

f. Recertification

An information system certified under an MSSP will remain certified until the MSSP is changed or three (3) years have elapsed since the information system was certified. If either the levels of concern or protection level described in the MSSP change, the MSSP shall be re-accredited by the SAO and all information systems certified under the MSSP shall be re-certified by the OCIO/DAA in coordination with the SAO.

g. Comingling of Unclassified and Classified Systems

Each location must have a technical review that addresses the risks associated with comingling classified and unclassified systems in a SWA. This review will address the specific technical concerns associated with having systems with different levels of risk co-located; and shall be documented and addressed in a co-utilization agreement. The co-utilization agreement must be reviewed and approved by the SSO and Information Assurance Manager (IAM).

## CHAPTER 6

### VISITS AND MEETINGS

#### 1. SENDING CLEARANCE FOR A CLASSIFIED VISIT

To pass a clearance to an organization outside of USDA, form [AD-1189](#), Request to Pass a Security Clearance, must be filled out and sent to PDSO at least 72 hours before the beginning of the event for which the access is required. The AD-1189 must be signed by the supervisor. Exemptions for this requirement apply to Deputy Under Secretaries, Under Secretaries and the immediate Office of the Secretary. All clearance verifications will be sent directly from PDSO to the receiving organization's security office and may not go through an intermediary.

In the event of a cancellation or termination of a visit request, the ISO/SSO, or their designated representative shall be notified immediately.

##### a. Visit Access request (VAR)

When sending a classified visit request the following information must be included:

- (1) Last name;
- (2) First Name;
- (3) Middle initial;
- (4) Social Security Number (SSN);
- (5) Level of access required for meeting, event, etc.;
- (6) Date of most recent investigation (investigation closed date);
- (7) Type of most recent investigation;
- (8) Agency/Office that granted access;
- (9) Date(s) of visit;
- (10) Purpose of visit;
- (11) The Point of Contact (POC) of the individual at the receiving Agency or Office that can be contacted by the receiving security office; and
- (12) Security office POC to include:
  - (a) Full name;
  - (b) Office phone number;

(c) Office fax number; and

(d) Email address.

b. Duration of Visit Limitations

A clearance shall only be passed for as long as the individual requires access at the location/agency. 12 month visit certifications are not authorized unless approved in writing by the SSO or designee.

A passed clearance cannot extend past the scope of the investigation (five [5] years for Top Secret, 10 years for Secret). If an investigation goes out of scope and the individual still requires access then as long as a new investigation is open at the Office of Personnel Management (OPM), monthly visits can be sent until the investigation comes back.

Passed clearances will be maintained by PDSD or delegated offices for two (2) years from the date the clearance was sent. They can be either hard copy or digital.

2. RECEIVING CLEARANCE FOR A CLASSIFIED VISIT

For non USDA individuals requiring access to CNSI/facilities controlled or owned by USDA a valid VAR must be on file at PDSD or a delegated office.

a. VAR Information

A valid VAR must include:

- (1) Last name;
- (2) First Name;
- (3) Middle initial;
- (4) SSN;
- (5) Level of access required for meeting, event, etc.;
- (6) Date of most recent investigation (investigation closed date);
- (7) Type of most recent investigation;
- (8) Agency/Office that granted access;
- (9) Date(s) of visit;
- (10) Purpose of visit;
- (11) The POC of the individual at USDA that can be contacted by PDSD to verify Need-to-Know and inform of the VAR receipt;

(12) Security office or POC to include:

- (a) Full name;
- (b) Office phone number;
- (c) Office fax number; and
- (d) Email address of sending agency or office (Contractors must include Security Management Office [SMO] code), or office that can be contacted by the receiving security office.

b. Duration of Visit Limitations

The VAR must be on Agency or company letterhead and should arrive at least 48 hours before the intended visit. Received VARs are subject to the same duration requirements as clearance passing mentioned above. IC blue badges, or other unique identification created by an outside organization will not be accepted as validation of security clearance or level of access.

VARs will be maintained by PDSD or delegated offices for two (2) years from the date the visit was sent. They can be either hard copy or digital.

3. MEETINGS

This section applies to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which CNSI is disclosed, hereafter called a "meeting".

a. Government Sponsorship of Meetings

Disclosure of CNSI to large diverse audiences such as conferences increases security risks. However, classified disclosure at such meetings which serve a government purpose and at which adequate security measures have been provided in advance may be conducted, provided the meeting is authorized by USDA and that has agreed to assume security jurisdiction. USDA must approve security arrangements, announcements, attendees, and the location of the meeting. USDA may delegate certain responsibilities to a cleared contractor for the security arrangements and other actions necessary for the meeting under the general supervision of USDA.

b. Requests for Authorization

Employees desiring to conduct meetings requiring sponsorship shall submit their requests to their Agency's ISC or to the SSO. The request for authorization shall include the following information:

- (1) An explanation of the government purpose to be served by disclosing CNSI at the meeting and why the use of conventional channels for release of the information will not advance those interests;

- (2) The subject of the meeting, and scope of classified topics, to include the classification level, to be disclosed at the meeting;
- (3) The expected dates and location of the meeting;
- (4) The general content of the proposed announcement and/or invitation to be sent to prospective attendees or participants;
- (5) The identity of any other non-government organization involved and a full description of the type of support it will provide;
- (6) A list of any foreign representatives (including their nationality, name, organizational affiliation) whose attendance at the meeting is proposed; and
- (7) A description of the security arrangements necessary for the meeting to comply with the requirements of this DM.

c. Location of Meetings

Classified sessions shall be held only in secure rooms or other approved spaces. The ISC or SSO is responsible for evaluating and approving the location proposed for the meeting.

d. Security Arrangements for Meetings

The SSO shall develop the security measures and procedures to be used. The security arrangements must provide for the following:

(1) Announcements

Approval of USDA shall be obtained for all announcements of the meeting. Announcements shall be unclassified and shall be limited to a general description of topics expected to be presented, names of speakers, and administrative instructions for requesting invitations or participation. Classified presentations shall not be solicited in the announcement. When the meeting has been approved, announcements may only state that USDA has authorized the conduct of classified sessions and will provide necessary security assistance. The announcement shall further specify that security clearances and justification to attend classified sessions are to be forwarded to PDSO or its designee. Invitations to foreign persons shall be sent by the authorizing federal agency.

(2) Clearance and need-to-know

All persons in attendance at classified sessions shall possess the requisite clearance and need-to-know for the information to be disclosed. Need-to-know shall be determined by the meeting host with the help of the ISC and SSO. Attendance shall be authorized only to those persons whose security clearance and need-to-know for attendance have been verified by the ISC, the SSO or a delegated Agency ISC office.

The names of all authorized attendees or participants must appear on an access list. Entry shall be permitted to the classified session only after verification of the attendee's identity, based on presentation of official photographic identification such as a passport, contractor or U.S. Government identification card, has been done.

### (3) Presentations

CNSI must be authorized for disclosure in advance by USDA. Individuals making presentations at meetings shall provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification. Classified presentations shall be delivered orally and/or visually. Copies of classified presentations or slides, etc., shall not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentations shall be classified, safeguarded, and transmitted as required by this DM.

If electronic equipment is brought by an external agency to be used to give a classified briefing, the external agency must coordinate this prior to the meeting with the ISC, SSO and/or OCIO. The external agency must also have an Authority to Operate (ATO) issued by their parent organization, on letterhead, that identifies the specific equipment to be used has been evaluated and approved for CNSI use.

Coordination must also be completed by the SSO or ISC, in conjunction with the OCIO/ASOC, to ensure projector equipment or display systems utilized are approved for use with CNSI systems.

### (4) Physical Security

The physical security measures for the classified sessions shall provide for control of, access to and dissemination of, the CNSI to be presented and shall provide for secure storage capability, if necessary.

## 4. DISCLOSURE

All employees shall ensure that CNSI is disclosed only to those authorized persons.

### a. Disclosure to Employees

Employees are authorized to disclose CNSI to other cleared employees as necessary for the performance of tasks or services essential to the employee's official duties in accordance with a need-to-know.

### b. Disclosure Authority at Meetings

Obtain prior written authorization for each proposed disclosure of CNSI from USDA.

Furnish a copy of the disclosure authorization to the federal agency sponsoring the meeting.

Agencies are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. Authority to disclose CNSI at meetings, whether disclosure is by officials of industry or government, must be granted by the federal agency or activity that has classification jurisdiction over the information to be disclosed. Each employee that desires to disclose CNSI at a meeting is responsible for requesting and obtaining disclosure approvals.

c. Disclosure to Other Federal Agencies

Employees shall not disclose CNSI received or generated from one (1) federal agency to any other federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

d. Disclosure of CNSI to Foreign Persons

Employees shall not disclose CNSI to foreign persons unless release of the information is authorized in writing by the federal agency having classification jurisdiction over the information involved (e.g., the DOE for RD and FRD, the NSA for COMSEC, the ODNI for SCI), and all other executive branch departments and agencies for CNSI under their jurisdiction. The disclosure must also be consistent with applicable U.S. laws and regulations and requires approval from the SSO.

e. Disclosure of Export Controlled Information to Foreign Persons

Employees shall not disclose export-controlled information and technology (classified or unclassified) to a foreign person, whether disclosure occurs in the United States or abroad, unless such disclosure is in compliance with applicable U.S. laws and regulations.

f. Disclosure to the Public

Employees shall not disclose CNSI to the public without prior review and clearance from the Classifying Official through the SSO and SAO.

Requests for approval shall be submitted through the SSO. Each request shall indicate the approximate date the employee intends to release the information for public disclosure and identify the media to be used for the initial release. A copy of each approved request for release shall be retained for a period of one (1) inspection cycle for review by the SSO. All information developed subsequent to the initial approval shall also be cleared by the appropriate office prior to public disclosure.

Information that has been declassified is not automatically authorized for public disclosure. Employees shall request approval for public disclosure of "declassified" information in accordance with the procedures of the previous paragraph.

CHAPTER 7  
CONTRACTING

1. CONTRACTING REQUIREMENTS

Contractors visiting USDA facilities and requiring access to CNSI 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 must receive a copy of the contractor's Defense Department (DD)-254 form, *DOD 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 PDSO before its employees may participate in classified meetings, events or work.

a. USDA Contracted Services

USDA Agencies that contract for work involving access to CNSI are required to provide security requirements to the contractor through a DD-254 form. The DD-254 form specifically addresses those enhanced security requirements that apply to the contractor or subcontractor and 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-254 form are incorporated into the solicitation and resultant contract. Prior to receiving the prime contractor's signature and releasing to the subcontractors, the DD-254 Forms must be forwarded to the ISC/SSO for approval.

- (1) The ISC must complete a DD-254 with the subcontractor's information to the SSO for approval. The ISC must include the reason for considering a subcontractor and have a proposed DD-254 Form attached to the justification. Each subcontractor or consultant will require a prepared DD-254 Form which must be approved by PDSO.
- (2) A final DD-254 Form must be issued for the storage and retention of program material. The storage and control requirements will be approved by the ISO.

b. Contract Clause

Federal Acquisition Regulation ([FAR Subpart 2.1](#), definitions, defines a classified contract as "any contract in which the contractor or its employees must have access to CNSI 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 DOD 5220.22-M, National Industrial Security Program Operating Manual ([NISPOM](#)). At a minimum, all classified contracts must contain FAR [subpart 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 ([AGAR Advisory NO. 61](#), Revision 01, *Safeguarding Classified National Security Information*).

c. Contractor Responsibilities

USDA contractors are responsible for protecting CNSI in accordance with the NISPOM and this DM. In the pre-contract phase, prior to any release of classified information, the prime contractor shall advise the prospective subcontractor of the procurement's enhanced special security requirements. Arrangements for the subcontractor program access shall be pre-coordinated with PDSD.

d. Contractor Violations

All violations involving contractor personnel must be reported by the SSO/PDSD using the appropriate DSS reporting channels.

e. Facility Clearance

In order for a subcontractor to have the necessary facility clearance, the prime contractor must initiate the appropriate paperwork and submit it to PDSD. The SSO will coordinate with DSS to initiate the action to provide the subcontractor with a facility clearance.

## CHAPTER 8

### REPORTING

#### 1. REQUIRED REPORTING

##### a. Report Submission

All reports required by this DM will be made through the PDSD via the appointed ISC or SSC. In those instances where the report affects the baseline SWA clearance or the incident is of a personnel security clearance nature, the report will also be provided to the Classified National Security Programs Branch (CNSPB) as well as to the SSO. In those rare instances where classified program information must be included in the report, the report will be provided only to the SSO, who will sanitize the report and provide the information to the CSA, if appropriate.

##### b. Adverse Information

Employees and contractors will report to the SSO via the ISC/SSC if appropriate, any information which may adversely reflect on the individual's ability to properly safeguard CNSI.

Serious adverse information that is of a nature that would be a deciding factor in granting an individual access (drug use, committing a felony, etc.) will immediately deny the individual further access to CNSI and report the circumstances to PDSD within 24 hours. After obtaining and reporting all necessary facts, the Chief, PDSD will determine what, if any, further action will be taken. All other adverse information will be reported to the SSO and the Chief, PDSD within 72 hours of the initial knowledge of the information. The ISC/SSC will report adverse information to the SSO, who in turn will report the information to the Chief, PDSD.

Should another Agency suspend or revoke an individual's access to their classified material, the individual is to be suspended from all USDA classified activities and the circumstances will be reported to the SSO within 24 hours. After obtaining and reporting all necessary facts, the Chief, PDSD will determine what, if any, further action will be taken.

#### 2. SF-312 NDA

A report will be submitted to the SSO on an employee who refuses to sign an NDA.

Prior to providing access to CNSI or briefing an individual to USDA classified, the SF-312 must be signed, and when necessary a signed polygraph supplement. If the required forms are not signed, access will not be granted.

### 3. CHANGE IN EMPLOYEE STATUS

A written report of all changes in the personal status of indoctrinated personnel will be provided to the SSO. In addition to those changes identified in this DM (marital status, home of record, etc.), include censure or probation arising from an adverse personnel action, and revocation, or suspension downgrading of a security clearance for reasons other than security administration purposes.

### 4. FOREIGN TRAVEL

All travel outside the contiguous U.S., Hawaii, Alaska and the U.S. Territories (i.e., Puerto Rico) except same-day travel to border areas (i.e., Canada, Mexico) for individuals cleared for Top Secret/SCI access must be reported. Individuals with a collateral clearance (Confidential, Secret or Top Secret) are encouraged to report foreign travel to allow the security office to provide any potential country specific, defensive counter intelligence, security related or other helpful information to assist the person while out of the country. Such travel is to be reported through the ISC/SSC to the SSO, and retained as specified in the retention guide. Travel by cleared individuals into or through countries identified as critical or high-risk area will require additional coordination. The list of critical or high-risk areas will be maintained by PDS and will be made available to all ISCs and SSCs as appropriate.

#### a. Prior to Travel

Report all foreign travel at least 15 business days prior to the departure (as described above) to the security official (ISC, SSC or SSO). The report will contain the following information:

- (1) Name, SSN, position, passport number (if applicable). Also identify any persons accompanying the accessed individual;
- (2) Facility information, including security officer's name and telephone number;
- (3) Describe the purpose of travel (i.e., business, pleasure, military) and the sponsor of the trip (i.e., company, military reserve, university, personal);
- (4) Detailed itinerary, including departure date, time, flight/cruise/train information, foreign location(s) to be visited (including dates), and return date and time (with associated travel method information);
- (5) Emergency contact information (someone other than a travel companion); and
- (6) Any expected foreign contacts with a detailed explanation.

#### b. Return from Travel

- (1) Upon return from travel, a foreign travel debrief template must be filled out and returned to the ISC or SSO after the completion of the foreign travel or at the request of the SSO.

- (2) The ISC will forward notification to the SSO where it will be maintained as a permanent record of foreign travel.

c. Foreign Contacts

The following types of foreign contact must be reported to the SSO:

- (1) Contact with personnel from foreign diplomatic establishments;
- (2) Information concerning actual or potential terrorism, terrorist groups, espionage, or sabotage of any U.S. facility, activity, person, or resource;
- (3) Recurring contact with a non-U.S. citizen;
- (4) When financial ties are established or involved with a foreign entity;
- (5) A request by anyone for illegal or unauthorized access to classified or controlled information; and
- (6) Contact with an individual (regardless of nationality) under circumstances that suggest the employee concerned may be the target of an attempted exploitation by the intelligence services of another country.

5. ARMS CONTROL TREATY VISITS

The SAO and SSO will be notified in advance of any Arms Control Treaty Visits. Such reports permit the SAO and SSO to assess potential impact on a classified activity and effectively provide guidance and assistance.

6. LITIGATION

Litigation or public proceedings which may involve CNSI will be reported. These include legal proceedings and/or administrative actions in which the prime contractor, subcontractors, or Government organizations and their accessed individuals are a named party. The ISC will report to the SSO any litigation actions that may pertain to classified, to include the physical environments, facilities or personnel or as otherwise directed by the SAO. The SSO is also required to notify Office of General Counsel (OGC) in the event that any CNSI under the control and custody of USDA is involved in litigation or a public proceeding.

7. SECURITY INCIDENTS, INFRACTIONS AND VIOLATIONS

All security incidents, infractions, and violations will be reported to the insider threat team within 72 hours of completion of the security incident report.

a. Security Incidents

The ISC/SSC must promptly advise PDSD in all instances where national security concerns would impact on collateral security programs or clearances of individuals under the cognizance of the SAO.

All security incidents will be reported through the ISC to PDSD within 24 hours. If an incident is not reported within a timely manner, the responsible individual may be suspended by PDSD or the SAO pending a review of the circumstances of the delay and the incident. In addition, all security incidents will be documented and made available for review by the ISC/SSO during visits.

b. Security Infractions

A security infraction is any other incident that is not in the best interest of security that does not involve the loss, compromise, or suspected compromise of CNSI. Security infractions will be documented and provided to the SSO for review and concurrence.

Within 24 hours, report all infractions through the ISC to the SSO. Report all known information. An initial written report will be provided through the ISC to the SSO within 72 hours of the incident. The report will include the circumstances surrounding the incident to help the SSO/Chief, PDSD determine what follow-up actions are necessary. After obtaining all necessary facts, the Chief, PDSD will determine what, if any, further action will be taken. Once the ISC/SSC of the affected facility has determined the scope of the corrective action to be taken, it will be reported to the SSO. If follow-up actions are required by the SSO or ISC, written interim reports will be provided through the ISC to the SSO every 30 days apprising the Chief, PDSD of the actions being taken. A final report will be submitted after all steps of the investigation have been taken. The ISC and SSO will maintain a local record of all infractions. They will be requested and reviewed by the security review team during the next annual review. All records are subject to review during any visits.

c. Security Violations

A security violation is any incident that involves the loss, compromise, or suspected compromise of CNSI.00 Security violations will be reported immediately to the PDSD through the ISC but not later than 24 hours.

Immediately following a security violation, the ISC/SSO will take the following actions:

(1) Protect

Seize control of and secure all CNSI material.

(2) Report

Within 24 hours, report all violations to the Chief, PDSD. Report all known information. Coordination with the Chief, PDSD should be accomplished prior to

interviewing any individuals. An initial written report will be provided through the SSO to the Chief, PDSD within 72 hours of the incident. Written interim reports will be provided through the ISC to the SSO every 30 days apprising the Chief, PDSD of the actions being taken. The SSO will contact the ISC in writing, informing them of the results of the investigation, recommending any corrective and or disciplinary actions deemed appropriate. A final report will be submitted after all steps of the investigation have been taken. After obtaining all necessary facts, the SAO will determine what, if any, further action will be taken.

At a minimum, the following information will be included in all reports:

- (a) A detailed description of the incident. Include statements from all key participants;
- (b) Date and location of the incident;
- (c) The CNSI/material, involved;
- (d) All persons involved, and their clearances/accesses (if any);
- (e) Likelihood of compromise;
- (f) A damage assessment;
- (g) Immediate remedial action to correct the cause of the incident;
- (h) Any planned remedial action; and
- (i) Other pertinent information.

(3) Investigate

Coordinate with the Chief, PDSD to determine proper investigative procedures. Initiate and control the investigation of the incident. Upon completion of investigation, the SAO will report the loss, possible compromise or unauthorized disclosure of classified information and any violation of Section 5.5 (b) (1), (2), and (3) of E.O. 13526 to the ISOO.

(4) Sanctions

Individuals who are found in violation of E.O. 13536 shall be subject to appropriate sanctions that may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

## 8. INADVERTNENT DISCLOSURE

Inadvertent disclosure is the involuntary, unauthorized access to CNSI by an individual without access authorization. Personnel determined to have had unauthorized or inadvertent

access to CNSI should be interviewed to determine the extent of the exposure, and may be requested to complete an Inadvertent Disclosure Oath/Agreement.

Any person who releases or exposes CNSI to an unauthorized individual has committed a security violation and must be reported pursuant to this DM.

a. Conditions

If during emergency response situations, guard personnel or local emergency authorities (e.g., police, medical, fire, etc.) inadvertently gain access to CNSI, they should be interviewed to determine the extent of the exposure. If circumstances warrant, a preliminary inquiry will be conducted. When in doubt, contact the SSO for advice.

Refusal to sign an Inadvertent Disclosure Oath/Agreement will be reported by the ISC to the SSO.

Contractors shall report all unauthorized disclosures involving RD or FRD to the DOE or NRC through their CSA, and to the ISC or SSO.

9. FWA REPORTING

Reporting of any potential FWA within this program is encouraged. However, to reduce the possibility of revealing CNSI to non-accessed individuals, DO NOT use other advertised FWA hotlines (e.g., USDA advertised FWA Hotline) when CNSI may be revealed.

a. Important factors

When requested, confidentiality may be granted. Individuals may be assured they can report FWA instances without fear of reprisal or unauthorized release of their identity.

Reports within this program will be forwarded the appointed Office of Inspector General (OIG) FWA representative.

For the program participant's reference, this information is to be posted within each accredited facility.

10. REPORTING FOR TRAVEL OR POSITNING IN CRITICAL HUMAN INTELLIGENCE (HUMINT) THREAT POSTS

Individuals that will be assigned more than 60 days to a critical HUMINT threat post must have their proposed assignment reviewed prior to being assigned. This includes all employees, contractors, and personnel on temporary duty assignments in excess of 60 days accumulated in one (1) year (not necessarily consecutive) to determine their assignment creates an unmanageable risk.

Agencies must prescreen assignment of personnel to CRITICAL HUMINT THREAT POSTS in accordance with 12 Foreign Affairs Handbook-6 H-211.5.

To confirm whether a location is a critical HUMINT threat post, the ISC can access a copy of the Security Environment Threat List (SETL) by contacting the SSO.

All requests will be reviewed, and a recommendation will be provided back to the requesting agency by PDSD.

## CHAPTER 9

### SELF-INSPECTION PROGRAM

#### 1. GENERAL

Self-inspections are the internal review and evaluation of individual USDA Offices and Agencies concerning their protection and handling of CNSI. These inspections can be accomplished by the SSC, ISC or the SSO. Copies of the initial inspection report created by the SSC or ISC must be sent within five (5) calendar days to the SSO for record purposes. Within 30 days of completion, the self-inspection report with corrective actions must be submitted to the SSO in PDSD. 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 will be completed annually and no later than the second week of August by Agencies and Staff Offices that receive, generate, and store classified information. PDSD will conduct random oversight inspections throughout USDA in order to meet the requirements of E.O. 13526. Self-inspections will also be completed when a pattern of security violations or infractions reveal a security weakness. Agencies and Staff Offices will ensure all classified products generated by USDA in which the declassification dated has passed are reviewed annually in accordance with E.O. 13526, Section 3.5.

#### 3. INSPECTION COVERAGE

USDA Agencies and Staff Offices will complete self-inspections that cover original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight. Agencies and Staff Offices will conduct a self-inspection that includes a representative sampling of 25% all USDA generated products. If during the self-inspection, 50% of the representative sampling is found to have errors in classification markings, then all USDA generated products must be reviewed. When this occurs, the SSO must be notified of the finding and a corrective action plan must be submitted to the SSO within 30 days of findings. Corrective action plan must include a plan for correcting all errors found, and also address remedial training for either the immediate staff involved in the errors, or for all derivative classifiers for that specific program or the agency as a whole.

Individuals who continue to classify or misclassify information in violation of E.O. 13526 will be subject to sanction outlined in E.O. 13526, Section 5.5(c). A self-inspection checklist can be found on the PDSD website, or you may request a copy from the SSO, to use when conducting a self-inspection. Self-inspections can be expanded if necessary.

#### 4. DOCUMENTATION

Self-inspection reports shall be maintained for two (2) years by submitting agency prior to the destruction of the self-inspection, all items requiring corrective actions must be

completed. Report results will be provided to PDSD to compile into a single Departmental response to annual requests from the ISOO on self-inspection activities.

## 5. REPORTS

PDSD will provide the SAO a list of agencies who fail to provide a self-inspection report in the required time. PDSD will verify the accuracy of information provided on the self-inspection reports, report findings to the SAO, maintain a copy of each agency self-inspection report for two (2) years, and prepare the Agency Annual Self-Inspection Program Data form required by ISOO annual for the SAO review and signature.

In addition to the self-inspection report, agencies will provide a copy of their completed SF-311, Agency Security Classification Management Program Data to PDSD annually within 30 days upon request from PDSD. PDSD will verify the accuracy of information provided on the report, complete a statistical analysis of all information provided by the agencies, consolidate input into a single Departmental response to the ISOO, and provide the report to the SAO for review and signature.

Agencies will provide the SF-716, Agency Security Classification Cost Estimates to PDSD annually within 30 days upon request from PDSD. PDSD will verify the accuracy of information provided on the report, complete a statistical analysis of all information provided by the agencies, consolidate input into a single Departmental response to the ISOO, and provide the report to the SAO for review and signature.

-END-

## APPENDIX A

### REFERENCES

[10 C.F.R. Part 1045](#), Subparts A, B, and C, *Nuclear Classification and Declassification*.

[32 C.F.R. Part 2001](#), *Classified National Security Information*.

[42 U.S.C. § 2011 et seq.](#), *Atomic Energy Act of 1954*, August 30, 1954.

[AGAR Advisory NO. 61](#), Revision 01, *Safeguarding Classified National Security Information*, March 20, 2008.

DOD 5220.00-M, *National Industrial Security Program Operating Manual (NISPOM)*, February 28, 2006.

[DR 3080-001](#), *Records Management*, May 23, 2013.

[DR 3440-001](#), *USDA Classified National Security Information Program Regulation*, October 5, 2011.

[DR 3440-002](#), *Control and Protection of "Sensitive Security Information"*, January 30, 2003.

[DR 4600-001](#), *USDA Personnel Security Clearance Program*, July 2, 2013.

[DR 4600-002](#), *Procedures for Denial or Revocation for Access to National Security Information*, September 13, 2013

[DR 4600-003](#), *USDA Insider Threat Program*, June 30, 2014.

Draft Security Executive Agent Directive 400, *Minimum Reporting Requirements for Personnel With Access to CNSI or Who Hold A Sensitive Position*.

E.O. 10450, *Security Requirements for Government Employment*, April 27, 1953.

E.O. 12333, *United States Intelligence Activities*, December 4, 1981 (amended).

[E.O. 12968](#), *Access to Classified Information*, August 2, 1995.

[E.O. 13587](#), *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011.

[E.O. 13556](#), *Controlled Unclassified Information*, November 4, 2010.

[E.O. 13526](#), *Classified National Security Information*, December 29, 2009.

[Federal Acquisition Regulation \(FAR\)](#).

[Federal Standard 809A](#), *Neutralization and Repair of GSA Approved Containers*, May 10, 2005.

[Federal Standard 832](#), *Construction Methods and Materials for Vaults*, September 1, 2002.

Federal Specification [FF-L-2740B](#), *Locks, Combination, Electromechanical*, June 15, 2011.

[Intelligence Authorization Act for FY 1995](#), Pub. L. 103–359, 108 Stat. 3423, October 14, 1994.

[ISOO Notice 2011-02](#), *Further Guidance and Clarification on Commingling Atomic Energy Information and Classified National Security Information*, May 18, 2011.

[OMB M-11-08](#), *Initial Assessment of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems*, January 3, 2011.

Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993.

[Presidential Memorandum](#), *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 21, 2012.

[UL 827](#), *Standard for Central-Station Alarm Services*, June 11, 2008.

[Whistleblower Protection Enhancement Act of 2012](#), 5 U.S.C. § 2301 *et seq.*

White House Memorandum, *Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies*, August 23, 1996.

## APPENDIX B

## DEFINITIONS

- a. Access: The ability and opportunity to obtain knowledge of classified information.
- b. Adverse Information: Any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security.
- c. Agency: A component within USDA such as the Foreign Agriculture Service, the Food and Nutrition Service, and the Office of the Inspector General.
- d. 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.
- e. “Authorized holder”: Of classified information means anyone who satisfies the conditions for access stated in section 4.1 of E.O 13526.
- f. 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.
- g. 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.
- h. Classification: The act or process by which information is determined to be classified information.
- i. 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.
- j. 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.
- k. Classified Visit: A visit during which a visitor will require, or is expected to require, access to classified information.
- l. 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.
- m. Cleared Employees: All employees granted a security clearance to include interims.
  - n. 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.
  - o. 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 transmission security, emissions security, and physical security of COMSEC material.
  - p. Compilation: means an aggregation of preexisting unclassified items of information.
  - q. Compromise: An unauthorized disclosure of classified information.
  - r. Confidential source: means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both are to be held in confidence.
  - s. Continental United States (CONUS): United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.
  - t. 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”).
  - u. 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 munitions, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable and highly explosive materials by type.
  - v. Courier: A cleared employee, designated by the SSO who is permitted to transmit classified material to its destination. The classified material remains in the personal possession of the courier except for authorized overnight storage.

- w. Damage to the National Security: Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of classified information.
- x. Declassification: The authorized change in the status of information from classified information to unclassified information.
- y. 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.
- z. 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.
- aa. 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.
- bb. 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.
- cc. Downgrading: A determination that information classified at a specified level shall be classified at a lower level.
- dd. Event: An occurrence or happening that is reasonably certain to occur and that can be set as the signal for automatic declassification of information.
- ee. File Series: Documentary material, regardless of its physical form or characteristics, which is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.
- ff. 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.
- gg. Foreign Interest: Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity

- organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.
- hh. 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.
  - ii. 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.
  - jj. 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.
  - kk. 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.
  - ll. 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”). 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.
  - mm. Intelligence: includes foreign intelligence and counterintelligence as defined by E.O. 12333 of December 4, 1981, as amended, or by a successor order
  - nn. Intelligence activities: means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or E.O. 12333, as amended, or a successor order.
  - oo. Intelligence Community: means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) or E.O. 12333, as amended.

- pp. Interagency Security Classification Appeals Panel (ISCAP): The ISCAP provides the public and users of the classification system with a forum for further review of classification decisions.
- qq. Mandatory Declassification Review: Review for declassification of classified information in response to a request for declassification that meets the requirements of E.O. 12958.
- rr. Material: Any product or substance on or in which information is embodied.
- ss. Multiple Sources: Two (2) or more source documents, classification guides, or a combination of both.
- tt. National Security: The national defense or foreign relations of the United States
- uu. 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.
- vv. Network: means a system of two or more computers that can exchange data or information.
- ww. 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.
- xx. Original Classification: An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.
- yy. 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.
- zz. Permanent Historical Value: Those records that have been identified in an agency records schedule as being permanently valuable.
- aaa. Records: The records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.
- bbb. Records having permanent historical value: Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

- ccc. Record management: The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.
- ddd. Regraded: To raise or lower the classification assigned to an item of information.
- eee. 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.
- fff. Safeguarding: Measures taken and controls employed that are prescribed to protect classified information.
- ggg. 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.
- hhh. Security Clearance: A determination that a person is eligible under the standards of E.O. 12968 for access to classified information.
- iii. 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 nonworking hours, closed-circuit video monitoring, or other safeguards that mitigate the vulnerability of unalarmed storage areas and security storage cabinets during nonworking hours.
- jjj. 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.
- kkk. Senior Agency Official (SAO). An official appointed by the Secretary of Agriculture under the provisions of Section 5.4(d) of E.O. 12958.
- lll. 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.

- mmm. Source document: means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.
- nnn. 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.
- ooo. 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.
- ppp. Subject Matter Expert (SME): An individual with in-depth knowledge of a business area, science, or technology.
- qqq. 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.
- rrr. Telecommunications: means the preparation, transmission, or communication of information by electronic means.
- sss. Transmission: The sending of information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.
- ttt. Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.
- uuu. U.S. entity includes: (1) State, local, or tribal governments; (2) State, local, and tribal law enforcement and firefighting entities; (3) Public health and medical entities; (4) regional, state, local, and tribal emergency management entities, including State Adjutant General and other appropriate public safety entities; or (5) private sector entities serving as part of the nation's Critical Infrastructure Key Resources. ,

- vvv. Upgrade: To raise the classification of an item of information from one level to a higher one.
- www. 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.
- xxx. 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.
- yyy. Working Papers: 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

## APPENDIX C

### ACRONYMS AND ABBREVIATIONS

AD	Agriculture Department
ADA	American Disabilities Act
AEA	Atomic Energy Act
AGAR	Agriculture Acquisition Regulation
AIS	Automatic Identification System
ASA	Assistant Secretary for Administration
ASOC	Agriculture Security Operations Center
ATO	Authority to Operate
C	Confidential
CD	Compact Disc
CFR	Code of Federal Regulation
CI	Counter Intelligence
CMC	Classified Material Conversion
CNSI	Classified National Security Information
CNSPB	Classified National Security Programs Branch
COMSEC	Communications Security
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
CPI	Critical Program Information
CRZH	National Industrial Security Systems
CSA	Cognizant Security Authority
CTS	Cosmic Top Secret
CTSA	Cosmic Top Secret ATOMAL
CUSR	Central U.S. Registry
DAA	Designated Approving Authority
DAAG	Department of the Army Adjutant General
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCS	Defense Courier Service
DD	Defense Department
DHS	Department of Homeland Security
DM	Departmental Manual
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DR	Departmental Regulation

DVD	Digital Versatile Disc
E.O.	Executive Order
EPL	Evaluated Product List
FAR	Federal Acquisition Regulation
FED-STD	Federal Standard
FF-L	Federal Specification
FIS	Foreign Intelligence Service
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRD	Formerly Restricted Data
FWA	Fraud Waste and Abuse
GSA	General Services Administration
HSDN	Homeland Secure Data Network
HSS	High Security Switch
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Information Assurance Manager
IAW	In Accordance With
IC	Intelligence Community
ICD	Intelligence Community Directive
IDS	Intrusion Detection System
IR	Infrared
ISC	Information Security Coordinator
ISCAP	Interagency Security Classification Appeals Panel
ISCR	Information System Certification Report
ISOO	Information Security Oversight Office
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communication System
MR	Manual Review
MSSP	Master System Security Plan
NACLC	National Agency Check with Law and Credit
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NC	NATO Confidential
NCA	NATO Confidential ATOMAL
NDA	Non-Disclosure Agreement
NISPOM	National Industrial Security Program Operating Manual
NITTF	National Insider Threat Task Force
NOFORN	Not Releasable to Foreign Nationals

NR	NATO Restricted
NRC	Nuclear Regulatory Commission
NS	NATO Secret
NSA	NATO Secret ATOMAL
NSA	National Security Agency
NSA/CSS	National Security Agency/Central Security Service
OADR	Original Agency's Determination Required
OCA	Original Classification Authority
OCIO	Office of the Chief Information Officer
OCONUS	Outside the Contiguous United States
ODNI	Office of the Director of National Intelligence
OGC	Office of General Counsel
OHSEC	Office Homeland Security and Emergency Coordination
OHRM	Office of Human Resources Management (OHRM)
OIG	Office of Inspector General
OO	Office of Operations
OMB	Office of Management and Budget
OPM	Office of Personnel Management
ORCON	Dissemination and Extraction of Information Controlled by Originator
PC	Personal Computer
PCU	Premise Control Unit
PDSD	Personnel and Document Security Division
PED	Portable Electronic Devices
PIN	Personal Identification Number
POC	Point of Contact
POD	Physical Operations Division
PROPIN	Caution-Proprietary Information Involved
RD	Restricted Data
REL TO	Authorized for Release To
RF	Radio Frequency
S	Secret
SAO	Senior Agency Official
SAP	Special Access Program
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SETA	Security Education, Training, and Awareness
SETL	Security Environment Threat List
SF	Standard Form
SME	Subject Matter Expert

SMO	Security Management Office
SOP	Standard Operating Procedures
SSBI	Single Scope Background Investigation
SSC	Site Security Coordinators
SSI	Sensitive Security Information
SSO	Special Security Office
SSP	System Security Plan
SSN	Social Security Number
STC	Sound Transmission Class
STE	Secure Terminal Equipment
SWA	Secure Work Area
TEMPEST	Transient Electromagnetic Pulse Surveillance Technology
TSWA	Temporary Secure Working Area
TFNI	Transclassified Foreign Nuclear Information
TS	Top Secret
TSCO	Top Secret Control Officer
U	Unclassified
U.S.	United States
U.S.C.	United States Code
UL	Underwriters Laboratories
USDA	U.S. Department of Agriculture
USSAN	U.S. Security Authority for NATO
VAR	Visit Access Request

APPENDIX D:

FOREIGN EQUIVALENT SECURITY CLASSIFICATIONS

**Table 1 Foreign Equivalent Security Classifications**

<b>COUNTRY</b>	<b>TOP SECRET</b>	<b>SECRET</b>	<b>CONFIDENTIAL</b>	<b>OTHER</b>
Albania	TEPER SEKRET	SEKRET	IMIREBESUESHEM	I KUFIZUAR
Argentina	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Australia	TOP SECRET	SECRET or HIGHLY PROTECTED	CONFIDENTIAL or PROTECTED	RESTRICTED
Austria	STRENG GEHEIM	GEHEIM	VERSCHLUSS	
Belgium (French)	TRES SECRET	SECRET	CONFIDENTIEL	DIFFUSION RESTREINTS
Belgium (Flemish)	ZEER GEHEIM	GEHEIM	VERTROUWELIJK	BEPERTKE VERSPREIDING
Bolivia	SUPERSECRETO or MUY SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Brazil	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Bulgaria	СТРОГО СЕКРЕТНО (STROGO SECRETNO)	СЕКРЕТНО (SEKRETNO)	ПОВЕРИТЕЛНО (POVERITELNO)	ЗА СЛУЖЕБНО ПОЛЗБАНЕ (ZA SLUZHEBNO POLZVANE – equates to For Official Use)
Canada	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Chile	SECRETO	RESERVADO	CONFIDENCIAL	
Colombia	ULTRASECRETO	SECRETO	RESERVADO	CONFIDENCIAL/ RESTRINGIDO
Costa Rica	ALTO SECRETO	SECRETO	CONFIDENCIAL	
Croatia	NAJVECI TAJNITAJNI	TAJNI	POVERLJIV	OGRANCIEN

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Denmark	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Ecuador	SECRETISIMO	SECRETO	CONFIDENCIAL	RESERVADO
Egypt	TOP SECRET	VERY SECRET	SECRET	OFFICIAL
El Salvador	ULTRA SECRETO	SECRETO	CONFIDENCIAL	
Estonia	TOP SECRET	SECRET	CONFIDENTIAL	
Ethiopia	YEMIAZ BIRTOU MISTIR	MISTIR	KILKIL	
Finland	ERITTAIN SALAINEN	Salainen	Luottamuksellinen	Viranomaiskaytto
France	TRES SECRET DEFENSE	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Germany	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	Vs- Nur für den Dienstgebrauch
Greece	AKΡΩΣ ΑΠΟΡΡΗΤΟ	ΑΠΟΡΡΗΤΟ	ΕΜΠΙΣΤΕΥΤΙΚΟ	ΠΡΕΠΙΩΡΙΑΣ ΜΕΝΗΣ ΧΡΗΣΕΩΣ
Guatamala	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Honduras	SUPER SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Hungary	SZIGORUAN TITKOS	TITKOS	TITKOS	KORLÁTOZOTT TERJESXTÉSŰ
Iceland	ALGJORTI	TRUNADARMAL		THJONUSTAJSKJAL
India	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Indonesia	SANGAT RAHASIA	RAHASIA	TERBATAS	
Iran	BENKOLI SERRI	SERRI	KHEILI MAHRAMANEH	MAHRAMANEH
Ireland	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Israel	SODI BE'YOTER	SODI	SHAMUR	MUGBAL
Italy	SEGRETISSIMO	SEGRETO	RISERVATISSIMO	RISERVATO
Japan	TOP SECRET	SECRET	CONFIDENTIAL	
Jordan	STRICTLY CONFIDENTIAL	CONFIDENTIAL	RESTRICTED	
Korea	I KUP PI MIL	II KUP PI MIL	III KUP PI MIL	

COUNTRY	TOP SECRET	SECRET	CONFIDENTIAL	OTHER
Laos	TRES SECRET	SECRET	SECRET/CONFIDENTIEL	DIFFUSION RESTREINTE
Latvia	SEVISKI SLEPENA	SLEPENA	KONFIDENCIALA	DIENESTA VAJADZĪBĀM
Lebanon	TRES SECRET	SECRET	CONFIDENTIEL	
Lithuania	VISIŠLAPTAI SLAPTAI	SLAPTAI	SLAPTAI	RIBOTO NAUDOJIMO
Malaysia	RAHSIA BESAR	RAHSIA	SULIT	TERHAD
Mexico	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESTRINGIDO
Morocco	SECRET DEFENSE	SECRET	CONFIDENTIEL	RESTREINT
Netherlands	STG. ZEER GEHEIM	STG. GEHEIM	STG. CONFIDENTIEEL	Departementaal VERTROUWELIJK
New Zealand	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Nicaragua	ALTO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Norway	STRENGT HEMMELIG	HEMMELIG	KONFIDENEIELT	BEGRENSET
Oman	TOP SECRET	SECRET	CONFIDENTIAL	
Pakistan	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Paraguay	SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Peru	ESTRICTAMENTE SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Philippines	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Poland	SCISLE TAJNE	TAJNE	POUFNE	ZASTREZONE
Portugal	MUITO SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
Romanian	STRICT-SECRET DE IMPORT ANT A DEOSEBITA	STRICT-SECRET	SECRET	SECRET DE SERVICIU
Saudi Arabia	SAUDI TOP SECRET	SAUDI VERY SECRET	SAUDI SECRET	SAUDI RESTRICTED
Singapore	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Slovakia	PRISNÉ TAJNÉ	TAJNÉ	DÔVERNÉ	VYHRADENÉ

<b>COUNTRY</b>	<b>TOP SECRET</b>	<b>SECRET</b>	<b>CONFIDENTIAL</b>	<b>OTHER</b>
Slovenia	STROGO ZAUPNO	OBRAMBA – DRŽAVNA SKRIVNOST Defense - State Secret	ZAUPNO	
South Africa	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Spain	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Sweden	H0/ TOP SECRET (the word HEMLIG enclosed with Red Borders)	H1/ SECRET	H2/ SECRET	
Switzerland	GEHEIM	VERTAULICH		
Taiwan	TOP SECRET (Not translatable into English characters)	SECRET	CONFIDENTIAL	
Thailand	LUP TISUD	LUP MAAG	LUP	POK PID
Tunisia	TOP SECRET	SECRET	SECRET CONFIDENTIAL	
Turkey	COK GIZLI	GIZLI	OZEL	HIZMETE ÖZEL
Ukraine	ОСОБЛИВОЇ ВАЖЛИВОСТІ	ЦІЛКОМ ТАЄМНО	ТАЄМНО	
UK	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO