United States Department of Agriculture
Animal and Plant Health Inspection Service
Marketing and Regulatory Programs Business Services
Emergency Management, Safety, and Security Division
Security Branch

APHIS
INFORMATION SECURITY PROGRAM MANUAL
3440

APHIS INFORMATION SECUIRTY PROGRAM MANUAL

This is the Animal and Plant Health Inspection Service (APHIS) Information Security Program Manual (ISPM). It is intended to provide guidance and instruction for all APHIS employees who have any duties and/or responsibilities for safeguarding and/or access to classified and sensitive information (users, supervisors, contractors, management, and security personnel).

The APHIS ISPM combines appropriate Federal regulations, Executive Orders, and USDA Departmental Manuals into one reference tool. This Manual applies to all APHIS employees working in the United States and foreign locations. This Manual contains specific procedures and instructions relating to the protection of classified and sensitive security information in APHIS. Adherence to the guidance contained herein is mandatory for all applicable APHIS personnel.

All references to responsibilities applying to personnel outside of the management and/or responsibility of APHIS are for informational purposes only and are provided herein to provide guidance as outlined in Executive Order 13526, CFR 32 Parts 2001 and 2003, and other applicable Federal directives, Instructions, etc., that provide direction and instruction for the protection of classified national security information.

Updating this Manual will occur on an as-needed basis to incorporate employee suggestions, changes in legislation, and general improvements. Comments should be sent to:

Emergency Management, Safety, and Security Division
4700 River Road, Unit 72
Riverdale, MD 20737

REFERENCES

10 Code of Federal Regulations (CFR) Part 1045, Nuclear Classification and Declassification

32 CFR Parts 2001 and 2003, Classified National Security Information

39 CFR Chapter 1, US Postal Service

31 U.S.C. 9701, Fees and Charges for Government Services and Things of Value

50 U.S.C. 401 et seq., National Security Act of 1947, as amended

Department of Defense (DoD) 5200.1-R, Information Security Program

DoD 5220.22.M, National Industrial Security Program Operating Manual

DoD Classification and Control Markings Implementation Manual

Executive Order 12829, as amended, National Industrial Security Program

Executive Order 12951, Release of Imagery Acquired by Space-Based Intelligence Reconnaissance Systems

Executive Order 12958, Title 3, Secretary of Agriculture Designation Authority

Executive Order 13526, Classified National Security Information

Federal Specification FF-L-2740A, Amendment to Federal Specification Locks, Combination

Federal Specification FF-P-110, Padlock, Changeable Combination

Intelligence Community Directive 206, Sourcing Requirements for Disseminated Analytic Products

Intelligence Community Directive 503 Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation

Intelligence Community Directive 705, Sensitive Compartmented Information Facilities

Intelligence Community Directive 710, Classification and Control Markings System

Intelligence Community Policy Guidance 704.5, Intelligence Community Personnel Security Database Scattered Castles

Intelligence Community Standard 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities

Intelligence Community Standard 705-2, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities

Intelligence Community Standard 2007-550-2

Intelligence Community Standard 2008-700-1

Information Security Oversight Office Marking Booklet

National Industrial Security Program Operating Manual

NSTISSI 7000, TEMPEST Countermeasures for Facilities

Public Law 105-261 Section 3161, Protection Against Inadvertent Release of Restricted Data and Formerly Restricted Data

Section 552 of Title 5, United States Code, Freedom of Information Act

Section 552a of Title 5, United States Code, The Privacy Act of 1974

SPB Issuance 6–97, National Policy on Technical Surveillance Countermeasures

USDA Departmental Regulation 3080-001, Records Management

USSAN 1-07, US Security Authority for NATO Instruction

US Atomic Energy Act of 1954

USDA Department Manual (DM) 3440-001, USDA Classified National Security Information Program Manual, dated May 1, 2008

TABLE OF CONTENTS

Page Subject

15 CHAPTER 1
GENERAL INFORMATION

15 1. Purpose
15 2. Policy
15 3. Scope
15 4. Availability
15 5. Authorities
15 6. Responsibilities
17 6.a. Secretary of Agriculture
17 6.b. Assistant Secretary for Administration
17 6.c. APHIS Information Security Specialist
17 6.d. Managers and Supervisors
17 6.e. APHIS Employees
17 6.f. Top Secret Control Officer (TSCO)
18 6.g. Escort Officials
18 6.h. Classified Couriers
18 6.i. Guard Force Members
18 6.j. Information Systems Security Program Manager (ISSPM)

19 CHAPTER 2
CLASSIFICATION MANAGEMENT

19 1. Original Classification
19 1.a. Authority to Originally Classify Information
19 1.b. Original Classification Conditions
19 1.c. Classification Levels
20 1.d. Classification Categories
20 1.e. Process
22 1.f. Duration of Information Classified under Prior Orders
23 1.g. Classification Prohibitions and Limitations
23 1.h. Declassification without Proper Authority
24 1.i. Reclassification
25 2. Classification Challenges
25 2.a. Formal Challenges
25 2.b. Agency Procedures
26 2.c. Additional Considerations
26 3. Security Classification Guides (SCGs)
26 3.a. Developing SCGs
27 3.b. General Content of SCGs
27 3.c. Dissemination of SCGs
27 3.d. Reviewing and Updating SCGs

28 4. Fundamental Classification Guidance Review
28 4.a. Coverage of Reviews
28 4.b. Participation in Reviews
29 4.c. Reports on Results

31 **CHAPTER 3**
MARKING

31 1. General
31 2. Originally Classified Documents
31 2.a. Classification Authority
32 2.b. Agency and Office of Origin
32 2.c. Reason for Classification
32 2.d. Declassification Instructions
33 2.e. Date of Origin of Document
33 3. Derivatively Classified Documents
33 3.a. Identity of Persons Who Apply Derivative Classification Markings
33 3.b. Source of Derivative Classification
34 3.c. Reason for Classification
34 3.d. Declassification Instructions
36 4. Document Markings
36 4.a. Page Markings
36 4.b. Portion Markings
37 4.c. Dissemination Control and Handling Markings
38 4.d. Portion Marking Waivers
38 4.e. Marking Information that has been Reclassified
38 4.f. Date of Document
39 5. Classification Marking in the Electronic Environment
39 5.a. Executive Order. 13526 Requirements
39 5.b. Proper Classification Markings
39 5.c. Electronic Output Markings
39 5.d. Marked in Accordance with Derivative Classification Procedures
39 5.e. Derivative Classification Prohibitions
39 5.f. Markings on Classified Email Messages
40 5.g. Marking Web Pages with Classified Content
41 5.h. Marking Classified URLs
41 5.i. Marking Classified Dynamic Documents and Relational Databases
42 5.j. Marking Classified Bulletin Board Postings and Blogs
43 5.k. Marking Classified Wikis
43 5.l. Instant Messaging, Chat, and Chat Rooms
43 5.m. Attached Files
44 6. Transmittal Documents
44 7. Foreign Government Information (FGI)
44 7.a. Portion Markings
44 7.b. Portion Markings when ID of Country Needs to be Concealed
44 7.c. Portion Markings when Containment of FGI Needs to be Concealed
44 7.d. Transfer to National Archives and Records Administration

45 8. Working Papers
45 8.a. Markings
45 8.b. Conditions
45 9. Other Material
45 10. Unmarked Materials
45 11. Classification by Compilation/Aggregation
45 12. Commingling of Restricted Data (RD) and Former Restricted Data (FRD) with Information Classified under E.0. 13526
46 12.a. Automatic Declassification Prohibitions
46 12.b. Declassification Line
46 12.c. Extraction of RD or FRD
46 12.d. Extraction of Information Classified under E.O. 13526
46 12.e. No Portion Marking
47 13. Transclassified Foreign Nuclear Information (TFNI)
47 13.a. Safeguarding TFNI
47 13.b. Automatic Declassification Prohibition
47 14. Marking of Electronic Storage Media
47 15. Declassification Markings
47 15.a. General Requirement
47 15.b. When Markings Cannot Be Affixed
47 15.c. Uniform and Conspicuous
48 15.d. Required Markings
48 16. Automatic Declassification Exemption Markings
48 16.a. Marking Information Exempted from Automatic Declassification at 25 Years
50 16.b. Marking Information Exempted from Automatic Declassification at 50 Years
51 16.c. Marking Information Exempted from Automatic Declassification at 75 Years
51 17. Declassification
51 17.a. Automatic Declassification
58 17.b. Systematic Declassification Review
58 17.c. Declassification Guides
59 17.d. Mandatory Review for Declassification
63 17.e. Referrals
66 17.f. Discretionary Declassification

67 CHAPTER 4
SAFEGUARDING

67 1. General Requirements
67 1.a. Protection
67 1.b. Storing Unclassified Information with CNSI
67 1.c. Storage
67 1.d. Security Requirements for SCIFs
67 1.e. Classified Material Reduction
67 1.f. APHIS Alternate Measures for Protection
68 1.g. NATO Classified Information Storage Requirements
68 1.h. FGI

68 2. Responsibilities of Holders
68 2.a. Protection Against Unauthorized Access
68 2.b. Meeting Safeguarding Requirements
68 2.c. Communication Requirements
68 3. Access
69 3.a. Access Requirements
69 3.b. Disclosure Requirements
69 3.c. Disclosure Determination Responsibilities
69 3.d. Control of CNSI
69 3.e. Removal of CNSI from APHIS Facilities
69 3.f. Safeguarding During Working Hours
60 4. Secure Areas
70 4.a. Definition
70 4.b. Accreditation Requirements
72 4.c. Accreditation Status
72 4.d. Access
77 4.e. Escorting Policy
77 4.f. Construction of Secure Areas
77 4.g. SF 702 Security Container Check Sheet
77 4.h. Secure Telephone Equipment (STE)
77 4.i. Classified Processing
77 4.j. TS Secure Storage and Supplemental Protection
78 5. Security Containers
78 5.a. New Equipment Procurement
78 5.b. Storage Requirements
79 5.c. External Markings
79 5.d. Absence of Authorized Storage Procedures
79 5.e. Leaving Classified Material Unattended
79 5.f. Weapons, Funds, etc.
79 5.g. Covering Security Containers
79 5.h. Combinations
82 5.i. Repair of Damaged Security Containers
82 6. Information Controls
82 6.a. Top Secret
85 6.b. Secret and Confidential
85 7. Reproduction
85 7.a. Minimum Requirements
85 7.b. Security Vulnerabilities
85 7.c. Security Precautions
86 7.d. Machine Markings
86 7.e. Location of Machines
86 7.f. Disposal of Equipment
86 7.g. Location
87 7.h. Diagnostic Capabilities
87 7.i. Safeguarding during Use
87 7.j. Connection to LAN/Telephone Lines

87 7.k. Servicing
87 7.l. Reproduction of TS Materials
87 8. Disposal and Destruction of Classified Materials
87 8.a. Retention
87 8.b. Disposal Provisions
87 8.c. Requirements
88 8.d. Record Copies
88 8.e. Authorized Equipment
89 8.f. Clearance Requirements
89 8.g. Destruction Methods
89 8.h. Destruction Procedures
90 8.i. Required Forms
90 8.j. Recordable Media Destruction
91 8.k. Bulk Destruction
92 9. Safeguarding U.S. CNSI Located in Foreign Countries
92 9.a. Retention of CNSI in Foreign Countries
92 9.b. Storage Requirements
92 10. Foreign Government Information (FGI)
92 10.a. NATO CNSI
92 10.b. General Storage Requirements
92 10.c. Storage Costs
92 10.d. Safeguarding Standards
94 10.e. Third Country Transfers
94 10.f. Foreign Disclosure of CNSI
94 11. Emergency Authority
94 11.a. Emergency Disclosure of CNSI
95 11.b. Declassification
95 12. Emergency planning
95 12.a. Planning Requirements
96 12.b. Plan Inclusions
96 12.c. Emergency Destruction or Removal
96 12.d. Storage Container Inspection

97 CHAPTER 5
TRANSPORTATION METHODS

97 1. General
97 2. Requirements
97 2.a. Recipients
97 2.b. Authorized Personnel
97 2.c. Means of Transportation
97 2.d. Local Procedures
97 2.e. Wrapping Requirements
98 2.f. Protection while Hand-carrying
99 2.g. Transportation Methods within and between the U.S., Puerto Rico, or a U.S. Possession or Trust Territory

85 2.h. Transportation Methods to a U.S. Government Facility located outside the U.S.
85 2.i. Transportation of U.S. CNSI to Foreign Governments
85 2.j. Receipt of CNSI
85 2.k. Hand-carrying CNSI

107 CHAPTER 6
TRANSMISSION METHODS

107 1. General
107 2. Requirements
107 2.a. Classified Discussions, Meetings, and Conferences
108 2.b. Transmission Prohibitions

111 CHAPTER 7
SPECIAL ACCESS PROGRAMS

111 1. Overview
111 2. Special Access Program Creation
111 3. Memorandum of Agreement/Memorandum of Understanding
111 4. Access

113 **CHAPTER 8**
SENSITIVE COMPARTMENTED INFORMATION

113 1. General
113 2. Security Administration Support
113 3. SCI Program Policy
113 3.a. Request for Access to SCI
114 3.b. When Access is no longer Required
114 4. Accreditation of SCIFs
114 4.a. Request Requirements
114 4.b. Physical Security Survey
114 5. SCI Security Education
114 5.a. Responsibilities
114 5.b. Requirements
115 6. Reporting Requirements
115 6.a. General
115 6.b. Listing
115 7. Travel of Employees with SCI Access
115 7.a. Requirements
115 7.b. Briefing Content

117 CHAPTER 9
SECURITY EDUCATION AND TRAINING

117 1. General

117 2. Policy
117 3. Requirements
117 3.a. Initial Briefing
117 3.b. OCA Training
118 3.c. Derivative Classifier Training
118 3.d. Annual Refresher Briefings
119 3.e. Specialized Security Position Training
119 3.f. Termination Briefings
119 3.g. Other Security Education and Training

121 CHAPTER 10
INDUSTRIAL SECURITY

121 1. General
121 1.a. Establishment
121 1.b. Security Requirements
121 1.c. Contractors
121 1.d. Application
121 2. Requirements
121 2.a. DD Form 254
121 2.b. Definition
121 2.c. Application
122 3. PDSD and Senior Agency Official Responsibilities
122 3.a. Assistance and Guidance
122 3.b. FCLs
122 3.c. Assistance
122 3.d. Representation
122 4. Contracting Officer Responsibilities
122 4.a. Requirements
122 4.b. Approve 254s
122 5. Contracting Officer Representative Responsibilities
122 5.a. Records Maintenance
123 5.b. Personnel Security Clearance Verification
123 5.c. Process Requirements
124 6. PDSD Responsibilities
124 6.a. Records Maintenance
124 6.b. Providing Assistance
124 6.c. Briefing

125 CHAPTER 11
LOSS, POSSIBLE COMPROMISE, OR UNAUTHORIZED DISCLOSURE OF CNSI

125 1. General Requirements
125 1.a. Discovery
125 1.b. Public Media

125 1.c. Requests from Media
125 1.d. Reporting
125 2. Cases involving FGI or Another Government Agency's Information
125 2.a. Reporting
125 2.b. Restrictions
125 3. Inquiry or Investigation
126 4. ISSO Reporting Requirements
126 4.a. Oversight Committee Reporting
126 4.b. Significant Public Attention
126 4.c. Large Amounts of CNSI
126 4.d. Potential Systematic Weaknesses
126 5. DOJ and Legal Counsel Coordination
126 5.a. ISS Responsibilities
126 5.b. Coordination with DOJ
126 6. Inquiries and Investigations
126 6.a. Formal Investigation
126 6.b. Purpose of Inquiry
127 7. Debriefings in Cases of Unauthorized Access
127 7.a. Unauthorized Access by Person with Appropriate Clearance
127 7.b. Unauthorized Access by Person without Appropriate Clearance
127 8. Appointment of Preliminary Inquiry Officer
127 8.a. PDSD Notification
128 8.b. ISS Actions
128 8.c. Preliminary Inquiry Officer Responsibilities
129 8.d. Inquiry
129 9. Corrective Actions
129 10. Sanctions
129 10.a. List of Offensives Subject to Sanctions
130 10.b. Sample Sanctions

131 CHAPTER 12
PROGRAM MANAGEMENT

131 1. General
131 1.a. Documentation
131 1.b. Counterintelligence Technical Inspections
131 2. Requirements
131 2.a. ISC Responsibilities
131 2.b. ISC Support
131 2.c. ISC Coordination with ISS
132 3. Entry and Exit Inspections

133 CHAPTER 13
SELF INSPECTIONS

133 1. General

133 1.a. Conduct of Self-inspection
133 1.b. Self-inspection Inclusion
133 1.c. Review of Classified Holdings
133 1.d. Interviews and Reviews
133 2. Requirements
134 2.a. Establishment of Self-inspection Coverage Requirements
134 2.b. Documentation
134 2.c. Format
134 2.d. Reporting

135 CHAPTER 14
AGENCY ANNUAL REPORTING REQUIREMENTS

135 1. Statistical Reporting
135 2. Accounting for Costs
135 3.a. Collection of Data
135 3.b. Data Inclusion

APPENDICES

A. Acronyms
B. Definitions
C. APHIS Secure Area Accreditation Request Form
D. APHIS Accreditation Status Form
E. Co-Utilization Agreement Request Format
F. Courier Agreement
G. APHIS Courier Card Template
H. APHIS Courier Aircraft Hand Carry Letter Sample
I. Distribution Controls, Dissemination Controls, Non-Intelligence Community Markings, Non-U.S. Classification Markings
J. Standard Form 700 Sample
K. Standard Form 701 Sample
L. Standard Form 702 Sample
M. Form AD 471 Sample
N. SF 312 Sample
O. Classification and Control Markings
P. Trigraphs and Tetragraphs
Q. APHIS ISP Inspection Checklist
R. U.S. Equivalent Classification
S. Sample Classified Email Marking Instructions
T. USDA Request for Passing a Security Clearance
U. HSDN Account Request Checklist

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 1

GENERAL INFORMATION

1. Purpose. This Manual outlines the Animal and Plant Health Inspection Service (APHIS) policies and assigns responsibility for the classification, declassification, and safeguarding of classified national security information (CNSI) and sensitive information for the APHIS Information Security Program (ISP). The policies and procedures described within apply to all CNSI in APHIS' custody, regardless of whether the material originated within APHIS or was released to APHIS by another agency. The policies, procedures, and instructions contained within this Manual comply with United States Department of Agriculture (USDA) and other Federal policies, manuals, and guidance.

   Executive Order (E.O.) 13526, Classified National Security Information, dated December 29, 2009, prescribes a uniform system for classifying, safeguarding, and declassifying CNSI, including information relating to defense against transnational terrorism. The national defense requires that certain information be maintained in confidence in order to protect our citizens, democratic institutions, homeland security, and interactions with foreign nations. The implementing directive for E.O. 13526 is 32 Code of Federal Regulations (CFR), parts 2001 and 2003.2.

2. Policy. It is APHIS policy to:

   a. Establish an ISP to ensure a uniform and coordinated approach to information security at all levels of the organization in accordance with USDA and other Federal directives; and

   b. Ensure each individual who possesses, has access to, or has knowledge of such information regardless of how it was obtained will protect CNSI and sensitive information.

3. Scope. This Manual applies to all APHIS employees and contractors utilizing, handling, and safeguarding CNSI and sensitive information.

4. Availability. Copies of this Manual will be maintained in each accredited APHIS Secure Area where CNSI and any area where sensitive information is handled and stored.

5. Authorities. The authorities are listed in the References section of this Directive.

6. Responsibilities. E.O. 13526 requires that each Department originating or handling CNSI designate a senior official to direct and administer an ISP that ensures the protection of CNSI. The APHIS Administrator has delegated to the Marketing and Regulatory Programs Business Services' Emergency Management,

Safety, and Security Division (EMSSD), the responsibility for the establishment and administration of the APHIS ISP.

a. The APHIS Information Security Specialist (ISS) is responsible for monitoring compliance with the regulations for safeguarding CNSI and sensitive information within APHIS. The ISS will:

(1) Monitor and inspect locations used for the handling and storage of CNSI to ensure appropriate security measures are in place and utilized;

(a) The ISS will maintain written documentation of inspections for a minimum of 2 years.

(b) The ISS will request counterintelligence technical inspections.

(2) Promulgate implementing instructions for protection of CNSI;

(3) Establish, coordinate, maintain, and/or conduct security education and training programs;

(4) Establish and maintain an ongoing periodic review and assessment of CNSI documents, products, and equipment;

(5) Establish procedures to prevent unnecessary access to CNSI, including procedures that:

(a) Require a need for access to CNSI be established;

(b) Ensure the number of persons granted access to CNSI is limited to the minimum, and is consistent with operational and security requirements;

(c) Ensure CNSI used in or near hostile or potentially hostile areas safeguarded;

(d) Assist the USDA Personnel and Document Security Division (PDSD) in collecting information pertinent to APHIS to meet requirements for annual reporting to the Information Security Oversight Office (ISOO); and

(e) Promptly assign personnel to respond to any request, appeal, challenge, or complaint regarding CNSI.

(6) Initiate a preliminary inquiry when there is suspicion of a possible compromise or loss of CNSI;

(7) Report security violations to PDSD;

(8) Inventory security equipment and evaluate requirements for protection of CNSI; and

(9) Coordinate document reviews and provide guidance regarding classification or declassification action to employees.

b. Managers and supervisors are responsible for effective ISP implementation and are accountable for ensuring that their subordinates handle and secure classified CNSI and sensitive information in accordance with this Manual. Managers and supervisors will:

(1) Establish procedures for the accountability of CNSI and sensitive information in their Division and the control of such information;

(2) Provide for tracing the movement of CNSI, its limited dissemination, the prompt retrieval of documents, the detection of the loss of information, and the prevention of excessive production or reproduction of documents;

(3) Safeguard, handle, and store CNSI in GSA approved storage containers, areas, or facilities when it is not in use or under the supervision of an authorized person; and

(4) Ensure that, prior to releasing CNSI and sensitive information to another individual, the recipient has an appropriate clearance and a valid need-to-know.

(a) Background checks and security badges do not verify the security clearance level and/or a valid need-to-know.

(b) Verification of clearance must be made through the ISS or PDSD.

c. The Top Secret Control Officer (TSCO) will maintain an accountability log of all TS materials secured within an accredited Secure Area. TSCOs and alternates must be designated within offices with TS CNSI, possess and maintain a TS security clearance, and be selected on the basis of experience and reliability. TSCOs and alternates will receive, dispatch, and maintain accountability registers of all TS documents in their possession.

d. Escort Officials are responsible for escorting uncleared individuals visiting APHIS Secure Areas. Escort Officials will:

(1) Ensure that Secure Areas are sanitized prior to allowing visitors to enter;

(2) Adhere to all security rules and regulations, and ensure CNSI is safeguarded from unauthorized access; and

(3) Maintain visual contact with visitors at all times.

e. APHIS Classified Couriers will:

(1) Request a Courier Card through the ISS prior to transporting CNSI;

(2) Receive an initial and annual briefing on their responsibilities; and

(3) Comply with Classified Courier duties and responsibilities for the protection of CNSI.

CHAPTER 2

CLASSIFICATION MANAGEMENT

1. Original Classification. Original classification is the process used to determine if information can potentially cause damage to U.S. national security.

   a. Authority to Originally Classify Information. In accordance with Federal Regulations, within the U.S. Department of Agriculture (USDA) the authority to originally classify National Security Information (CNSI) at the Secret or Confidential level may be exercised only by the Secretary who is the USDA's sole Original Classification Authority (OCA). This authority may not be delegated. In accordance with Federal Regulations the Secretary cannot originally classify information at the Top Secret (TS) level.

   b. Original Classification Conditions. Information may only be originally classified under the terms of Executive Order (E.O.) 13526 when all of the following conditions are met:

      (1) The Secretary (as the OCA) classifies the information;

      (2) The information is owned by, produced by or for, or is under the control of the U.S. Government;

      (3) The Secretary determines that the unauthorized disclosure of the information could reasonably be expected to result in damage to the national security, which includes defense against transnational terrorism, and the Secretary is able to identify or describe the damage; and

      (4) The information falls within one or more of the eight categories of information which may be classified as outlined in E.O. 13526.

   c. Classification Levels. CNSI that requires protection against unauthorized disclosure can be classified by the Secretary at one of the following levels:

      (1) "Secret" for information that could reasonably be expected to cause *serious damage* to the national security if disclosed to unauthorized sources; or

      (2) "Confidential" for information that reasonably could be expected to cause *damage* to the national security if disclosed to unauthorized sources.

NOTE: Except as specifically provided by statute, no additional terms such as "Sensitive," "Agency," "Business," or "Administratively", et al will be used in conjunction with either of the two classification levels defined above.

d. Classification Categories. Information will not be considered for classification unless it pertains to one or more of the following categories of information outlined in E.O. 13526:

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

(2) Foreign government information;

(3) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;

(4) Foreign relations or foreign activities of the U.S., including confidential sources;

(5) Scientific, technological, or economic matters relating to the national security;

(6) U.S. Government programs for safeguarding nuclear materials or facilities;

(7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

(8) The development, production, or use of weapons of mass destruction.

e. Process. Section 1.1(a) of E.O. 13526 specifies the following conditions that must be met when making classification decisions.

(1) Identifying or Describing Damage to the National Security. Section 1.4 of E.O. 13526 specifies that information will not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable damage to the national security. There is no requirement, at the time of the decision, for an OCA to prepare a written description of such damage; however, if the classification decision becomes the subject of a challenge or access demand pursuant to E.O. 13526 or law, the OCA must be able to support the decision in writing, including identifying or describing the damage.

(2) Establishing Duration of Classification. Except for information that will clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, an OCA will follow the sequence listed in the paragraphs below when determining the duration of classification.

(a) The OCA of the information will attempt to determine a date or event that is less than 10 years from the date of original classification and that coincides with the lapse of the information's national security sensitivity, and will assign such date or event as the declassification instruction.

(b) If unable to determine a date or event of less than 10 years, the OCA will ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(c) If unable to determine a date or event of 10 years, the OCA will assign a declassification date not to exceed 25 years from the date of the original classification decision.

Duration of classification of special categories of information. The only exceptions to the sequence in the paragraphs above are as follows:

(a) If an OCA is classifying information that will clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, the duration will be up to 75 years and will be designated "50X1-HUM;" or

(b) If an OCA is classifying information that will clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, the duration will be up to 75 years and will be designated "50X2-WMD".

(c) Extending duration of classification for information classified under E.O. 13526. Extensions of classification are not automatic. If an OCA with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

(d) If the date or event assigned by the original classification authority has not passed, an OCA with jurisdiction over the information may extend the classification duration of such information for a period not to exceed 25 years from the date of origin of the record.

(e) If the date or event assigned by the OCA has passed, an OCA with jurisdiction over the information may reclassify the information in accordance with E.O. 13526 and 32 CFR only if it meets the standards for classification as outlined in E.O. 13526.

In all cases, when extending the duration of classification, the OCA must:

(a) Be an OCA with jurisdiction over the information;

(b) Ensure that the information continues to meet the standards for classification under E.O. 13526; and

(c) Make reasonable attempts to notify all known holders of the information.

f. Duration of Information Classified under Prior Orders.

(1) Specific Date or Event. Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. If the specific date or event has not passed, an OCA with jurisdiction over the information may extend the duration in accordance with the requirements of paragraph (b) of this section. If the date or event assigned by the OCA has passed, an OCA with jurisdiction over the information may only reclassify information in accordance with the standards and procedures under E.O. 13526. If the information is contained in records determined to be permanently valuable, and the prescribed date or event will take place more than 25 years from the date of origin of the document, the declassification of the information will instead be subject to section 3.3 of E.O. 13526.

(2) Indefinite Duration of Classification. For information marked with X1, X2, X3, X4, X5, X6, X7, or X8; ‘‘Originating Agency’s Determination Required’’ or its acronym "OADR;" “Manual Review” or its acronym “MR;” “Director of Central Intelligence” or its acronym “DCI Only;" “Director of National Intelligence” or its acronym DNI Only;" and any other marking indicating an

indefinite duration of classification under a prior order, or in those cases where a document is missing a required declassification instruction or the instruction is not complete:

(a) A declassification authority, as defined in section 3.1(b) of E.O. 13526, may declassify it;

(b) An OCA with jurisdiction over the information may re-mark the information to establish a duration of classification of no more than 25 years from the date of origin of the document, consistent with the requirements for information originally classified under E.O. 13526, as provided in paragraph (a) of this section; or

(c) Unless declassified earlier, such information contained in records determined to be permanently valuable will remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.3 of E.O 13526.

(3) Release of Imagery Acquired by Space-based Intelligence Reconnaissance Systems. The duration of classification of imagery as defined in E.O. 12951, Release of Imagery Acquired by Space-Based Intelligence Reconnaissance Systems, that is otherwise marked with an indefinite duration, such as "DCI Only" or "DNI Only," will be established by the DNI in accordance with E.O. 12951 and consistent with E.O. 13526. Any such information will be remarked in accordance with instructions prescribed by the DNI.

g. Classification Prohibitions and Limitations. In no case will information be classified in order to:

(1) Conceal violations of law, inefficiency, or administrative error;

(2) Prevent embarrassment to a person, organization, or agency;

(3) Restrain competition; or

(4) Prevent or delay the release of information that does not require protection in the interest of the national security.

h. Declassification Without Proper Authority. Information that has been declassified without proper authority, as determined by an OCA with jurisdiction over the information, remains classified and administrative action will be taken to restore markings and controls, as appropriate. All such determinations will be reported to the Senior Agency Official (SAO)

who will promptly provide a written report to the Director of the Information Security Oversight Office (ISOO).

If the information at issue is in records in the physical and legal custody of National Archives and Records Administration (NARA) and has been made available to the public, the OCA with jurisdiction over the information will, as part of determining whether the restoration of markings and controls is appropriate, consider whether the removal of the information from public purview will significantly mitigate the harm to national security or otherwise draw undue attention to the information at issue. Written notification, classified when appropriate under E.O. 13526, will be made to the Archivist, NARA, that will include a description of the record(s) at issue, the elements of information that are classified, the duration of classification, and the specific authority for continued classification. If the information at issue is more than 25 years of age and the Archivist does not agree with the decision, the information will nonetheless be temporarily withdrawn from public access and will be referred to the Director of ISOO for resolution in collaboration with affected parties.

i. Reclassification. In making the decision to reclassify information that has been declassified and released to the public under proper authority, the basis that the Secretary must approve, in writing, a determination on a document-by-document the reclassification is required to prevent significant and demonstrable damage to the national security. As part of making such a determination, the following will apply:

(1) The information must be reasonably recoverable without bringing undue attention to the information which means that:

(a) Most individual recipients or holders are known and can be contacted and all instances of the information to be reclassified will not be more widely disseminated;

(b) If the information has been made available to the public via a means such as Government archives or reading room, consideration is given to length of time the record has been available to the public, the extent to which the record has been accessed for research, and the extent to which the record and/or CNSI at issue has been copied, referenced, or publicized; and

(c) If the information has been made available to the public via electronic means such as the internet, consideration is given as to the number of times the information was accessed,

the form of access, and whether the information at issue has been copied, referenced, or publicized.

(2) If the reclassification concerns a record in the physical custody of NARA and has been available for public use, reclassification requires notification to the Archivist and approval by the Director of ISOO.

(3) Any recipients or holders of the reclassified information who have current security clearances will be appropriately briefed about their continuing legal obligations and responsibilities to protect this information from unauthorized disclosure. The recipients or holders who do not have security clearances will, to the extent practicable, be appropriately briefed about the reclassification of the information that they have had access to and their obligation not to disclose the information, and be requested to sign an acknowledgment of this briefing.

(4) The reclassified information must be appropriately marked in accordance with 32 Code of Federal Regulations (CFR) and safeguarded. The markings will include the authority for and the date of the reclassification action.

(5) Once the reclassification action has occurred, it must be reported to the National Security Advisor and to the Director of ISOO by the Secretary or SAO within 30 days.

2. Classification Challenges. Authorized holders, including authorized holders outside the classifying agency, who want to challenge the classification status of information will present such challenges to an OCA with jurisdiction over the information. An authorized holder is any individual who has been granted access to specific CNSI in accordance with the provisions of, and to include, the special conditions set forth in section 4.1(h) of E.O. 13526.

a. Formal Challenges. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

b. Agency Procedures. Because E.O. 13526 encourages authorized holders to challenge classification as a means of promoting proper and thoughtful classification actions, APHIS will ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

(1) APHIS will establish a system for processing, tracking, and recording formal classification challenges made by authorized holders. Agencies will consider classification challenges separately from Freedom of Information Act (FOIA) or other access requests, and will not process such challenges in turn with pending access requests.

(2) APHIS will provide an initial written response to a challenge within 60 days. If APHIS is unable to respond to the challenge within 60 days, APHIS must acknowledge the challenge in writing, and provide a date by which the Agency will respond. The acknowledgment must include a statement that if no Agency response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) for a decision. The challenger may also forward the challenge to the ISCAP if APHIS has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. APHIS responses to those challenges it denies will include the challenger's appeal rights to the ISCAP.

(3) Whenever APHIS receives a classification challenge to information that has been the subject of a challenge within the past 2 years, or that is the subject of pending litigation, APHIS is not required to process the challenge beyond informing the challenger of this fact and of the challenger's appeal rights, if any.

c. Additional Considerations. Challengers and APHIS will attempt to keep all challenges, appeals, and responses unclassified. However, CNSI contained in a challenge, the APHIS response, or an appeal will be handled and protected in accordance with E.O. 13526 and 32 CFR. Information being challenged for classification will remain classified unless and until a final decision is made to declassify it.

The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries will be encouraged as a means of holding down the number of formal challenges and to ensure the integrity of the classification process.

3. Security Classification Guides (SCGs). Originators of classified materials are encouraged to consult users of SCGs for input when developing or updating content.

a. Developing SCGs. When possible, originators of SCGs are encouraged to communicate within their agencies and with other agencies that are developing Guides for similar activities to ensure the consistency and

uniformity of classification decisions. Each APHIS activity will maintain a list of its SCGs in use.

b. General Content of SCGs. SCGs will, at a minimum:

(1) Identify the subject matter of the SCG;

(2) Identify the OCA by name and position, or personal identifier;

(3) Identify an agency point of contact or points of contact for questions regarding the SCG;

(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, the marking "50X1-HUM" or "50X2-WMD" as appropriate, or one or more of the exemption codes listed in 32 CFR provided that:

(a) The exemption has been approved by the ISCAP under section 3.3(j) of E.O. 13526;

(b) The ISCAP is notified of the intent to take such actions for specific information in advance of approval and the information remains in active use; and

(c) The exemption code is accompanied with a declassification date or event that has been approved by the ISCAP.

c. Dissemination of SCGs. SCGs will be disseminated as necessary to ensure the proper and uniform derivative classification of information.

d. Reviewing and Updating SCGs.

(1) APHIS will incorporate original classification decisions into SCGs as soon as practicable.

(2) Originators of SCGs are encouraged to consult the SCG users and other subject matter experts when reviewing or updating SCGs. Also, SCG users are encouraged to notify the originator of the SCG when they acquire information that suggests the need for a change in the instructions contained in the SCG.

4. Fundamental Classification Guidance Review. An initial fundamental classification guidance review will be completed by every activity that authors SCGs no later than June 27, 2012. Activities will conduct fundamental classification guidance reviews on a periodic basis thereafter. The frequency of the reviews will be determined by each Activity considering factors such as the number of SCGs and the volume and type of information they cover. However, a review will be conducted at least once every 5 years.

a. Coverage of Reviews. At a minimum, the fundamental classification guidance review will focus on:

(1) Evaluating content;

(2) Determining if the guidance conforms to current operational and technical circumstances; and

(3) Determining if the guidance meets the standards for classification under Section 1.4 of E.O. 13526 and an assessment of likely damage under Section 1.2 of E.O. 13526;

(4) Evaluating use;

(5) Determining if the dissemination and availability of the guidance is appropriate, timely, and effective; and

(6) Examining recent classification decisions that focus on ensuring that classification decisions reflect the intent of the guidance as to what is classified, the appropriate level, the duration, and associated markings.

b. Participation in Reviews. Pursuant to the requirements of E.O. 13526 APHIS personnel as assigned by the Secretary will direct the conduct of a fundamental classification guidance review and will ensure the appropriate Agency subject matter experts participate to obtain the broadest possible range of perspectives. To the extent practicable, input will also be obtained from external subject matter experts and external users of the reviewing Agency's classification guidance and decisions.

c. Reports on Results. The assigned APHIS personnel will provide to the Secretary a detailed report summarizing the results of each classification guidance review to be provided to ISOO and release an unclassified version to the public except when the existence of the SCG or program is itself classified.

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 3

MARKING

1. General. Executive Order (E.O.) 13526 requires a uniform security classification system with standard markings and other indicia be applied to classified National Security Information (CNSI).

    a. Except in extraordinary circumstances, or as approved by the Director of Information Security Oversight Office (ISOO), the marking of classified information will not deviate from the formats prescribed in 32 Code of Federal Regulations (CFR).

    b. If markings cannot be affixed to specific CNSI or materials, E.O. 13526 directs that the Original Classification Authority (OCA) will provide holders or recipients of the information with written instructions for protecting the information.

    c. Markings will be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

    d. Markings other than "Top Secret" (TS), "Secret" (S) and "Confidential" (C) will not be used to identify collateral CNSI.

    e. The guidance prescribed in this Chapter is not specific to the Animal and Plant Health Inspection Service (APHIS) or the U.S. Department of Agriculture (USDA); it applies to all CNSI regardless of origin.

2. Originally Classified Documents. (NOTE: The following requirements of the Original Classification Authority are extracted from E.O. 13526 and are contained herein for information purposes) At the time of original classification decision, the identity of the OCA, Agency and Office, Reason, and Declassification instructions will be provided in the classification block of the document. The document will also be dated.

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

    Classified By: David Smith, Chief, Division 5
    Or
    Classified By: ID#IMNO1

b. Agency and Office of Origin. If not otherwise evident, the Agency and Office of Origin will be identified and follow the name on the "Classified By" line. An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration.

c. Reason for Classification. The OCA will identify the reason(s) for the decision to classify the information. The OCA will include the number 1.4 plus the letter(s) that corresponds to the classification category in section 1.4 of E.O. 13526. An example might appear as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)

d. Declassification Instructions. The duration of the classification will be identified on the ''Declassify On'' line. When declassification dates are displayed numerically, the following format will be used: YYYYMMDD. The OCA will apply one of the following instructions:

(1) A date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which is equal to or less than
10 years from the date of the original decision. The duration of classification is marked as:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20201014
or
Declassify On: Completion of Operation XYZ

(2) A date not to exceed 25 years from the date of the original decision. For example, on a document that contains information classified on October 10, 2010, apply a date up to 25 years on the ''Declassify On'' line:

Classified By: David Smith, Chief, Division 5, Department of Good Works, Office of Administration
Reason: 1.4(g)
Declassify On: 20351010

(3) If the CNSI will clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence

source, no date or event is required and the marking "50X1-HUM" will be used in the "Declassify On" line;

(4) If the CNSI will clearly and demonstrably be expected to reveal key design concepts of weapons of mass destruction, no date or event is required and the marking "50X2-WMD" will be used in the "Declassify On" line.

e. Date of Origin of Document. The date of origin of the document will be indicated in a manner that is immediately apparent.

3. Derivatively Classified Documents. Information classified derivatively on the basis of source documents or security classification Guide (SCG) will bear all markings prescribed for originally CNSI except as provided in this section. Information for these markings will be carried forward from the source document or taken from instructions in the appropriate SCG.

A determination that information is classified through the compilation of unclassified
information is a derivative classification action based upon existing original classification guidance. If the compilation of unclassified information reveals a new aspect of information that meets the criteria for classification, it will be referred to an OCA with jurisdiction over the information to make an original classification decision and the requirements posted in an appropriate SCG.

a. Identity of Persons who Apply Derivative Classification Markings. Derivative classifiers will be identified by name and position, or personal identifier, in a manner that is immediately apparent on each derivatively classified document. If not otherwise evident, the agency and office of origin will be identified and follow the name on the "Classified By" line. An example might appear as:

Classified By: Peggy Jones, Lead Analyst, Research and Analysis Division
or
Classified By: ID # IMN01

b. Source of Derivative Classification.

(1) The derivative classifier will concisely identify the source document or the SCG on the "Derived From" line, including the Agency and, where available, the office of origin, and the date of the source or SCG. An example might appear as:

Derived From: Memo, "Funding Problems," October 20, 2008, Office of Administration, Department of Good Works

or

Derived From: CG No. 1, Department of Good Works, dated October 20, 2008.

(2) When a document is classified derivatively on the basis of more than one source document or SCG, the "Derived From" line will appear as:

Derived From: Multiple Sources

(a) The derivative classifier will include a listing of the source materials on, or attached to, each derivatively classified document to include any and all copies of the derivatively classified document.

(b) A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" will cite the source document on its "Derived From" line rather than the term "Multiple Sources." An example might appear as:

Derived From: Report titled, "New Weapons," dated October 20, 2009, Department of Good Works, Office of Administration.

c. Reason for Classification. The reason for the original classification decision, as reflected in the source document(s) or SCG, is not transferred in a derivative classification action.

d. Declassification Instructions.

(1) When declassification dates are displayed numerically, the following format will be used: YYYYMMDD; example: 20200101.

(2) When declassification dates of month, day, and year (not numerical) are used, the following format will be used: (Month), (Day), (Year); example: January 1, 2020.

(3) The derivative classifier will carry forward the instructions on the "Declassify On" line, if available, from the source document to the derivative document, or the duration instruction from the SCG or declassification guide. An example might appear as:

(Source document: "Declassify on: January 1, 2020")
Derivatively classified document: Declassify on January 1, 2020.

(4) If the source document is missing the declassification instruction, a calculated date of 25 years from the date of the source document will be used to determine the declassification instructions for the derivatively classified document. An example might appear as:

(Date of source document is September 12, 1998; no declassification instructions present on the document)
Derivatively classified document: Declassify on September 12, 2023.

(5) If there is no declassification date on the source document, and there is no document date on the source document, a date of 25 years from the date of derivative classification will be used to calculate the declassification date. An example might appear as:

(No date or declassification instructions on the source document)
Derivative classification took place on April 14, 2011; the declassification date will read "Declassify on April 14, 2036."

(6) When a document is classified derivatively on the basis of more than one source document or more than one element of a SCG, the "Declassify On" line will reflect the longest duration of any of its sources. An example might appear as:

Source #1: Declassify on May 26, 2018
Source #2: Declassify on October 20, 2017
Source #3: Declassify on March 1, 2019
Derivatively classified document declassification instruction will read: "Declassify on March 1, 2019."

When determining the most restrictive declassification instruction among multiple source documents, adhere to the following hierarchy for determining the declassification instructions for the "Declassify On" line:

(a) 50X1-HUM or 50X2-WMD, or an ISOO-approved designator reflecting the Interagency Security Classification Appeals Panel (ISCAP) approval for classification beyond 50 years in accordance with section 3.3(h)(2) of E.O. 13526;

(b) 25X1 through 25X9, with a date or event; or

(c) A specific declassification date or event within 25 years.

(7) When a document is classified derivatively either from a source document or a SCG that contains one of the following declassification instructions: “Originating Agency's Determination Required” (OADR), or “Manual Review” (MR), or any of the exemption markings X1, X2, X3, X4, X5, X6, X7, and X8, the derivative classifier will calculate a date that is 25 years from the date of the source document when determining the derivative document’s date or event to be placed in the "Declassify On” line. Examples might appear as:

Date of source document is July 12, 1995, source document declassification instruction reads: "Declassify on "OADR." Derivatively classified document declassification instruction will read: "Declassify on July 12, 2020."

Date of source document is November 21, 1998, source document declassification instruction reads "Declassify on X4." Derivatively classified document declassification instruction will read: "Declassify on November 21, 2023."

(8) When a document is classified derivatively either from a source document or a SCG that contains the declassification instructions "Director of Central Intelligence (DCI) Only" or "Director of National Intelligence (DNI) Only" and the information is subject to E.O. 12951, the derivative classifier will use a date or event as prescribed by the DNI.

4. Document Markings. Documents will be marked in accordance with 32 CFR.

a. Page Markings. Conspicuously label the top, bottom, front, and back of each page with the highest classification level of the information contained on the page, or with the highest overall classification of the document, including the designation "UNCLASSIFIED" on individual pages when it is applicable. The front cover, title page, and first page must also include the date the document was finalized, a classification block in the lower left corner, and portion markings on the subject or title.

b. Portion Markings. Each subject line, title, paragraph, subparagraph, section, (i.e., classified diagram, map, picture, drawing, etc.) or similar portion of a classified document will be marked to indicate the classification level of that portion or to indicate that it is unclassified.

(1) Portions of text will be marked with the appropriate abbreviation (“TS,” “S,” “C,” or “U” (unclassified)), placed in parentheses

immediately before the beginning of the portion. If the portion is numbered or lettered, place the abbreviation in parentheses between the letter or number and the start of the text. Examples might appear as:

(C) This sentence contains information about the timeframe for Operation XYZ.

(TS) This sentence contains information about the location of Operation XYZ.

(U) This is a graph depicting the budget expenditures for Operation XYZ.

(2) The portion marking that precedes the subject or title indicates the classification of the subject or title, not the classification of the document. When possible, select unclassified subjects and titles for classified documents. Place the portion markings for subjects and titles of classified documents immediately preceding the subject or title. An example might appear as follows for a document classified as Secret with an unclassified title:

(U) Operation XYZ.

c. Dissemination Control and Handling Markings. Many agencies require additional control and handling markings that supplement the overall classification markings.

(1) Dissemination control and handling markings identify the expansion or limitation on the distribution of the information. These markings are in addition to, and separate from, the level of classification.

(2) Only those external dissemination control and handling markings approved by ISOO or, with respect to the Intelligence Community (IC) by the DNI for intelligence and intelligence-related information, may be used by agencies to control and handle the dissemination of CNSI pursuant to agency regulations and to policy directives and Directives issued under section 5.4(d)(2) and section 6.2(b) of E.O. 13526. Such approved markings will be uniform and binding on all agencies and must be available in a central registry.

(3) If used, the dissemination control and handling markings will appear at the top and bottom of each page after the level of classification.

d. Portion Marking Waivers. The Secretary or Senior Agency Official (SAO) may request a waiver from the portion marking requirement for a specific category of information. Such a request will be submitted to the Director of ISOO and will include the reasons that the benefits of portion marking are outweighed by other factors. The request must also demonstrate that the requested waiver will not create impediments to information sharing. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

(1) Any approved portion marking waiver will be temporary with specific expiration dates.

(2) A document not portion marked, based on an ISOO-approved waiver must contain a warning statement that it may not be used as a source for derivative classification.

(3) If a classified document that is not portion marked, based on an ISOO-approved waiver, is transmitted outside the originating organization, the document must be portion marked unless otherwise explicitly provided in the waiver approval.

e. Marking Information that has been Reclassified. Specific information may only be reclassified if all the conditions of section 1.7(d) of E.O. 13526 and its implementing directives have been met. When taking this action, an OCA must include the following markings on the information:

(1) The level of classification;

(2) The identity, by name and position, or by personal identifier of the OCA;

(3) Declassification instructions;

(4) A concise reason for classification, including reference to the applicable classification category from section 1.4 of E.O. 13526; and

(5) The date the reclassification action was taken. The OCA will notify all known authorized holders of this action.

f. Date of Document. The date of the document will be indicated in a manner that is immediately apparent.

5. Classification Marking in the Electronic Environment. CNSI in the electronic environment will be:

a. Subject to all requirements of E.O. 13526;

b. Marked with proper classification markings to the extent that such marking is practical, including portion marking, overall classification, “Classified By”, “Derived From,” "Reason" for classification (originally classified information only), and “Declassify On”;

c. Marked with proper classification markings when appearing in an electronic output (e.g., database query) in which users of the information will need to be alerted to the classification status of the information;

d. Marked in accordance with derivative classification procedures, maintaining traceability of classification decisions to the OCA. In cases where CNSI in an electronic environment cannot be marked in this manner, a warning will be applied to alert users that the information may not be used as a source for derivative classification and providing a point of contact and instructions for users to receive further guidance on the use and classification of the information; and

e. Prohibited from use as source of derivative classification if it is dynamic in nature (e.g., wikis and blogs) and where information is not marked in accordance with E.O. 13526.

f. Markings on Classified Email Messages.

(1) Email transmitted on or prepared for transmission on classified systems or networks will be configured to display the overall classification at the top and bottom of the body of each message. The overall classification marking string for the email will reflect the classification of the header and body of the message. This includes 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. A single linear text string showing the overall classification and markings will be included in the first line of text and at the end of the body of the message after the signature block.

(2) Classified email will be portion marked. Each portion will be marked to reflect the highest level of information contained in that portion. A text portion containing a uniform resource locator (URL) or reference (i.e., link) to another document will be portion marked based on the classification of the content of the URL or link text, even if the content to which it points reflects a higher classification marking.

(3) A classified signature block will be portion marked to reflect the highest classification level markings of the information contained in the signature block itself.

(4) Subject lines will be portion marked to reflect the sensitivity of the information in the subject line itself and will not reflect any classification markings for the email content or attachments. Subject lines and titles will be portion marked before the subject or title.

(5) For a classified email, the classification authority block will be placed after the signature block, but before the overall classification marking string at the end of the email. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) When forwarding or replying to an email, individuals will ensure that in addition to the markings required for the content of the reply or forward email itself, the markings will reflect the overall classification and declassification instructions for the entire string of emails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.

g. Marking Web Pages with Classified Content.

(1) Web pages will be classified and marked on their own content regardless of the classification of the pages to which they link. Any presentation of information to which the web materials link will also be marked based on its own content.

(2) The overall classification marking string for every web page will reflect the overall classification markings (and any dissemination control or handling markings) for the information on that page. Linear text appearing on both the top and bottom of the page is acceptable.

(3) If any graphical representation is utilized, a text equivalent of the overall classification marking string will be included in the hypertext statement and page metadata. This will enable users without graphic display to be aware of the classification level of the page and allow for the use of text translators.

(4) Classified Web pages will be portion marked. Each portion will be marked to reflect the highest level of information contained in that portion. A portion containing a URL or reference to another

document will be portion marked based on the classification of the content of the URL itself, even if the content to which it points reflects a higher classification marking.

(5) Classified Web pages will include the classification authority block on either the top or bottom of the page. These blocks may appear as single linear text strings instead of the traditional appearance of three lines of text.

(6) Electronic media files such as video, audio, images, or slides will carry the overall classification and classification authority block, unless the addition of such information would render them inoperable. In such cases, another procedure will be used to ensure recipients are aware of the classification status of the information and the declassification instructions.

h. Marking Classified URLs. URLs provide unique addresses in the electronic environment for Web content and will be portion marked based on the classification of the content of the URL itself. The URL will not be portion marked to reflect the classification of the content to which it points. URLs will be developed at an unclassified level whenever possible. When a URL is classified, a classification portion mark will be used in the text of the URL string in a way that does not make the URL inoperable to identify the URL as a classified portion in any textual references to that URL. An example may appear as:

http://www.center.xyz/SECRET/filename_(S).html
http://www.center.xyz/filename2_(TS).html
http://www.center.xyz/filename_(TS//NF).html

i. Marking Classified Dynamic Documents and Relational Databases.

(1) A dynamic page contains electronic information derived from a changeable source or ad hoc query, such as a relational database. The classification levels of information returned may vary depending upon the specific request.

(2) If there is a mechanism for determining the actual classification markings for dynamic documents, the appropriate classification markings will be applied to and displayed on the document. If such a mechanism does not exist, the default will be the highest level of information in the database and a warning will be applied at the top of each page of the document. Such content will not be used as a basis for derivative classification. An example of such an applied warning may appear as:

"This content is classified at the [insert system-high classification level] level and may contain elements of information that are unclassified or classified at a lower level than the overall classification displayed. This content may not be used as a source of derivative classification, refer instead to the pertinent SCG(s)."

(3) This will alert the users of the information that there may be elements of information that may be either unclassified or classified at a lower level than the highest possible classification of the information returned. Users will be encouraged to make further inquiries concerning the status of individual elements in order to avoid unnecessary classification and/or impediments to information sharing. Resources such as SCGs and points of contact will be established to assist with these inquiries.

(4) Users developing a document based on query results from a database must properly mark the document in accordance with 32 CFR. If there is doubt about the correct markings, users will contact the database originating agency for guidance.

j. Marking Classified Bulletin Board Postings and Blogs.

(1) A blog, an abbreviation of the term "web log," is a Web site consisting of a series of entries, often commentary, description of events, or other material such as graphics or video, created by the same individual as in a journal or by many individuals. While the content of the overall blog is dynamic, entries are generally static in nature.

(2) The overall classification marking string for every bulletin board or blog will reflect the overall classification markings for the highest level of information allowed in that space. Linear text appearing on both the top and bottom of the page is acceptable.

(3) Subject lines of bulletin board postings, blog entries, or comments will be portion marked to reflect the sensitivity of the information in the subject line itself, not the content of the post.

(4) The overall classification marking string for the bulletin board posting, blog entry, or comment will reflect the classification markings for the subject line, the text of the posting, and any other information in the posting. These strings will be entered manually or by utilizing an electronic classification tool in the first line of text and at the end of the body of the posting. These strings may appear as single linear text.

(5) Bulletin board postings, blog entries, or comments will be portion marked. Each portion will be marked to reflect the highest level of information contained in that portion.

k. Marking Classified Wikis.

(1) Initial wiki submissions will include the overall classification marking string, portion marking, and the classification authority block string in the same manner as mentioned above for bulletin boards and blogs. All of these strings may appear as single line text.

(2) When users modify existing entries which alter the classification level of the content or add new content, they will change the required markings to reflect the classification markings for the resulting information. Systems will provide a means to log the identity of each user, the changes made, and the time and date of each change.

(3) Wiki articles and entries will be portion marked. Each portion will be marked to reflect the highest level of information contained in that portion.

l. Instant Messaging, Chat, and Chat Rooms.

(1) Instant messages and chat conversations generally consists of brief textual messages but may also include URLs, images, or graphics. Chat discussions captured for retention or printing will be marked at the top and bottom of each page with the overall classification reflecting all of the information within the discussion and, for classified discussions, portion markings and the classification authority block string will also appear.

(2) Chat rooms will display system-high overall classification markings and will contain instructions informing users that the information may not be used as a source for derivative classification unless it is portion marked, contains an overall classification marking, and a classification authority block.

m. Attached Files. When files are attached to another electronic message or document, the overall classification of the message or document will account for the classification level of the attachment and the message or document will indicate on its face the highest classification level of any CNSI attached or enclosed. The transmittal will also include conspicuously on its face the following or similar instructions, as appropriate:

Unclassified When Classified Enclosure Removed
or
Upon Removal of Attachments, This Document is (classification level).

6. Transmittal Documents. A transmittal document such as a fax cover sheet will indicate on its face the highest classification level of any CNSI attached or enclosed. The transmittal will also include conspicuously on its face the following or similar instructions, as appropriate:

Unclassified When Classified Enclosure Removed
or
Upon Removal of Attachments, This Document is (Classification Level).

7. Foreign Government Information (FGI). Unless otherwise evident, documents that contain FGI will include the marking, "This Document Contains (indicate country of origin) Information."

a. Portion Markings. Agencies may also require that the portions of the documents that contain FGI be marked to indicate the government and classification level, using accepted country code standards, e.g., "(Country code—C)."

b. Portion markings when ID of Country Needs to be Concealed. If the identity of the specific government must be concealed, the document will be marked, "This Document Contains Foreign Government Information," and pertinent portions will be marked "FGI" together with the classification level, e.g., "(FGI–C)". In such cases, a separate record that identifies the foreign government will be maintained in order to facilitate subsequent declassification actions.

c. Portion markings when Containment of FGI Needs to be Concealed. If the fact that information is FGI must be concealed, the markings described in paragraphs "a" or "b" above will not be used and the document will be marked as if it were wholly of U.S. origin.

d. Transfer to National Archives and Records Administration. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation will, at a minimum, identify the boxes that contain FGI.

8. Working Papers. A working paper is defined as a document or material, regardless of the media, that is expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers can by typed, handwritten, or computer-generated products.

a. Markings. Working papers containing CNSI will be dated when created, marked with the highest classification of any information contained therein, protected at that level, and if otherwise appropriate, destroyed when no longer needed.

b. Conditions. When any of the following conditions apply, working papers will be controlled, marked, and safeguarded in the same manner prescribed for a finished document at the same classification level:

(1) Released by the originator outside the originating activity;

(2) Retained more than 180 days from the date of origin; or

(3) Filed permanently.

9. Other Material. Bulky material or equipment will be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal CNSI, such identification is not required. Supporting documentation for such a finding must be maintained and a copy provided to the APHIS Information Security Specialist (ISS).

10. Unmarked Materials. Information contained in unmarked records, presidential or related materials, and which pertains to the national defense or foreign relations of the U.S. created, maintained, and protected as classified information under prior orders will continue to be treated as classified information under E.O. 13526, and is subject to its provisions regarding declassification.

11. Classification by Compilation/Aggregation. Compilation of items that are individually unclassified may be classified if the compiled information meets the standards established in section 1.2 of E.O. 13526 and reveals an additional association or relationship, as determined by the OCA. 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). In any such situation, clear instructions must appear with the compiled information as to the circumstances under which the individual portions constitute a classified compilation, and when they do not.

12. Commingling of Restricted Data (RD) and Formerly Restricted Data (FRD) with Information Classified under E.O. 13526. To the extent practicable, the commingling in the same document of RD or FRD with information classified under E.O. 13526 will be avoided. When it is not practicable to avoid such commingling, the marking requirements in E.O. 13526 and 32 CFR, as well as the marking requirements in 10 CFR Part 1045, Nuclear Classification and Declassification, must be followed.

a. Automatic Declassification Prohibitions. Automatic declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from the automatic declassification provisions of E.O. 13526 until the RD or FRD designation is properly removed by the Department of Energy (DOE). When DOE determines that an RD or FRD designation may be removed, any remaining information classified under E.O. 13526 must be referred to the appropriate agency in accordance with the declassification provisions of E.O. 13526
and 32 CFR.

b. Declassification Line. For commingled documents, the "Declassify On" line required by E.O. 13526 and 32 CFR will not include a declassification date or event and will instead be annotated with "Not Applicable (or N/A) to RD/FRD portions" and "See source list for CNSI portions." The source list will include the declassification instruction for each of the source documents classified under E.O. 13526 and will not appear on the front page of the document.

c. Extraction of RD or FRD. If an RD or FRD portion is extracted for use in a new document, the requirements of 10 CFR Part 1045 must be followed.

d. Extraction of Information Classified under E.O. 13526. If a portion classified under E.O. 13526 is extracted for use in a new document, the requirements of E.O. 13526 and 32 CFR must be followed. The declassification date for the extracted portion will be determined by using the source list in the pertinent SCG, or consultation with the OCA with jurisdiction for the information. However, if a commingled document is not portion marked, it will not be used as a source for a derivatively classified document.

e. No Portion Marking. If a commingled document is not portion marked based on appropriate authority, annotating the source list with the declassification instructions and including the "Declassify on" line in accordance with paragraph (3) of this section are not required. The lack of declassification instructions does not eliminate the requirement to process commingled documents for declassification in accordance with E.O. 13526, 32 CFR, the Atomic Energy Act, or 10 CFR Part 1045 when they are requested under statute or E.O. 13526.

13. Transclassified Foreign Nuclear Information (TFNI). As permitted under 42 U.S.C. 2163(e), DOE will remove from the RD category such information concerning the atomic energy programs of other nations as the Secretary of Energy and the DNI jointly determine to be necessary to carry out the provisions of 50 U.S.C. 403 and 403-1 and safeguarded under applicable Executive Orders as CNSI under a process called transclassification.

a. Safeguarding TFNI. When RD information is transclassified and is safeguarded as CNSI it will be handled, protected, and classified in conformity with the provisions of E.O. 13526 and 32 CFR. Such information will be labeled as "TFNI" and with any additional identifiers prescribed by the DOE. The label "TFNI" will be included on documents to indicate the information's transclassification from the RD category and its declassification process governed by the Secretary of Energy under the Atomic Energy Act.

b. Automatic Declassification Prohibition. Automatic declassification of documents containing TFNI is prohibited. Documents marked as containing TFNI are excluded from the automatic declassification provisions of E.O. 13526 until the TFNI designation is properly removed by DOE. When DOE determines that a TFNI designation may be removed, any remaining information classified under E.O. 13526 must be referred to the appropriate agency in accordance with the declassification provisions of E.O. 13526 and 32 CFR.

14. Marking of Electronic Storage Media. Classified computer media such as Universal Serial Bus (USB) removable storage devices, hard drives (external or internal), Compact Disc (CD) Read-only Memory (ROM)s, and diskettes will be marked to indicate the highest overall classification of the information contained within or ever written to the media, whichever is higher.

15. Declassification Markings. A uniform security classification system requires that standard markings be applied to CNSI.

a. General Requirement. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of CNSI will not deviate from prescribed formats.

b. When Markings Cannot Be Affixed. If declassification markings cannot be affixed to specific information or materials, the OCA or derivative classifier will provide holders or recipients of the information with written instructions for marking the information.

c. Uniform and Conspicuous. Markings will be uniformly and conspicuously applied to leave no doubt about the declassified status of the information and who authorized the declassification.

d. Required Markings. The following markings will be applied to records, or copies of records, regardless of media:

(1) The word, "Declassified;"

(2) The identity of the declassification authority, by name and position, or by personal identifier, or the title and date of the declassification Guide. If the identity of the declassification authority must be protected, a personal identifier may be used or the information may be retained in agency files.

(3) The date of declassification; and

(4) The lining out with an "X" or straight line of overall classification markings that appear on the cover page or first page. An example might appear as:

~~**SECRET**~~
Declassified by David Smith, Chief, Division 5, August 17, 2008.

16. Automatic Declassification Exemption Markings.

a. Marking Information Exempted from Automatic Declassification at 25 Years.

(1) When the ISCAP has approved an agency proposal to exempt permanently valuable information from automatic declassification at 25 years, the "Declassify On" line will be revised to include the symbol ''25X'' plus the number(s) that corresponds to the category(ies) in section 3.3(b) of E.O. 13526. Except for when the exemption pertains to information that will clearly and demonstrably be expected to reveal the identity of a confidential human source, or a human intelligence source, or key design concepts of weapons of mass destruction, the revised "Declassify On" line will also include the new date for declassification as approved by the ISCAP not to exceed 50 years from the date of origin of the record. Records that contain information, the release of which will clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source, or key design concepts of weapons of mass destruction, are exempt from automatic declassification at 50 years.

(2) The pertinent exemptions, using the language of section 3.3(b) of E.O. 13526 are:

25X1: reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an

intelligence method currently in use, available for use, or under development.

25X2: reveal information that would assist in the development, production, or use of weapons of mass destruction;

25X3: reveal information that would impair U.S. cryptologic systems or activities;

25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

25X5: reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

25X6: reveal information, including FGI, that would cause serious harm to relations between the U.S. and a foreign government, or to ongoing diplomatic activities of the U.S.;

25X7: reveal information that would impair the current ability of U.S. Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

25X8: reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

25X9: violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at
25 years.

(3) The pertinent portion of the marking would appear as:

Declassify On: 25X4, 20501001

(4) Documents will not be marked with a “25X” marking until the agency has been informed that the ISCAP concurs with the proposed exemption.

(5) Agencies need not apply a “25X” marking to individual documents contained in a file series exempted from automatic declassification under section 3.3(c) of E.O. 13526 until the individual document is

removed from the file and may only apply such a marking as approved by the ISCAP under section 3.3(j) of E.O. 13526.

(6) Information containing FGI will be marked with a date in the "Declassify On" line that is no more than 25 years from the date of the document unless the originating agency has applied for and received ISCAP approval to exempt FGI from declassification at 25 years. Upon receipt of ISCAP approval, the agency may use either the 25X6 or 25X9 exemption markings, as appropriate, in the "Declassify On" followed by a date that has also been approved by ISCAP. An example might appear as:

25X6, 20600129, or 25X9, 20600627.

The marking "subject to treaty or international agreement" is not to be used at any time.

b. Marking Information Exempted from Automatic Declassification at 50 Years. Records exempted from automatic declassification at 50 years will be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the ISCAP.

(1) When the information clearly and demonstrably could be expected to reveal identity of a confidential human source or a human intelligence source, the marking will be "50X1-HUM."

(2) When the information clearly and demonstrably could reveal key design concepts of weapons of mass destruction, the marking will be "50X2-WMD."

(3) In extraordinary cases in which the ISCAP has approved an exemption from declassification at 50 years under section 3.3(h) of E.O. 13526, the same procedures as those under marking information exempted from automatic declassification at 25 years will be followed with the exception that the number "50" will be used in place of the "25."

(4) Requests for exemption from automatic declassification at 50 years from elements of the IC (to include pertinent elements of the Department of Defense (DoD)) will include a statement of support from the DNI or his/her designee. Requests for automatic declassification exemptions from elements of DoD (to include pertinent elements of the IC will include a statement of support from the Secretary of Defense or his/her designee). Requests for

automatic declassification exemptions from elements of the Department of Homeland Security (DHS) will include a statement of support from the Secretary of DHS or his/her designee.

c. Marking Information Exempted from Automatic Declassification at 75 Years. Records exempted from automatic declassification at 75 years will be automatically declassified on December 31 of the year that has been formally approved by the ISCAP.

(1) Information approved by the ISCAP as exempt from automatic declassification at 75 years will be marked "75X" with the appropriate automatic declassification exemption category number followed by the approved declassification date or event.

(2) Requests for exemption from automatic declassification at 75 years from elements of the IC (to include pertinent elements of DoD) will include a statement of support from the DNI or his or her designee. Requests for automatic declassification exemptions from elements of DoD (to include pertinent elements of the IC) will include a statement of support from the Secretary of Defense or his or her designee.

17. Declassification.

a. Automatic Declassification. All agencies that have, or had, OCA decision responsibility or maintain records determined to be permanently valuable that contain CNSI, will comply with the automatic declassification provisions of
E.O. 13526. APHIS will cooperate with NARA in managing automatic declassification of accessioned Federal records, Presidential papers and records, and donated historical materials under the control of the Archivist, NARA.

Presidential Papers, Materials, and Records.

(1) The Archivist, NARA, will establish procedures for the declassification of
Presidential, Vice-Presidential, or White House materials transferred to the legal custody of NARA or maintained in the Presidential libraries.

(2) CNSI in the Custody of Contractors, Licensees, Certificate Holders, or Grantees. Pursuant to the provisions of the National Industrial Security Program (NISP), agencies must provide security classification/ declassification guidance to such entities or individuals who possess CNSI. Agencies must also determine if

classified Federal records are held by such entities or individuals, and if so, whether they are permanent records of historical value and thus subject to section 3.3 of E.O. 13526. Until such a determination has been made by an appropriate agency official, such records will not be subject to automatic declassification, or destroyed, and will be safeguarded in accordance with the most recent security classification/declassification guidance provided by the agency.

(3) Transferred Information. In the case of CNSI transferred in conjunction with a transfer of functions, and not merely for storage, the receiving agency will be deemed to be the originating agency.

(4) Unofficially Transferred Information. In the case of CNSI that is not officially transferred as described in this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, the agency in possession will serve as the originating agency and will be responsible for actions for those records in accordance with section 3.3 of E.O. 13526 and in consultation with the Director of the National Declassification Center (NDC).

(5) Processing Records Originated by Another Agency. When an agency uncovers classified records originated by another agency that appear to meet the criteria for referral according to section 3.3(d) of E.O. 13526, the finding agency will identify those records for referral to the originating agency as described in 32 CFR.

(6) Unscheduled Records. CNSI in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.3 of E.O. 13526. CNSI in records that become scheduled as permanently valuable when that information is already more than 20 years old will be subject to the automatic declassification provisions of section 3.3 of E.O. 13526 5 years from the date the records are scheduled. CNSI in records that become scheduled as permanently valuable when that information is less than 20 years old will be subject to the automatic declassification provisions of section 3.3 of E.O. 13526 at 25 years.

(7) Temporary Records and Non-record Materials. CNSI contained in records determined not to be permanently valuable or non-record materials will be processed in accordance with section 3.6(c) of E.O. 13526.

(8) FGI. The declassifying agency is the agency that initially received or classified the information. When FGI appears to be subject to automatic declassification, the declassifying agency will determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency will also determine if another exemption under section 3.3(b) of E.O. 13526, such as the exemption that pertains to U.S. foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it will consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government prior to declassification.

(9) Assistance to the Archivist of the U.S. Agencies will consult with the Director of the NDC established in section 3.7 of E.O. 13526 concerning their automatic declassification programs. At the request of the Archivist, agencies will cooperate with the Director of the NDC in developing priorities for the declassification of records to ensure that declassification is accomplished efficiently and in a timely manner.

Agencies will consult with NARA and the Director of the NDC before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate and sufficient information about agency declassification actions, including metadata and other processing information, when records are accessioned by NARA. This data will include certification by the agency that the records have been reviewed in accordance with Public Law 105-261, section 3161 governing RD and FRD.

(10) Use of Approved Declassification Guides. Approved declassification guides are the sole basis for the exemption from automatic declassification of specific information as provided in section 3.3(b) of E.O. 13526 and the sole basis for the continued classification of information under section 3.3(h) of E.O. 13526. These guides must be prepared in accordance with section 3.3(j) of E.O. 13526 and include additional pertinent detail relating to the exemptions described in sections 3.3(b) and 3.3(h) of E.O. 13526 and follow the format required of declassification guides as described in32 CFR. During a review under section 3.3 of E.O. 13526 agencies will use these guides to identify specific information for exemption from automatic declassification. These guides or detailed declassification guidance will be made available to the NDC under section 3.7(b) of E.O. 13526 and to

appropriately cleared individuals of other agencies to support equity recognition.

(11) Automatic Declassification Date. No later than December 31 of the year that is 25 years from the date of origin, classified records determined to be permanently valuable will be automatically declassified unless automatic declassification has been delayed for any reason as provided in E.O. 13526 and 32 CFR. If the date of origin of an individual record cannot be readily determined, the date of original classification will be used instead.

(12) Exemption from Automatic Declassification at 25, 50, or 75 Years. Agencies may propose to exempt from automatic declassification specific information, either by reference to information in specific records, in specific file series of records, or in the form of a declassification Guide, in accordance with section 3.3(j) of E.O. 13526. Agencies may propose to exempt information within 5 years of, but not later than1 year before the information is subject to automatic declassification. The agency head or SAO, within the specified timeframe, will notify the Director of ISOO, serving as the Executive Secretary of the ISCAP, of the specific information being proposed for exemption from automatic declassification.

(13) Delays in the Onset of Automatic Declassification.

(a) Media that make a review for possible declassification exemptions more difficult or costly. E.O. 13526 requires the Secretary or SAO to consult with the Director of the NDC before delaying automatic declassification for up to 5 years for CNSI contained in media that make a review for possible declassification more difficult or costly. When determined by NARA or jointly determined by NARA and another agency, the following may be delayed due to the increased difficulty and cost of conducting declassification processing:

1 Records requiring extraordinary preservation or conservation treatment, to include reformatting, to preclude damage to the records by declassification processing;

2 Records that pose a potential menace to health, life, or property due to contamination by a hazardous substance; and

3 Electronic media if the media is subject to issues of software or hardware obsolescence or degraded data.

(b) Referred Records. Records containing CNSI that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies and could reasonably be expected to fall under one or more of the exemption categories of section 3.3(b) of E.O. 13526 will be identified prior to the onset of automatic declassification for later referral to those agencies. Declassification reviewers will be trained periodically on other agency equities to aid in the proper identification of other agency equities eligible for referral.

1 Information properly identified as a referral to another agency contained in records accessioned by NARA or in the custody of the Presidential libraries will be subject to automatic declassification only after the referral has been made available by NARA for agency review in accordance with 32 CFR, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of E.O. 13526.

2 Information properly identified as a referral to another agency contained in records maintained in the physical, but not legal custody of NARA will be subject to automatic declassification after accessioning and in accordance with 32 CFR, provided the information has not otherwise been properly exempted by an equity holding agency under section 3.3 of E.O. 13526.

(c) Newly Discovered Records. The Secretary or SAO must consult with the Director, ISOO, on any decision to delay automatic declassification of newly discovered records no later than 90 days from the discovery of the records. The notification will identify the records, their volume, the anticipated date for declassification, and the circumstances of the discovery. An agency may be granted up to three years from the date of discovery to make a declassification, exemption, or referral determination. If referrals to other agencies are properly identified, they will be handled as outlined above.

(d) Integral File Blocks. Classified records within an integral file block that are otherwise subject to automatic declassification under section 3.3 of E.O. 13526 will not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block. For purposes of automatic declassification, integral file blocks will contain only records dated within 10 years of the oldest record in the file block. Integral file blocks applied prior to December 29, 2009, that cover more than 10 years remain in effect until December 31, 2012, unless APHIS requests an extension from the Director of ISOO on a case-by-case basis prior to December 31, 2011, which is subsequently approved.

(e) File Series Exemptions. Agencies seeking to delay the automatic declassification of a specific series of records as defined in section 6.1(r) of E.O. 13526 because it almost invariably contains information that falls within one or more of the exemption categories under section 3.3(b) must submit their request in accordance with section 3.3(c) of E.O. 13526 to the Director of ISOO, serving as Executive Secretary of the ISCAP at least 1 year prior to the onset of automatic declassification. Once approved by the ISCAP the records in the file series exemption remain subject to section 3.5 of E.O. 13526. This delay applies only to records within the specific file series. Copies of records within the specific file series or records of a similar topic to the specific file series located elsewhere may be exempted in accordance with exemptions approved by the ISCAP.

(f) Redaction Standard. Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.3 of E.O. 13526, especially if the information that must remain classified comprises a relatively small portion of the document. Any such redactions will be performed in accordance with policies and procedures established in accordance with 32 CFR.

(g) RD and FRD. RD and FRD are excluded from the automatic declassification requirements in section 3.3 of E.O. 13526 because they are classified under the Atomic Energy Act of 1954, as amended. RD concerns:

1 The design, manufacture, or utilization of atomic weapons;

2 The production of special nuclear material, e.g., enriched uranium or plutonium; or

3 The use of special nuclear material in the production of energy.

FRD is information that is still classified under the Atomic Energy Act of 1954, as amended, but which has been removed from the RD category because it is related primarily to the military utilization of atomic weapons.

1 Any document marked as containing RD or FRD or identified as potentially containing unmarked RD or FRD will be referred to the DOE in accordance with 32 CFR.

2 Automatic declassification of documents containing RD or FRD is prohibited. Documents marked as containing RD or FRD are excluded from the automatic declassification provisions of E.O. 13526 until the RD or FRD designation is properly removed by the DOE. When the DOE determines that a RD or FRD designation may be removed, any remaining information classified under E.O. 13526 must be referred to the appropriate agency in accordance with the declassification provisions of E.O. 13526 and 32 CFR.

3 Any document containing information concerning foreign nuclear programs that was removed from the RD category in order to carry out provisions of the National Security Act of 1947, as amended, will be referred to the DOE.

4 The Secretary of Energy will determine when information concerning foreign nuclear programs that was removed from the RD category in order to carry out the provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, information concerning foreign nuclear programs (e.g., intelligence assessments or reports, foreign nuclear program information provided to the U.S. Government) will be declassified when comparable information concerning the U.S. nuclear program is declassified.

When the Secretary of Energy determines that information concerning foreign nuclear programs may be declassified, any remaining information classified under E.O. 13526 must be referred to the appropriate agency in accordance with the classification provisions of E.O. 13526 and 32 CFR.

b. Systematic Declassification Review.

(1) Agencies will establish systematic review programs for those records containing information exempted from automatic declassification. This includes individual records as well as file series of records.

(2) Agencies will prioritize their review of such records in accordance with priorities established by the NDC.

c. Declassification Guides.

(1) Preparation of Declassification Guides. Beginning one year after the effective date of 32 CFR, declassification guides must be submitted to the Director of ISOO, serving as the Executive Secretary of the ISCAP at least 1 year prior to the onset of automatic declassification for approval by the ISCAP Currently approved guides remain in effect until a new guide is approved, to the extent they are otherwise applied consistent with section 3.3(b) of E.O. 13526. The information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions must be based upon specific content and not type of document. Exemptions for general categories of information are not acceptable. APHIS must prepare guides that clearly delineate between the exemptions proposed under 32 CFR.

(2) General Content of Declassification Guides. Declassification guides must be specific and detailed as to the information requiring continued classification and clearly and demonstrably explain the reasons for continued classification. Declassification guides will:

(a) Be submitted by the Agency head or the designated SAO;

(b) Provide the date of issuance or last review;

(c) State precisely the information that the agency proposes to exempt from automatic declassification and to specifically declassify;

(d) Identify any related files series that have been exempted from automatic declassification pursuant to section 3.3(c) of E.O. 13526; and

(e) To the extent a guide is used in conjunction with the automatic declassification provisions in section 3.3 of E.O. 13526, state precisely the elements of information to be exempted from declassification to include:

1 The appropriate exemption category listed in section 3.3(b), and, if appropriate, section 3.3(h) of E.O. 13526; and

2 A date or event for declassification.

(3) Internal review and update. APHIS declassification guides will be reviewed and updated as circumstances require, but at least once every 5 years. APHIS will maintain a list of its declassification guides in use.

(4) Dissemination of Guides.

(a) Declassification guides will be disseminated within APHIS to be used by all personnel with declassification review responsibilities.

(b) Declassification guides or detailed declassification guidance will be submitted to the Director, NDC, in accordance with section 3.7(b)(3) of E.O. 13526.

d. Mandatory Review for Declassification.

(1) U.S. Originated Information.

(a) Regulations. APHIS will publish and update, as needed or required in the Federal Register regulations concerning the handling of mandatory declassification review requests, to include the identity of the person(s) or office(s) to which requests will be addressed.

(b) Processing.

1 Requests for Classified Records in the Custody of the Originating Agency. A valid mandatory declassification review request must be of sufficient

specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. Requests for broad types of information, entire file series of records, or similar non-specific requests may be denied by agencies for processing under this section. In responding to mandatory declassification review requests, APHIS will make a final determination within 1 year from the date of receipt. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable laws, those declassified portions of the requested information that constitute a coherent segment. Upon denial, in whole or in part, of an initial request, APHIS will also notify the requestor of the right to an administrative appeal, which must be filed within 60 days of receipt of the denial. When APHIS receives mandatory review requests, APHIS will conduct a line-by-line review of the record(s) for public access and will release the information to the requestor, unless that information is prohibited from release under the provisions of a statutory authority, such as, but not limited to, the Freedom of Information Act (FOIA), the Presidential Records Act, or the National Security Act of 1947.

2 Requests for Classified Records in the Custody of an Agency other than the Originating Agency. When APHIS receives a mandatory declassification review request for records in its possession that were originated by another agency, it will refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, APHIS will review the requested records in accordance with APHIS declassification guides or guides provided by the originating agency. Upon receipt of a request from APHIS, the originating agency will promptly process the request for declassification and release in accordance with this section. The originating agency will communicate its declassification determination to APHIS. APHIS is responsible for collecting all agency review results and informing the requestor of any final decision regarding the

declassification of the requested information unless a prior arrangement has been made with the originating agency.

3 Appeals of Denials of Mandatory Declassification Review Requests. The Agency appellate authority will normally make a determination within 60 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority will notify the requester of the additional time needed and provide the requester with the reason for the extension. The Agency appellate authority will notify the requestor, in writing, of the final determination and of the reasons for any denial. The appellate authority must inform the requestor of his/ her final appeal rights to the ISCAP

4 Appeals to the Interagency Security Classification Appeals Panel (ISCAP). In accordance with section 5.3(c) of E.O. 13526, the ISCAP will publish in the Federal Register the rules and procedures for bringing mandatory declassification appeals before it.

5 Records Subject to Mandatory Declassification Review. Records containing information exempted from automatic declassification in accordance with section 3.3(c) of E.O. 13526 are still subject to the mandatory declassification review provisions of section 3.5 of E.O. 13526.

(c) FGI. Except as provided in this paragraph, agencies will process mandatory declassification review requests for classified records containing FGI in accordance with this section. The declassifying agency is the agency that initially received or classified the information. When FGI is being considered for declassification, the declassifying agency will determine whether the information is subject to a treaty or international agreement that does not permit automatic or unilateral declassification. The declassifying agency or the Department of State, as appropriate, may consult with the foreign government(s) prior to declassification.

(d) Cryptologic Information. Mandatory declassification review requests for cryptologic information will be processed in accordance with special procedures issued by the Secretary of Defense and, when cryptologic information pertains to intelligence activities, the DNI.

(e) Intelligence Information. Mandatory declassification review requests for information pertaining to intelligence sources, methods, and activities will be processed in accordance with special procedures issued by the DNI.

(f) Fees. In responding to mandatory declassification review requests for classified records, the Secretary may charge fees in accordance with 31 U.S.C. 9701 or relevant fee provisions in other applicable statutes.

(g) Requests Filed Under Mandatory Declassification Review and the FOIA. When a requester submits a request both under mandatory declassification review and under FOIA, APHIS will require the requestor to select one process or the other. If the requestor fails to select one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory declassification review.

(h) FOIA and Privacy Act Requests. E.O. 13526 requires that the Secretary process requests for declassification that are submitted under the provisions of FOIA, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

(i) Redaction Standard. APHIS will redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction. The specific reason for the redaction, as provided for in section 1.4 or 3.3(b) of E.O. 13526, as applicable, must be included for each redaction. Information that is redacted due to a statutory authority must be clearly marked with the specific authority that authorizes the redaction. Any such redactions will be performed in accordance with policies and procedures established in accordance with 32 CFR.

(j) Limitations on Requests. Requests for mandatory declassification review made to an element of the IC by anyone other than a citizen of the U.S. or an alien lawfully

admitted for permanent residence, may be denied by the receiving IC element. Documents required to be submitted for pre-publication review or other administrative process pursuant to an approved nondisclosure agreement are not subject to mandatory declassification review.

e. Referrals. Referrals are required under sections 3.3(d)(3) and 3.6(b) of E.O. 13526 in order to ensure the timely, efficient, and effective processing of reviews and requests and in order to protect CNSI from inadvertent disclosure.

(1) Automatic Declassification. The referral process for records subject to automatic declassification entails identification of records containing CNSI that originated from other agencies or the disclosure of which would affect the interests or activities of other agencies. Those records that could reasonably be expected to fall under one or more of the exemptions in section 3.3(b) of E.O. 13526 are eligible for referral. The referral process also entails formal notification to those agencies, making the records available for review by those agencies, and recording final agency determinations.

(a) In accordance with section 3.3(d)(3) of E.O. 13526, the identification of records eligible for referral is the responsibility of the primary reviewing agency and will be completed prior to the date of automatic declassification established by section 3.3(a) of E.O. 13526.

(b) Except as otherwise determined by the Director of the NDC, primary reviewing agencies will utilize the Standard Form 715, “Government Declassification Review Tab," to tab and identify any Federal record requiring referral and record the referral in a manner that provides the referral information in an NDC database system.

(c) Notification of referral of records accessioned into NARA or in the custody of the presidential libraries, and making the records available for review, is the responsibility of NARA and will be accomplished through the NDC.

(d) Within 180 days of the effective date of this provision, the NDC will develop and provide the affected agencies with a comprehensive and prioritized schedule for the resolution of referrals contained in accessioned Federal records and Presidential records. The schedule will be developed in

consultation with the affected agencies, consider the public interest in the records, and be in accordance with the authorized delays to automatic classification set forth in section 3.3(d) of E.O. 13526. The initial schedule will cover the balance of the first effective fiscal year and 4 subsequent fiscal years. Thereafter, the schedule will cover 5 fiscal years. The NDC will consult with the affected agencies and update and provide such schedules annually.

(e) The NDC will provide formal notification of the availability of a referral to the receiving agency and records will be subject to automatic declassification in accordance with the schedule promulgated by the NDC in subsection (4) above, unless the information has been properly exempted by an equity holding agency under section 3.3 of E.O. 13526.

(f) Records in the physical but not legal custody of NARA will be subject to automatic declassification after accessioning and in accordance with subsections above.

(g) Agencies that establish a centralized facility as described in section 3.7(e) may make direct referrals provided such activities fall within the priorities and schedule established by the NDC and the activity is otherwise coordinated with the NDC. In such cases, the centralized facility is responsible for providing formal notification of a referral to receiving agencies and for making the records available for review or direct formal referral to agencies by providing a copy of the records unless another mechanism is identified in coordination with the NDC. Referrals to agencies from a centralized agency records facility as described in section 3.7(e) of E.O. 13526 will be automatically declassified up to three years after the formal notification has been made, if the receiving agency fails to provide a final determination.

(h) Records marked as containing RD or FRD or identified as potentially containing unmarked RD or FRD will be referred to the DOE through the NDC. If the DOE confirms that the document contains RD or FRD, it will then be excluded from the automatic declassification provisions of E.O. 13526 until the RD or FRD designation is properly removed.

1 When the DOE provides notification that a RD or FRD designation is not appropriate or when it is

properly removed, the record will be processed for automatic declassification through the NDC.

2 In all cases the subject of an access demand made pursuant to E.O. 13526 or provision of law, the information classified pursuant to Executive order (rather than the Atomic Energy Act, as amended) must stand on its own merits.

(i) The NDC, as well as any centralized agency facility established under section 3.7(e) of E.O. 13526, will track and document referral actions and decisions in a manner that facilitates archival processing for public access. Central agency facilities must work with the NDC to ensure documentation meets NDC requirements, and transfer all documentation on pending referral actions and referral decisions to the NDC when transferring the records to NARA.

(j) In all cases, receiving agencies will acknowledge receipt of formal referral notifications in a timely manner. If a disagreement arises concerning referral notifications, the Director, ISOO, will determine the automatic declassification date and notify the SAO, as well as the NDC or the primary reviewing agency.

(k) Remote Archives Capture (RAC). Presidential records or materials scanned in the RAC process will be prioritized and scheduled for review by the NDC. The initial notification will be made to the agency with primary equity, which will have up to 1 year to act on their information and to identify all other equities eligible for referral. All such additional referrals in an individual record will be made at the same time, and once notified by the NDC of an eligible referral, such receiving agencies will have up to 1 year to review the records before the onset of automatic declassification.

(2) Agencies eligible to receive referrals. The Director of ISOO will publish annually a list of those agencies eligible to receive referrals for each calendar year.

(3) Systematic declassification review. The identification of equities will be accomplished in accordance with section (b) of this part. Priorities for review will be established by the NDC.

(4) Identification of interests other than national security. Referrals under sections 3.3(d)(3) and 3.6(b) of E.O. 13526 will be assumed to be intended for later public release unless withholding is otherwise authorized and warranted under applicable law. If a receiving agency proposes to withhold any such information, they must notify the referring agency at the time they otherwise respond to the referral. Such notification will identify the specific information at issue and the pertinent law.

f. Discretionary Declassification.

(1) In accordance with section 3.1(d) of E.O. 13526, agencies may declassify information when the public interest in disclosure outweighs the need for continued classification.

(2) Agencies may also establish a discretionary declassification program that is separate from their automatic, systematic, and mandatory review programs.

CHAPTER 4

SAFEGUARDING

1. General Requirements.

   a. Classified National Security Information (CNSI), regardless of its form, will be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification and will be secured under conditions adequate to prevent access by unauthorized persons. These standards are established in Executive Order (E.O.) 13526, 32, Code of Federal Register (CFR), the National Industrial Security Program Operating Manual (NISPOM) and U.S. Department of Agriculture (USDA) Departmental Manual (DM) 3440-001. Exceptions to these requirements within the Animal and Plant Health Inspection Service (APHIS) can be requested by the Personnel and Document Security Division (PDSD) through the APHIS Information Security Specialist (ISS).

   b. Items such as unclassified forms or documents not related to classified materials or documents will not be stored in the same container drawer used to safeguard CNSI.

   c. CNSI will only be stored in a Government Services Administration (GSA) approved security container in a Secure Area accredited by the ISS or PDSD.

   d. Security requirements for Sensitive Compartmented Information Facilities SCIFs) are established by Intelligence Community Directive (ICD) 705 and its appendices. Additional requirements are imposed for the storage of SCI information and will require accreditation from the Central Intelligence Agency (CIA).

   e. Current holdings of classified material will be maintained at the minimum level required for mission accomplishment. Classified information no longer required will be destroyed or transferred to the National Archives and Records Administration (NARA) to reduce classified holdings.

   f. Except for Foreign Government Information (FGI), APHIS may adopt alternative measures, using risk management principles, to protect against loss or unauthorized disclosure when necessary to meet operational requirements if approved in writing by the ISS.

      (1) When alternative measures are used for other than temporary, unique situations the alternative measures will be documented and provided to the PDSD by the ISS.

(2) Upon request, the description will be provided to Programs with which CNSI or secure facilities are shared.

(3) In all cases, the alternative measures will provide protection sufficient to reasonably deter and detect loss or unauthorized disclosure.

(4) Risk management factors considered will include sensitivity, value, and crucial nature of the information, analysis of known and anticipated threats, vulnerability, and countermeasure benefits versus cost.

g. North Atlantic Treaty Organization (NATO) classified information will be safeguarded in compliance with U.S. Security Authority for NATO (USSAN) 1-07.

h. FGI will be safeguarded as described herein for U.S. information except as required by an existing treaty, agreement or other obligation.

(1) When the information is to be safeguarded pursuant to an existing obligation, the additional requirements outlined in 32 Code of Federal Register (CFR) may apply to the extent they were required in the obligation as originally negotiated or are agreed upon during amendment.

(2) Negotiations on new obligations or amendments to existing obligations will strive to bring provisions for safeguarding FGI into accord with standards for safeguarding U.S. information as described in 32 CFR.

2. Responsibilities of Holders. Authorized persons who have access to CNSI are responsible for:

a. Protecting it from persons without authorized access to the information to include securing it in GSA-approved security containers whenever it is not under the direct control of an authorized person;

b. Meeting safeguarding requirements prescribed by thisManual; and

c. Ensuring that CNSI is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

3. Access. No employee has a right to gain access to CNSI solely by virtue of title, position, or level of security clearance.

a. A person may have access to CNSI provided that:

(1) A favorable determination of eligibility for a security clearance (equal to or higher than marked classified material) is granted;

(2) The person has signed an Standard Form (SF)-312, Classified Information Non-Disclosure Agreement; and

(3) The person has a valid need-to-know.

b. Before CNSI is disclosed, the holder must:

(1) Verify the recipient's security clearance;

(2) Determine the recipient's valid need-to-know;

(3) Verify the recipient's identification; and

(4) Advise the recipient of the classification level of the information.

c. The final responsibility for determining whether an individual obtains access to CNSI rests with the individual who has possession, knowledge, or control of the information and not with the prospective recipient.

d. CNSI will remain under the control of the originating agency or its successor in function. APHIS personnel will not disclose information originally classified by another agency without its authorization. The Secretary may waive this requirement for specific information originated within the USDA.

e. An official, employee, or contractor leaving APHIS facilities may not remove CNSI from APHIS' control without proper authorization. Personnel transporting CNSI outside APHIS facilities must be trained and approved by the ISS as a classified courier.

f. Safeguarding During Working Hours.

(1) CNSI removed from its storage container will be kept under constant surveillance and/or control by persons with authorized access.

(2) When not in use, the material will be physically protected and secured from unauthorized view of its classified content until returned to a GSA-approved security container.

(a) Such protection will be provided by the material's unclassified cover and/or by an appropriate cover sheet.

(b) Cover sheets to be used are SF 703, 704, and 705 for Top Secret (TS), Secret (S), and Confidential (C) documents respectively.

(c) Cover sheets for these purposes will be maintained and available for use in all APHIS Secure Areas.

(3) Normal working hours for Secure Areas are 7 a.m. to 5 p.m. Monday through Friday.

(a) Working in a Secure Area beyond normal hours of operation will require approval from the local Information Security Coordinator (ISC). The ISC will contact the facility security guards and inform them of personnel working past normal hours.

(b) When work is completed, personnel will secure CNSI inside a GSA-approved security container. They will conduct a check of the area to ensure all CNSI is secured, turn off the light(s), ensure the door is securely closed, and contact the local ISC and/or facility security guards to inform him/her that the room is secured.

4. Secure Areas.

a. Secure Areas are normally defined as Closed Storage Secure Areas. When the room is not occupied by an authorized person, all CNSI materials and equipment stored in the Secure Area (documents, laptops, KSV-21 cards, etc.) will be secured in a GSA-approved security container and all secure networks will be secured from access.

b. Accreditations are required prior to the use of Secure Areas for the storage, discussion, or processing of classified information. Refer to the appendices of this Manual for the forms associated with an accreditation request. Guidance for physical security requirements for the Secure Area can be provided by the ISS.

(1) If an activity determines a Secure Area is required, it must prepare a written request identifying the:

(a) Reason for the request;

(b) The location;

(c) The highest level of CNSI to be stored, discussed, or processed (Confidential, Secret, or Top Secret);

(d) A brief description of the program requirements to include (as applicable):

1 Storage;

2 Secure communications or discussion;

3 Classified material review; and/or

4 Classified processing.

(e) A point of contact for the request.

(2) The following documentation will accompany the request:

(a) Alarm certifications (Underwriters Laboratory ((UL)) 2050);

(b) Proposed standard operating procedures; and

(c) Room construction specifics (electrical diagram, plumbing and construction materials to be utilized)

(3) Requests will be processed through the ISS to PDSD. If approved, accreditation will be awarded by a memorandum citing:

(a) The specific location;

(b) Building number or other identifier;

(c) Room number;

(d) Highest level of CNSI authorized to be stored, viewed, discussed, etc. in the Secure Area;

(e) Restrictions, if any; and

(f) Other information deemed appropriate.

(4) Accreditations will be valid for three years from the date of the approval memorandum. The program responsible for the Secure Area must request, through the ISS to the PDSD, any construction, modification, or classification level changes involving the room prior to implementation.

(5) Reaccreditation.

(a) Secure Areas Require Reaccreditation Every Three Years. The Program responsible for the Secure Area will request reaccreditation of all accredited areas in their area of responsibility by providing the appropriate information using the Accreditation Status Form (Appendix B) and forwarding it to the ISS. The ISS will complete the appropriate information in Section B and return it to the responsible Program.

(b) The reaccreditation will consist of a review of the Secure Area for continued compliance of all pertinent policies and procedures.

(6) If an accredited area is no longer required, the responsible Program will request an accreditation withdrawal by completing the appropriate information in Section A of the Accreditation Status Form and forward it to the ISS. The ISS will complete the appropriate information in Section C and return it to the responsible Program.

c. The ISS will maintain a database of all accredited Secure Areas and their accreditation status.

d. Access.

(1) Access to Secure Areas will be controlled to preclude unauthorized entry. This may be accomplished through the use of a cleared employee authorized escorted entry, acting as an escort, or by an access control device or system.

(2) Unescorted access will be limited to authorized persons who have an appropriate level security clearance and a valid need-to-know for the classified material within the area.

(3) Persons without the appropriate level security clearance and valid need-to-know will be escorted at all times by an authorized person after all classified material in the area has been properly secured from view and/or access.

(4) Access requests to secure networks will be forwarded to the USDA Office, Chief Information Officer (OCIO) through the ISS.

(a) Requestor must possess, at a minimum, a current Secret security clearance.

(b) Access requests must be approved the Department of Homeland Security (DHS).

(c) Before being granted access to secure networks, the requestor must complete Derivative Classifier Training through the ISS.

e. Escorting Policy.

(1) Only authorized personnel with a valid USDA identification, appropriate clearance, recognized valid need-to-know, and valid justification for access into Secure Areas will be authorized unescorted access into Secure Areas. All other personnel must sign in and be escorted. The following are not authorized to perform escort duties:

(a) Non-APHIS employees,

(b) Contractors,

(c) Maintenance personnel, and/or

(d) Delivery personnel.

(2) The escort must be knowledgeable of escorting requirements and Directives, and assume responsibility for the visitor(s) at all times while occupying the Secure Area.

(3) The escort must observe all security rules and regulations and will ensure escorted personnel comply with APHIS Instructions and Directives for the Secure Area.

(4) The escort must maintain visual contact with escorted personnel at all times and must be in a position to control the movement and actions of escorted personnel.

(5) The escort must remain with visitors at all times until they are turned over to another authorized escort or leave the Secure Area.

(6) The ratio for escorting groups is one escort per five escorted persons.

(7) Escorts need to ensure the area is sanitized prior to allowing access by escorted personnel. The escort will ensure:

(a) Security containers are locked or drawers closed;

(b) Classified data is not visible on a computer screen;

(c) Classified documents are secured/covered from view;

(d) No classified discussions are held in the presence of visitors; and

(e) Reproduction machines, facsimiles, and printers are free of classified materials.

(8) APHIS employees whose clearances are suspended will be escorted at all times, as described above.

(9) Visitors who have not yet had their security clearance passed by their security office will be treated as uncleared visitors and escorted at all times.

(10) A visitors log will be maintained to account for escorted visitors in the space and maintained by the ISC or ISS for a minimum of 90 days.

(11) Challenges.

(a) It is the responsibility of all employees and contractors who observe an uncleared/unescorted individual within a Secure Area, to become an escort to that person.

(b) The uncleared person without an escort must be detained while the local ISC or facility security guard is called to respond to the area, or the individual must be escorted out of the area.

f. Construction of Secure Areas.

(1) All construction must be completed to provide visual evidence of unauthorized penetration.

(a) Perimeter walls will be true floor to true ceiling, permanently constructed and attached to each other at the top and bottom.

(b) All walls will be constructed, at a minimum, with two layers of drywall. The drywall will be affixed with one layer in a vertical and the next layer in a horizontal pattern. The ends and seams will be staggered, filled, and smooth finished.

(c) If classified processing will take place in the Secure Area one layer of the drywall will be foil-backed to prevent the electronic emissions from emanating from the area.

(d) All openings, to include spaces around ventilation systems, pipes, conduit, etc. will be filled.

(e) All walls will have insulation installed that, coupled with the drywall, meets Sound Transmission Class (STC) 45 or higher standards.

(2) All doors affording entrance to the Secure Area will be constructed of wood, metal, or other solid material. Doors will be secured with a lock meeting Federal Specification FF-L-2740A.

(a) Doors other than those secured with the aforementioned locks will be secured from the inside with emergency egress hardware that is building and fire code compliant.

(b) The combination for the lock will be classified at the highest level of classification accreditation for the room and protected accordingly.

(c) The door will be alarmed; the alarm signal must be monitored at an area providing 24/7 coverage and response to the area.

(3) All windows which might reasonably afford visual observation of classified activities within the Secure Area will be made opaque or equipped with blinds, drapes, or other coverings.

(a) Windows at ground level will be constructed from or covered with materials to provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

(b) Windows that open and close will be made inoperable either by sealing them or equipping them on the inside with a locking mechanism.

(c) The windows will be monitored by an Intrusion Detection System (IDS) (either independently or by the motion detection sensors within the area).

(4) All openings, to include ventilation ducts, into the area larger than 96 square inches will be protected by steel grating or steel bars a minimum of 1/2 inch in diameter not more than 6 inches apart.

(5) Ventilation ducts will have a "Z" duct installed into the system between the entry/exit wall(s) and the first opening into the room for sound attenuation.

(a) Ventilation ducts will have sound attenuation rubber gasketing installed in close proximity to the entry/exit walls.

(b) Ventilation ducts will have an inspection port installed no more than 6 inches from the wall to afford visual inspection of installed bars or grates, if present.

(c) All conduit, fire suppression pipes, water pipes, and similar metal devices entering into the room will be clamped and grounded for sound attenuation purposes.

g. SF 702, Security Container Check Sheet. An SF 702 will be placed on the exterior of the entry door to record each time the door is locked, unlocked, or checked. A sample of the SF 702 is provided in Appendix O. The individual conducting such actions will include their initials and the time in the applicable part of the form.

(1) The “Checked By” column will be used every time that the Secure Area is occupied to conduct work ensuring that the Area was not left open accidentally.

(2) The “Guard Check” column is used for annotating checks by guard force members.

(3) The individual who conducts the end-of-the-day check must ensure the door is properly locked and secured by attempting to open the door and then spinning the combination dial at least one full rotation left and one full rotation right. Although it is not always possible, the person conducting the end-of-the-day check will not

be the same person who locked or unlocked the door during the duty day.

(4) Reversible OPEN-CLOSED signs, or similar signs, will be used as a reminder each time the door is locked or unlocked.

h. Secure Telephone Equipment (STE).

(1) STEs and associated KSV 21 cards are obtained by the Communications Security (COMSEC) Manager through the ISS and are authorized for use at the classification level up to the accreditation of the KSV 21. NOTE: the STE can only be used at the highest level of the accreditation of the Secure Area; example: if the Secure Area is accredited to the Secret level, the highest level of STE/KSV 21 used in the Secure Area is Secret.

(2) The room must meet the appropriate sound attenuation requirements and be accredited for the discussion of CNSI.

(3) When not in use, the KSV-21 card for the STE must be removed from the phone and

(a) Secured in a GSA-approved security container if stored in the Secure Area; or

(b) Secured in a locked device (cabinet, desk, etc.) when stored outside of the Secure Area.

i. Classified Processing. Classified computer processing is authorized with approval of a System Security Plan (SSP) for stand-alone systems only. If connected to an Homeland Security Defense Network (HSDN) or similar system, the area must meet the standards of, and approved by, the DHS and PDSD.

j. TS Secure Storage and Supplemental Protection:

(1) TS information will be stored in a GSA-approved security container with one of the following supplemental controls:

(a) Twenty-four hour protection by cleared personnel;

(b) Inspection of the security container will occur every 2 hours by cleared guard or duty personnel authorized access to the area;

(c) An IDS with the personnel responding within 15 minutes of the alarm annunciation; and/or

(d) PDSD approved security-in-depth conditions provided the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740A.

(2) Secret information will be stored by one of the following methods when not in use or if the area is unoccupied:

(a) In the same manner as prescribed for TS information; or

(b) In a GSA-approved class 5 or 6 (letter or legal size) security container or vault without supplemental controls.

5. Security Containers.

a. New equipment will be procured from those items listed on the GSA Federal Supply Schedule, with approval of the ISS. The GSA establishes and publishes minimum standards and specifications for safes, containers, vault doors, and associated equipment suitable for the storage and protection of CNSI. The following five companies currently or have historically manufactured safes and containers which meet GSA-established standards. No other companies will be used to procure security containers:

(1) Diebold, Inc

(2) Hamilton Products Group, Inc

(3) Alpha

(4) Fedsafe

(5) Mosler

b. CNSI must be stored under conditions that will provide adequate protection and prevent access by unauthorized persons.

(1) Whenever classified information is not under the personal control and observation of a cleared person, it must be stored in an accredited open storage area or in a GSA- approved class 5 or 6 (legal or letter size) security container equipped with a locking meeting FF-L-2740A specifications.

(2) The ISS or ISC may determine more stringent requirements are needed based on the volume, nature, and sensitivity of the information to be protected in relation to other factors, such as types of containers, presence of guards, vault-type space, or intrusion alarms.

c. There will be no external markings revealing the level of CNSI authorized or stored in a given container or vault, or to the priority assigned to the container for emergency evacuation and destruction.

(1) No stickers or similar devices will be affixed to the exterior of the container.

(2) No equipment or items will be placed on the top of the container.

(3) Mark(s) or symbol(s) on the container for other purposes (e.g., identification and/or inventory number or barcode) are authorized.

(4) No marking will be affixed to the container identifying the level of information contained within or authorized for storage.

d. An office that receives CNSI (in any form), and does not possess a GSA-approved security container for storage/protection must do one of the following:

(1) Return the CNSI to the sender;

(2) Arrange with another office to properly store the information in a GSA-approved security container; or

(3) Destroy it through the use of an National Security Agency (NSA)-approved device.

e. Under no circumstances will CNSI be left unattended, stored in an unauthorized security container, taken to a personal residence, or placed in the custody of a person who does not have the proper security clearance or a valid need-to-know.

f. Weapons or items such as funds, jewels, precious metals, or drugs, will not be stored in the same container used to safeguard CNSI.

g. The security container must not be covered in any manner.

h. Combinations.

(1) Access to and protecting classified combinations.

(a) Only appropriately cleared and authorized employees will have access to, or knowledge of, classified combinations.

(b) The number of employees with access to the combination will be kept to a minimum (normally two to three) and be clearly identified on the SF-700, Security Information Form. A sample of the SF-700 is provided in Appendix M.

(c) Combinations will not be provided to anyone who is not identified on the SF-700 with the exception of the ISS or PDSD.

(d) The classification of combination locks will be equal to the highest level of CNSI that is protected by the lock (e.g., the combination of a lock used for securing Secret materials must be classified as Secret).

(e) Any written record of the combination will be marked with, and protected at, the appropriate classification level.

(f) Combinations are not to be recorded on any unsecured forms; i.e. calendars, on rolodex lists, in desk drawers, in key-locked filing cabinets, in wallets, on unclassified computer files, or stored at home or similar manner.

(g) Copies of all combinations will be provided to the ISS for the purpose of emergency entry and/or in the event the combination is required.

(h) A record of each container's information and combination must be maintained on an SF-700.

1 Attachment 1 to the SF-700 identifies the current location of the container, the name, home address, and home telephone number of each individual responsible for, and having access to, the combination. Attachment 1 to the SF-700 remains with the security container and will be attached to the inside of the control drawer.

2 Attachment 2 to the SF-700 is the sealed envelope portion of the form that documents a record of the classified combination. The perforated combination section of the SF-700 will be

completed recording the combination, detached, and sealed in the envelope portion of the form. The envelopes will be marked top, bottom, front and back with the appropriate classification.

3 Attachment 2 will be provided to the ISS.

(i) The ISS will maintain an SF-700 record for each vault, open storage area, or container used for storing CNSI in their area of responsibility, provided they have the means to store the combinations at the protection level required by the classification of the information within the safe or container.

(2) Changing Classified Combinations.

(a) Combinations will be changed only by the persons with the appropriate level security clearance and a valid need-to-know for access to the Secure Area or security container contained therein. The ISS may also change combinations upon request of the responsible office.

(b) Combinations will be changed:

1 Whenever the container, individual container drawer, or Secure Area door is first placed into use;

2 Each time a person with knowledge of the combination no longer requires access to it or knowledge of it, unless other sufficient controls exist to prevent access to the lock;

3 When the combination has been subject to possible or actual compromise; or

4 At least once every three years.

(c) When a container is taken out of service, it will be inspected by the responsible office to ensure that no CNSI remains. The combination lock will be reset to the unclassified combination "50-25-50" prior to removal from the Secure Area.

(d) Selecting Combinations.

1 Combinations for each lock will be unique to that lock and will have no systematic relationship to other combinations used by a specific office.

2 Combination numbers will not be derived from numbers otherwise associated with the specific office or its employees; for example room numbers.

3 The numbers of a combination will be selected on a random basis without deliberate relationship to the other except to provide appropriate variance to operate the lock properly; example: 01-02-03.

(e) Declassification of combinations occurs at the time they are changed. Unless completed by the ISS, ensure the ISS is notified of the change to ensure the Part 2 of the old SF 700 is properly destroyed. Provide a Part 2 of the SF 700 identifying the new combination to the ISS for record.

(4) Reversible OPEN-CLOSED signs, or similar signs, will be used as reminders on all classified storage container drawers each time they are locked or unlocked.

i. Repair of Damaged Security Containers. Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for the storage of CNSI will be accomplished only by authorized persons who have been the subject of a trustworthiness determination. Contact the ISS for guidance.

6. Information Controls.

a. Top Secret.

(1) Top Secret Document Control Officer (TSCO). TSCOs and at least one alternate will be designated within offices that prepare, receive, store, or handle TS information.

(a) TS material received by APHIS program offices must be logged in by the TSCO and then receipted to the appropriately cleared person.

(b) All TSCOs and alternates must possess a TS clearance (interim clearance is not acceptable for this position).

(c) TSCOs will be selected on the basis of experience and reliability.

(d) TS material must be taken to the TSCO or alternate for accountability on an AD Form 147.

1 TS Registers will be retained for 5 years from the date of the disposition of the last item on each sheet.

2 As a minimum, the TS Register will reflect the following:

a Document Control Number. A control number identifiable with the Program or Activity receiving the document will be assigned to all TS documents upon receipt. While not recommended, past practice has permitted assigning the same control number to all copies of the document. The control number will consist of the organizational code, a sequentially assigned number beginning with "0001" and the last two digits of the calendar year in which received.

b Date of Receipt. The date of the document or date the material was received.

c Unclassified Title or Description Sufficient to Adequately Identify the TS Document or Material. This description includes the unclassified title or appropriate short title, date of the document, serial number, and copy number(s).

d Originating Agency. Name of the originating agency or the agency the document was received from.

e Disposition. The file location, receipt number, destruction certificate, downgrading or declassification disposition, and disposition date, as appropriate.

f Serialization and Copy Numbering. TS documents originated and derivatively classified by APHIS activities that are numbered serially. In addition, each TS

document will be marked to indicate its copy number, for example, copy 1 of 2 copies.

(2) Disclosure Records. The TSCO will maintain a, GSA Form 1566, Top Secret Access Record, appended to each TS document or material. Record the name, title, and signature of all individuals, including stenographic and clerical personnel, to whom information in the document has been disclosed, and the date of disclosure. The GSA Form 1566 will:

(a) Remain attached to the document until the document is downgraded, transmitted outside APHIS, or destroyed; and

(b) Be retained 5 years from the disposition date of the document.

(3) Inventories. All TS documents and material will be inventoried semi-annually or more frequently where circumstances warrant.

(a) The inventory will reconcile the TS accountability register with the documents or material on hand. Each document or material will be examined for completeness.

(b) A report will be submitted to the ISS by the TSCO within 3 working days from the requested date of the inventories and will include any unresolved discrepancies, total number of documents by location, and the total number of documents derivatively classified during the previous 6 months.

(4) Retention. TS information will be retained only to the extent necessary to satisfy mission requirements.

(a) TSCOs will destroy copies of TS documents when they are no longer needed.

(b) Record copies of documents that cannot be destroyed will be, when appropriate, retired to designated records centers.

(5) Receipt. TS documents and material will be accounted for by a continuous chain of receipts using Form 1566. Receipts will be maintained for 2 years.

b. Secret and Confidential.

(1) All offices maintaining Secret or Confidential CNSI must conduct an annual review of their classified holdings. Each document must be visually inspected to determine possible downgrade, declassification, or destruction of classified holdings to reduce the amount necessary for operational requirements. The results of this annual review will be forwarded to the ISS.

(2) Retention. CNSI will be retained only to the extent necessary to satisfy mission requirements.

(a) Custodians will destroy non-record copies of classified documents when no longer needed.

(b) Record copies of documents that cannot be destroyed will be, when appropriate, retired to designated records centers.

7. Reproduction.

a. Reproduction of all CNSI will be held to the minimum consistent with operational requirements.

b. New technology available for copiers increases security vulnerabilities. The term copier refers to photocopying machines, facsimile machines, printers that produce hard copy output, electronic blackboards that provide a reproduction of what is written on the board, and any machine with a combination of these functions.

c. The following security precautions will be observed to prevent the possible compromise of CNSI as a result of copier use or other duplicating means:

(1) Reproduction will be accomplished by authorized persons knowledgeable of the procedures for classified reproduction;

(2) Unless restricted by the originating agency Secret and Confidential information may be reproduced to the extent required by operational needs, or to facilitate review for declassification;

(3) Copies of CNSI will be subject to the same safeguarding controls as the original information;

(4) TS information will not be reproduced without the consent of the originator; and

(5) Records must be maintained of reproduced TS documents to show the number, distribution, and authority for reproduction.

d. Reproduction machines within APHIS will be designated as "approved" or "non-approved" for the reproduction of CNSI if they are located in a Secure Area that contains both classified and unclassified information. After designation of a copier as "approved" or "non-approved," it will be clearly identified by a posted notice.

(1) The ISS will issue classified copy machine approval letters to the office managers possessing these machines.

(2) The approval letters will identify the machine(s) that are approved, the location, and the Point of Contact (POC) in the office.

(3) The POC will be required to coordinate with the ISS when potential security problems arise, or when there are incidents of possible compromise.

e. All employees handling CNSI will be notified where the copier is located, and will ensure that the equipment is under their control when copying classified materials.

f. Disposal of Equipment. Many offices within USDA lease their equipment from the Department. A machine previously used to reproduce CNSI could be returned to the Office of Operations and later leased to another agency.

(1) Offices using equipment for classified reproduction must take precaution to avoid inadvertently disclosing CNSI left on this equipment prior to the transfer or removal of the equipment.

(2) Secure fax machines, printers, and copiers used to reproduce classified materials must be properly cleared to ensure there are no latent images on the equipment before disposing of the equipment by running a blank sheet of paper through the machine at least three times.

(3) Contact the ISS to coordinate the disposal of equipment used for classified reproduction and processing.

g. Designated classified copying machines will be located in an accredited Secure Area to deny access by unauthorized users.

h. Remote diagnostic capabilities of classified reproduction equipment will not be utilized because most copy machines have internal memory which could be accessed remotely.

i. When used, authorized individuals will remain at the equipment until classified reproduction is complete.

(1) Before leaving the equipment, individuals must check the copier for any copies or originals that may be left in the copier.

(2) If the equipment malfunctions and cannot be cleared or the copies cannot be retrieved, the ISS will be notified to ensure that the machine is removed from service until the supervising office manager certifies that the malfunction has been properly cleared, at which time, the machine may be re-certified for classified reproduction.

j. Copiers used to reproduce CNSI will not be connected to any network or telephone line.

k. Servicing. The local ISC will be notified of the scheduled service visit and arrange for an appropriately cleared employee to be present.

(1) Any documents, image retaining drum sheets, or memory chips must be removed from the machine and will be collected by the ISC prior to servicing.

(2) No unescorted maintenance person will be allowed access to any reproduction equipment used for the reproduction of classified materials.

l. TS material can be reproduced only by the TSCO or Alternate TSCO.

8. Disposal and Destruction of Classified Materials.

a. Classified documents and other material will be retained only if they are required for mission requirements or if law or regulation requires their retention.

b. Documents that are no longer required will be destroyed or disposed of in accordance with the provisions of the Federal Records Act and this Manual.

c. Destruction of classified documents will be accomplished by means that eliminate the risk of reconstruction of the CNSI they contain.

(1) Classified waste material (in any form) will be appropriately protected at all times until it can be properly destroyed.

(2) Classified waste is defined as notes (working papers), carbon paper, typewriter and printer ribbons, and computer media, currently or ever, containing CNSI.

d. Official records that are considered the "record copy" must be kept in accordance with the requirements set forth by NARA and USDA Departmental Regulation (DR) 3080-001.

(1) If the material is considered the record copy, USDA records managers can provide further guidance.

(2) Non-record classified material will be destroyed as soon as it has served its intended purpose.

e. Effective January 1, 2011, only equipment listed on an Evaluated Products List (EPL) issued by the National Security Agency (NSA) may be utilized to destroy CNSI.

(1) Equipment approved for use prior to January 1, 2011, and not found on an EPL, may be utilized for the destruction of CNSI until December 31, 2016. The NSA maintains a list of approved destruction devices for classified materials. A copy of this list can be obtained from the NSA or the ISS. These devices also appear on the GSA Federal Supply Schedule.

(2) Unless NSA determines otherwise, whenever an EPL is revised, equipment removed from an EPL may be utilized for the destruction of CNSI up to 6 years from the date of its removal from an EPL.

(3) In all cases, if any such previously approved equipment needs to be replaced or otherwise requires a rebuild or replacement of a critical assembly, the unit must be taken out of service for the destruction in accordance with this section.

(4) The Administrator of General Services will, to the maximum extent possible, coordinate supply schedules and otherwise seek to make equipment on an EPL available through the Federal Supply System.

(5) Questions regarding destruction devices or their use will be directed to the ISS.

(6) Offices wishing to purchase a destruction device must contact the ISS, who will:

(a) Certify the destruction device. This can be accomplished via e-mail but must include the make/model of the device, and the proposed location for the device;

(b) Schedule revalidation of the device every three years. This will ensure that the ISS maintains a current list of approved destruction equipment within APHIS; and

(c) Maintain documented approvals by the office responsible for the device.

f. All classified materials must be destroyed by individuals holding a security clearance equal to or higher than the level of information being destroyed.

g. Classified materials must be destroyed by burning, melting, chemical decomposition, pulping, pulverizing, shredding, disintegration, or mutilation sufficient to preclude recognition or reconstruction of the CNSI.

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

(1) Machines are clearly labeled as approved for the destruction of classified material;

(2) Classified materials being destroyed are protected from casual visual observance during the destruction process; and

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

(4) APHIS will utilize shredding as the approved method of destroying classified paper material.

(a) Only NSA-approved crosscut shredders will be used for destruction of Top Secret, Secret, and Confidential information.

(b) TS material must be destroyed through the use of a crosscut shredder that turns the material into powder form; the destruction must be witnessed and recorded by the TSCO on a Form AD 471.

(c) Secret and Confidential material may be destroyed by a crosscut shredder that renders the material in pieces that do not exceed 1/32" x 3/8" in (1 mm x 5 mm). Material shredded to these specifications need no further destruction.

i. A Form AD 471 will be used for documenting the destruction of classified materials. If a Form AD 471 is not available, a list of documents being destroyed can be generated and initialed by the person conducting the destruction and one witness. A copy of the list will be provided if the destruction of TS has taken place. The list will include:

(1) The document title or number;

(2) The date of the document;

(3) The originating organization;

(4) The level of classification; and

(5) The date of the destruction.

j. Diskettes, film, CDs, USB storage devices, microfiche, slides, and hard drives (internal or external) can be sent, brought, or mailed to the ISS or PDSD for destruction.

(1) When requesting the destruction of materials by the ISS or PDSD, the material must be delivered or mailed with a copy of the Form AD 471 to ensure that there is a record of what was transferred between offices.

(2) Materials mailed to the ISS or PDSD for destruction must be properly packaged and mailed in accordance with the packaging requirements for classified materials.

k. Bulk Destruction. Burn bags can be acquired from PDSD for bulk destruction of materials. They can be used for destruction of all levels of CNSI.

(1) All burn bags will be protected at the highest level of information they contained until the contents can be properly destroyed.

(2) Place no more than 10 pounds in each bag, fold the top, and staple it shut. Care must be taken to ensure that all burn bags are stapled across the top to prevent them from opening during transit.

(3) Mark each bag with the highest classification level of the information contained inside and with the organization's name and phone number.

(4) Ensure paper documents and other types of materials such as diskettes are separated into individual bags; do not comingle paper and other types of materials in the same bag.

(5) Within the Washington, DC National Capital Region (NCR), PDSD will provide guidance to offices on bulk destruction of CNSI.

(6) If an office is not within the NCR, contact your local ISC or the APHIS ISS to locate a nearby Federal facility that has an incinerator approved for destroying CNSI. Most military installations can provide assistance in finding an approved local facility for destruction.

(7) Agencies unable to locate an approved incinerator may mail the information to the ISS or PDSD for destruction. You must contact the ISS or PDSD prior to sending classified documents for destruction and follow proper mailing procedures for classified materials.

(8) Transportation of Bulk Classified Material.

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

(b) It may be necessary for the individuals transporting the material to witness the actual destruction. Classified

material will be left at an approved facility only after clearance verification is made.

9. Safeguarding U.S. CNSI Located in Foreign Countries.

a. Except for CNSI that has been authorized for release to a foreign government or international organization and is under the security control of such government or organization, the retention of U.S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U.S. Government requirements. This includes classified material temporarily transferred into a foreign country by U.S. Government personnel authorized to escort or hand-carry such material.

b. Whether permanently or temporarily retained, the classified materials will be stored under U.S. Government control, at either the U.S. Embassy or a military base with appropriate storage capability.

10. Foreign Government Information (FGI). The requirements described below are additional baseline safeguarding standards that may be necessary for FGI, other than NATO information, that requires protection pursuant to an existing treaty, agreement, bilateral exchange or other obligation.

a. NATO CNSI will be safeguarded in compliance with USSAN 1-07.

b. To the extent practical, and to facilitate its control, FGI will be stored separately from other CNSI.

c. To avoid additional costs, separate storage may be accomplished by methods such as separate drawers of a container.

d. The safeguarding standards described below may be modified if required or permitted by treaties or agreements, or for other obligations, with the prior written consent of the National Security Authority of the originating government, hereafter "originating Government."

(1) Records will be maintained of the receipt, internal distribution, external dispatch, destruction, access, reproduction, and transmittal of foreign government TS information.

(2) Reproduction requires the consent of the originating government.

(3) Destruction will be witnessed.

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

(5) Restricted and other FGI provided in confidence. In order to assure the protection of other FGI provided in confidence (e.g., foreign government “Restricted," “Designated,” or unclassified provided in confidence), such information must be classified under E.O. 13526.

(a) APHIS, or a receiving APHIS contractor, licensee, grantee, or certificate holder acting in accordance with instructions received from the U.S. Government, will provide a degree of protection to the FGI at least equivalent to that required by the government or international organization that provided the information.

(b) When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information.

(c) If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements will be met:

1 Documents may retain their original foreign markings if the responsible agency determines that these markings are adequate to meet the purposes served by U.S. classification markings. Otherwise, documents will be marked, “This document contains (insert name of country) (insert classification level) information to be treated as U.S. (insert classification level).” The notation, “Modified Handling Authorized,” may be added to either the foreign or U.S. markings authorized for FGI. If remarking foreign originated documents or matter is impractical, an approved cover sheet is an authorized option;

2 Documents will be provided only to persons in accordance with sections 4.1(a) and (h) of E.O. 13526 and this Manual;

3 Individuals being given access to the information will be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet;

4 Documents will be stored in such a manner so as to prevent unauthorized access; and

5 Documents will be transmitted in a method approved for CNSI, unless this method is waived by the originating government.

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

f. Foreign Disclosure of CNSI.

(1) CNSI originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government or international organization of governments, or any element thereof, in accordance with statute, E.O. 13526, directives implementing E.O. 13526, direction of the President, or with the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the CNSI.

(2) Markings used to implement this section will be approved in accordance with 32 CFR.

(3) With respect to the Intelligence Community (IC), the Director, National Intelligence may issue policy directives or directives pursuant to section 6.2(b) of E.O. 13526 that modify such prior authorization.

11. Emergency Authority. Administrator, APHIS, or any designee may prescribe special provisions for the dissemination, transmission, safeguarding and destruction of classified CNSI during certain emergency situations.

a. In emergency situations, in which there is an imminent threat to life or in defense of the homeland, the Administrator, APHIS or designees may authorize the disclosure of CNSI to an individual or individuals who are otherwise not routinely eligible for access. Precautions will be taken to:

(1) Limit the amount of CNSI disclosed to the absolute minimum to achieve the purpose;

(2) Limit the number of individuals who receive it to the minimum to achieve operational requirements;

(3) Transmit the CNSI via approved Federal Government channels by the most secure and expeditious method to include those required in 32 CFR, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified, how it will be safeguarded; physical custody of CNSI must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement; and

(6) Within 72 hours of the disclosure of CNSI, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

(a) A description of the disclosed information;

(b) To whom the information was disclosed;

(c) How the information was disclosed and transmitted;

(d) Reason for the emergency release;

(e) How the information is being safeguarded; and

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

b. Information disclosed in emergency situations will not be required to be declassified as a result of such disclosure or subsequent use by a recipient.

12. Emergency Planning.

a. Plans will be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Such plans will establish detailed procedures and responsibilities for the protection of classified materials to ensure that the material does not come into the possession of unauthorized persons.

b. Emergency plans will provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement and securing of classified documents in GSA-approved security containers is the first priority.

c. In the event of an alarm malfunction, posting authorized employees around the affected area who are pre-instructed and trained to prevent the removal of classified material by unauthorized personnel is an acceptable means of protecting classified material and reducing the risk of compromise. Such plans will provide for emergency destruction to preclude capture of classified material. Emergency destruction procedures will need to be developed and posted for each storage location.

d. Properly cleared personnel will inspect classified storage containers and information processing equipment before removal from protected areas or unauthorized persons are allowed access to them. The inspection will be accomplished to ensure no CNSI remains within the equipment. Some examples of equipment that will be inspected are:

(1) Reproduction or facsimile machines and other office equipment used to process CNSI;

(2) GSA-approved security containers used for safeguarding CNSI; and

(3) Other items of equipment that may inadvertently contain CNSI.

CHAPTER 5

TRANSPORTATION METHODS

1. General. Classified National Security Information (CNSI) will be transported and received in an authorized manner which ensures that evidence of tampering can be detected, that
inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient.

2. Requirements.

   a. Persons transporting CNSI are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Manual

   b. Only appropriately cleared personnel or authorized carriers may transmit, transport, escort, or hand-carry CNSI.

   c. Unless a specific kind of transportation is restricted, the means selected will minimize the risk of a loss or compromise while permitting use of the most cost-effective mode of conveyance.

   d. Local procedures will be established to protect incoming mail, bulk shipments, and items delivered that contain classified material.

   e. All CNSI physically transported outside facilities will be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents.

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

      (2) Material used for packaging must provide durability to protect materials in transit, prevent viewing of the contents, and prevent items from breaking out of the cover.

      (3) Packages will be sealed with tape containing rayon fibers or nylon filament tape or its equivalent. These supplies can be purchased from the General Services Administration (GSA) supply services schedule.

      (4) The inner enclosure will be marked top, bottom, front, and back indicating the highest level of CNSI the enclosure contains.

(5) The outer enclosure will be the same except that no markings to indicate that the contents are classified will be visible. Intended recipients will be identified by organization, division, and/or office only as part of an attention line. The following exceptions apply:

(a) If the CNSI is an internal component of a packable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal CNSI.

(b) If the CNSI is an inaccessible internal component of a bulky item of equipment, the outside or body of the item may be considered to be a sufficient enclosure provided observation of it does not reveal CNSI.

(c) If the CNSI is an item of equipment that is not reasonably packable and shell or body is classified, it will be concealed with an opaque enclosure that will hide all classified features.

(6) Specialized shipping containers, including closed cargo transporters or diplomatic pouch may be considered the outer enclosure when used.

(7) When CNSI is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure.

f. Couriers and authorized persons designated to hand-carry CNSI will ensure that the information remains under their constant and continuous protection and that direct point-to point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF-P-110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(1) When a requirement exists for overnight delivery within the U.S. and its Territories, the use of the current holder of the GSA contract for overnight delivery of information as long as applicable postal regulations (39 Code of Federal Register ((CFR)) Chapter 1) are met. The GSA has approved nine contract carriers for overnight mail express delivery for urgent overnight transportation of Secret and Confidential material within the continental U.S. when overnight delivery cannot reasonably be accomplished by the

U.S. Postal Service (USPS). The most widely used carrier for APHIS is United Parcel Service (UPS).

(a) Any such delivery service will be U.S. owned and operated, provide automated in-transit tracking of the CNSI, and ensure package integrity during transit.

(b) The contract will require cooperation with government inquiries in the event of a loss, theft, or possible unauthorized disclosure of CNSI.

(c) The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address.

(d) The package may be addressed to the recipient by name.

(e) The release signature block on the receipt label will not be executed under any circumstances.

(f) The use of external (street side) collection boxes is prohibited.

(g) Classified Communications Security Information (COMSEC), North Atlantic Treaty Organization (NATO), and Foreign Government Information (FGI) will not be transmitted in this manner.

(h) Carrier employees will not be notified that the package contains classified material.

(i) Senders may not use a USPS Post Office Box as the destination address. Instead, a street delivery address approved for overnight shipments by the recipient's Information Security Coordinator (ISC) or security office will be used.

(j) A release signature block on the receipt label will not be executed under any circumstances.

g. Transportation methods within and between the U.S., Puerto Rico, or a U.S. Possession or Territory.

(1) Top Secret. Under no circumstances will TS information be transported via the USPS or any other cleared or uncleared commercial carrier. TS information will be transported by:

(a) Direct contact between authorized persons;

(b) The Defense Courier Service (DCS) or an authorized Government agency courier service; or

(c) A designated courier with a TS clearance trained by the APHIS Information Security Specialist (ISS)..

(2) Secret. Secret information will be transported by:

(a) Any of the methods established for TS;

(b) USPS Express Mail or USPS Registered Mail, as long as the Waiver of Signature block on the USPS Express Mail label will not be completed; or

(c) Cleared commercial carriers or cleared commercial messenger services.

(3) Confidential. Confidential information will be transported by:

(a) Methods established for Secret information or USPS Certified Mail; or

(b) U.S. First Class Mail when the recipient is a U.S. Government (USG) facility. When First Class mail is used, the envelope or outer wrapper will be marked to indicate that the information is not to be forwarded, but is to be returned to sender.

(c) Confidential information will not be transported to government contractor facilities via first class mail.

h. Transportation Methods to a USG Facility Located Outside the U.S.

(1) The transportation of CNSI to a USG facility located outside the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, will be by methods specified above for TS information or by the Department of State Courier Service.

(2) U.S. Registered Mail through Military Postal Service facilities may be used to transport Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

i. Transportation of U.S. CNSI to Foreign Governments.

(1) Such transportation will take place between designated government representatives using the government-to-government transmission methods described above or through channels agreed to by the National Security Authorities of the two governments.

(2) When CNSI is transferred to a foreign government or its representative a signed receipt is required.

j. Receipt of CNSI. All personnel will follow procedures which ensure that CNSI is received in a manner which precludes unauthorized access, provides for inspection of all CNSI received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of TS and Secret CNSI by an authorized recipient.

k. Hand-carrying CNSI.

(1) Couriers and authorized persons designated and trained to hand-carry CNSI will ensure that the information remains under their constant and continuous protection and that direct point-to-point delivery is made. As an exception, agency heads may approve, as a substitute for a courier on direct flights, the use of specialized shipping containers that are of sufficient construction to provide evidence of forced entry, are secured with a combination padlock meeting Federal Specification FF-P-110, are equipped with an electronic seal that would provide evidence of surreptitious entry and are handled by the carrier in a manner to ensure that the container is protected until its delivery is completed.

(2) An APHIS Courier Card will be issued by the APHIS ISS only to those individuals whose duties require routine hand-carrying of classified material.

(3) Authorized APHIS couriers may hand-carry CNSI up to the TS level within their geographical limits indicated on their courier authorization. To be an authorized courier, the employee must:

(a) Be appointed by his/her supervisor;

(b) Possess a security clearance at or above the level of classified he/she is authorized to transport;

(c) Be trained on courier procedures. As a minimum, the courier briefing will include information on:

1 Proper receipting and control procedures;

2 Physical protection, wrapping, and storage procedures; and

3 Procedures to be taken in an emergency.

(d) Sign a courier agreement; and

(e) Possess a valid courier authorization card. The APHIS courier card authorizes the bearer to transport or hand-carry CNSI on a recurring basis.

1 The card is valid for a period of 1 year; the courier must receive annual refresher courier training to have the card renewed.

2 The card will identify the holder by name, employee ID number (last four of his/her Social Security Number), date and place of birth, issue and expiration date, assigned office code, level of CNSI authorized to be hand carried, the geographical limits authorized to the courier, and the signatures of both the holder and the ISS.

3 The bearer of the courier card must report the loss or damage of the card immediately to the ISS. The bearer may request a replacement card, which will be issued at the ISS's discretion.

4 The courier card can be issued to APHIS employees for 1 year from the date of issue. APHIS contractors, licensees, and consultants may be issued a card not to exceed the expiration of their contract.

5 The bearer must return the courier card to the ISS upon termination, suspension, or revocation of his/her security clearance, when the authorization is no longer needed, when leaving the employment with APHIS or when an occurrence dictates the need to withdraw the courier authorization, as determined by the ISS.

6 The courier card does not authorize the courier to hand-carry CNSI aboard commercial aircraft. Permission to hand-carry classified information aboard commercial aircraft will be granted by the ISS in accordance with the instructions outlined below.

(4) Classified material will not be read, studied, displayed, or used in any manner on public conveyances or in public places.

(5) When CNSI is carried in a private, public, or government conveyance, it will not be stored in any detachable storage compartment, such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks.

(6) When transporting classified materials, the route will be mapped out ahead of time to ensure door-to-door transport.

(7) If door-to-door transport is not possible, prior arrangements for proper storage of the CNSI materials must be made.

(a) Classified material will not be stored overnight in an individual's hotel room or private residence.

(b) Classified materials can be taken to the following facilities for storage:

1 A Federal Bureau of Investigation (FBI) field office. A list of all field offices can be found at: http://www.fbi.gov/contact/fo/fo.htm

2 A Department of Defense (DoD) military installation. Military installations by State can be found at: http://www.military.com/InstallationDirectives/ChooseInstallation/1,11400,,00.html

3 For 24-hour assistance, contact the Emergency Operations Center (EOC) at **1-877-677-2369.**

(8) If stops are necessary, the classified materials must be kept in the courier's possession, or within an authorized area for storing CNSI.

(9) APHIS employees who are infrequently authorized to act as couriers for classified material will be designated by a courier authorization letter issued for each trip.

(10) CNSI may be hand-carried aboard commercial passenger aircraft only when there is neither time nor means available to properly transmit the information by any other authorized methods.

(a) Written authorization from the ISS is required by the courier to carry CNSI aboard commercial aircraft.

(b) The ISS may grant permission to carry classified material to overseas locations on a case-by-case basis.

(11) Procedures for hand-carrying CNSI through borders or airports.

(a) If airline travel is authorized, the material will be subject to routine security screening.

(b) Screening officials may check the sealed package, zippered pouch or closed briefcase by X-ray machine.

(c) Screening officials are not permitted to open the classified material.

1 If airline security requests that the package be opened, the courier will show his/her written authorization letter and inform airline security that the package contains USG CNSI, and state that it cannot be opened.

2 If there are further problems with airport security checkpoints, the courier will contact the Airport Security Manager.

3 If the issues are still not resolved, the courier will contact the ISS or the EOC.

(d) When traveling to a foreign country, the courier must travel aboard a U.S. carrier. Foreign carriers can only be used when no U.S. carrier is available. The courier must ensure that the information remains in his/her custody and control at all times.

(e) When passing through foreign customs areas, there is no assurance of immunity from search by the customs, police, or immigration officials of the U.S. or various countries whose borders the courier may cross. If these officials inquire as to the contents of the classified consignment, the

courier will present his/her orders and ask to speak to the senior customs, police, or immigration official. This action will normally suffice to pass the material through unopened.

1 If the senior official still has questions and concerns, have them contact the ISS at 301-436-3198 or 301-741-1834.

2 If the senior official demands to see the actual contents of the package, precaution will be taken to ensure compromise of the information does not occur.

3 The outer envelope may be opened but will be done in an area out of sight of the general public.

4 Precautions will be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item.

5 The courier will ask the official to repack or assist in the repackaging of the material immediately upon completion of the examination.

6 The senior official will be requested to provide evidence of the opening and inspection of the package by signing it when closed and by confirming on the shipping documents (if any) or courier certificate that the package has been opened.

7 The addressee and the ISS will be informed, in writing, of the incident with the following information:

a Date and time of the incident;

b Name of the senior official requiring the package to be opened;

c The official's organization;

d His/her supervisor’s name and telephone number; and

e The location where the incident took place.

CHAPTER 6

TRANSMISSION METHODS

1. General. All personnel authorized access to Classified National Security Information (CNSI) will ensure that it is electronically accessed, processed, stored, transmitted and protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation.

2. Requirements. Based upon the risk management factors referenced in 32 Code of Federal Register (CFR) the Personnel and Document Security Division (PDSD) will determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures and TEMPEST necessary to detect or deter exploitation of classified CNSI through technical collection methods and may apply countermeasures in accordance with National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, TEMPEST Countermeasures for Facilities, and SPB Issuance 6–97, National Policy on Technical Surveillance Countermeasures.

   a. Classified Discussions, Meetings, and Conferences.

      (1) Once an APHIS component accepts sponsorship of a meeting, the sponsor assumes overall security responsibility, ensuring:

         (a) That the invitations are unclassified;

         (b) That all attendees have the appropriate level of clearances and the valid need-to-know has been certified;

         (c) That access rosters are prepared, checked, and coordinated with the local Information Security Controller (ISC); and

         (d) That the subject matter, location, and other aspects of the meeting are coordinated with the local ISC or APHIS Information Security Specialist (ISS).

      (2) The ISS must be notified if loss or compromise occurs before, during, or after the meeting.

      (3) The sponsor ensures that:

         (a) All participants are advised of their security responsibilities; and

(b) That classified presentations are appropriately marked and safeguarded for later compilation and distribution through secure channels if required.

(4) CNSI to be presented must be authorized for disclosure in advance by the department or agency having jurisdiction over the information involved.

(5) Before presenting or distributing CNSI, the presenter will announce the overall classification level of the information being presented/distributed.

(6) If foreign nationals are invited, submit a list containing their names, and the dates and locations of the sessions they will attend to the PDSD for vetting.

b. CNSI will not be transmitted over any non-secure telephone, facsimile machine, or electronic mail system. Approved facsimile machines can be connected to a Secure Telephone Equipment (STE) terminal for the transmission of classified faxes. The following controls are established for use of secure fax machines to transmit CNSI.

(1) The machine must be located in an accredited Secure Area.

(2) The sender of a classified fax is responsible for verifying that the intended recipient has the appropriate security clearance and valid need-to-know.

(3) Transmission details will be worked out before the actual transmission, by the sender, to ensure the fax is received by the intended recipient.

(a) The fax number will be verified.

(b) Effort will be taken to verify the identification of the recipient.

(4) All TS faxes received will be taken to the Top Secret Control Officer (TSCO) for accountability.

(5) Form AD 471, Classified Document Accountability Record, will be completed for all classified fax transmissions and will be prepared by the sender and included with the fax. The Form AD 471 also serves as the receipt for the CNSI, and will be completed

by the recipient and faxed back to the sender at the completion of the transmission.

(6) Cover sheets affixed to classified documents will not be obscured by transmittal notes, routing sheets, etc.

(a) Cover sheets will not be removed from the document when the document is returned to the security container.

(b) A transmitted document will indicate on the cover sheet the highest classification level of any CNSI attached or enclosed.

(c) If the transmittal contains no CNSI in the body of the cover or transmittal letter, the following statement will be centered at the bottom of the page:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED

(d) If CNSI is contained in the body of the letter, the following statement will be centered at the bottom of the page:

UPON REMOVAL OF ATTACHMENTS,
THIS DOCUMENT IS (*CLASSIFICATION*)

(7) All pages of a secure fax must be accounted for by the recipient.

(8) The user of the secure fax must ensure all classified material is cleared from the fax prior to exiting the Secure Area.

(a) The KSV 21 will be removed from the STE upon termination of the transmission.

(b) When transmission is completed, the recipient will be contacted to confirm receipt.

(c) Return the KSV 21 to secure storage upon completion of the transmission.

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 7
SPECIAL ACCESS PROGRAMS

1. General. Special Access Programs (SAP) have been established to impose access, storage, and handling controls beyond those normally required for access to information classified as Confidential, Secret, or Top Secret. Such programs require special access authorizations, special investigative requirements, special briefings, and/or lists of persons who require access to SAPs due to job or organizational requirements.

2. Requirement. Unless otherwise authorized by the President, only the Secretaries of State, defense, and Energy, and the Director, Central Intelligence Agency may create a SAP.

3. Oversight. To appropriately and fully address support requirements and supporting Agency oversight responsibilities, a memorandum of agreement/understanding (MOA/MOU) will be established for each SAP that has significant interagency support requirements.

4. Access. The granting of access to SAPs will be controlled under the strictest application of the need-to-know principle in accordance with the personnel security standards and procedures set forth by the programs. APHIS employees who require information on obtaining authorization for access to a SAP will contact the APHIS Information Security Specialist.

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 8

SENSITIVE COMPARTMENTED INFORMATION

1. General. The Sensitive Compartmented Information (SCI) program at APHIS is sponsored by the Central Intelligence Agency (CIA). Through their sponsorship, they provide SCI program oversight, adjudications, access approvals, and accreditations of SCI Facilities (SCIFs).

2. Administration. The Personnel and Document Security Division (PDSD) provides security administration support for APHIS SCI cleared employees, maintains a copy of the SCI Nondisclosure Agreements, forwards SCI clearance requests for visits, administers continuing SCI education and training program, conducts SCI security debriefings, and executes the debriefing acknowledgement portion of the SCI Nondisclosure Agreement.

3. Access. APHIS employees granted access to SCI will comply with the directives, regulations, and manuals that govern the SCI program. Security policies for SCI are documented in applicable Intelligence Community Directives (ICDs).

   a. Request for Access to SCI.

      (1) Requests for access to SCI will be submitted to the APHIS Information Security Specialist (ISS) on an AD Form 1188. The request must include a specific, unclassified valid need-to-know justification for the special access clearance and be signed by the individual's supervisor.

      (2) The ISS will verify that employees requiring access to SCI have been afforded appropriate investigations and granted the appropriate security clearance. The requirements for access to SCI include a Top Secret (TS) clearance, a favorable Single Scope Background Investigation (SSBI) or Periodic Review (PR) completed within the last 5 years.

         (a) If eligibility clearance requirements are not met, the ISS will notify the requestor to initiate a clearance upgrade or periodic review of their current clearance. When the employee is granted the proper Clearance to meet eligibility requirements, he/she will submit another request for access to SCI through the PDSD.

         (b) If the eligibility requirements are met, the SCI access request will be forwarded to the CIA for adjudication. The CIA will notify PDSD when access has been approved. The ISS will notify the requestor and provide him/her with

instructions to obtain initial SCI training, program indoctrination briefs, and execution of the SF- 4414, SCI Nondisclosure Agreement. The SF-4414 must be executed prior to an employee being granted access to SCI information.

b. When access is no longer required,

(1) The PDSD will administer an employee a SCI security debriefing to the individual;

(2) The individual will be asked to sign the debriefing acknowledgment on the SF-4414. The security debriefing is also required for separation, transfer, change in duties, suspension, or revocation of access. A copy will be Retained in the employee's personnel security file; and

(3) The CIA will update the SCI database to reflect withdrawal of access.

4. Accreditation of SCIFs.

a. SCI material will be maintained only in APHIS Secure Areas accredited as SCIFs by the CIA. To request establishment and accreditation of a SCIF, forward a request through the ISS to PDSD. The request must include:

(1) The complete address;

(2) Point of contact;

(3) Justification;

(4) Description of any automated equipment that will be housed in the SCIF; and

(5) Whether open or closed storage is desired.

b. Upon approval, the PDSD will arrange a physical security survey by the CIA accrediting official.

(1) Recommendations for any security upgrades will be provided upon completion of the survey.

(2) After implementing the recommendations, a follow-up inspection will be conducted by the CIA accrediting official.

(3) A final accreditation letter will be provided in writing to the PDSD.

(4) The file copy will be maintained by the PDSD and a copy provided to the requesting office and the APHIS ISS.

5. SCI Security Education.

a. The PDSD will administer a continuing security education program for all APHIS Employees authorized access to SCI.

b. Under the program, employees with SCI access will be reminded of their obligation to properly handle and safeguard SCI materials and of the potential consequences to the U.S. Government of any compromise or unauthorized use of such information. This reminder will be given to the employee at least annually through an SCI refresher briefing.

6. Reporting Requirements.

a. Individuals authorized SCI access have special responsibilities and obligations to report to the ISS, in writing and when feasible in advance, activities, conduct, or employment that could conflict with their ability to protect CNSI from unauthorized disclosure or counterintelligence threats.

b. A detailed listing of an individual's reporting responsibilities are documented in the ICDs.

7. Travel of Employees with SCI Access.

a. APHIS SCI-cleared employees who require official or unofficial foreign travel to any country must contact the PDSD to arrange for a defensive security briefing prior to such travel.

b. The PDSD will determine the briefing requirement for each specific country visited.

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 9

SECURITY EDUCATION AND TRAINING

1. General. All APHIS employees who create, process, or handle Classified National Security Information (CNSI) must have a satisfactory knowledge and understanding of classification, safeguarding, and declassification policies and procedures to reduce instances of over-classification or improper classification, improper safeguarding, and inappropriate or inadequate declassification practices.

2. Policy. All APHIS programs will ensure that employees who possess a security clearance will fulfill the security education requirements as indicated in this chapter.

3. Requirements. The APHIS Information Security Specialist (ISS) will maintain records of employee participation in meeting training requirements.

   a. Initial Security Briefing. An initial briefing will be provided to every person who has met the standards for access to CNSI in accordance with section 4.1 of Executive Order (E.O.) 13526.

      (1) All cleared personnel will receive initial training on basic security policies, principles, practices, and criminal, civil, and administrative penalties.

      (2) Initial training will be provided in conjunction with the granting of a security clearance, and prior to accessing CNSI.

   b. Original Classification Authorities (OCAs). Pursuant to E.O. 13526, OCAs will receive training on proper classification and declassification prior to originally classifying information and at least once each calendar year thereafter. This training is conducted by the USDA Personnel and Document Security Division (PDSD)

      (1) OCAs will receive detailed training on proper classification and declassification, with an emphasis on the avoidance of over-classification.

      (2) At a minimum, the training will outline classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, Security Classification Guides (SCGs), and information sharing.

(3) OCAs who do not receive such mandatory training at least once within a calendar year will have their classification authority suspended until such training has taken place.

c. Derivative Classifiers. Persons who derivatively classify documents, to include those with access to classified computer networks, will receive training in the proper application of the derivative classification principles of E.O. 13526 and 32 Code of Federal Register (CFR), emphasizing the avoidance of over-classification of information.

(1) At a minimum, the training will cover the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing.

(2) Personnel will receive this training prior to derivatively classifying information to include being afforded access to classified computer networks.

(3) In addition to this initial training, derivative classifiers will receive refresher derivative classification training at least once every 2 years.

(4) Derivative classifiers who do not receive derivative classification training at least once every 2 years will have their authority to apply derivative classification markings suspended until they have received such training.

(a) The Secretary or designee may grant a waiver of this requirement if an individual is unable to receive this training due to unavoidable circumstances. All such waivers will be documented.

(b) Whenever such a waiver is granted, the individual will receive the required training as soon as practicable.

d. All APHIS security clearance holders will complete security refresher training annually. The annual training will:

(1) Reinforce the policies, principles, and procedures covered in initial and specialized training (courier, derivative classification, etc.);

(2) Address identification and handling of other agency-originated information and Foreign Government Information (FGI), as well as the threat and the techniques employed by foreign intelligence

activities attempting to obtain CNSI, and advise personnel of penalties for engaging in espionage activities; and

(3) Address issues or concerns identified during agency self-inspections.

e. Classification management officers, security managers, security specialists, declassification authorities, and all other personnel whose duties significantly involve the creation or handling of CNSI will receive more detailed or additional training no later than 6 months after assumption of duties that require other specialized training.

f. Termination Briefings.

(1) Except in extraordinary circumstances, all APHIS programs will ensure that each employee who is granted access to CNSI and leaves the Agency receives a termination briefing and signs the Standard Form
(SF) 312.

(2) Additionally, any APHIS employee whose clearance is withdrawn, suspended, or revoked must receive such a briefing.

(3) At a minimum, termination briefings will impress upon each employee the continuing responsibility not to disclose any CNSI to which the employee had access and the potential penalties for non-compliance, as well as the obligation to return to APHIS all classified documents and materials in the employee's possession.

g. Other Security Education and Training. The ISS has developed additional security education and training and can tailor a briefing or training to meet program and policy needs.

THIS PAGE INTENTIONALLY
LEFT BLANK

CHAPTER 10

INDUSTRIAL SECURITY

1. General. The principles and concepts for APHIS participation in the National Industrial Security Program (NISP) are outlined in the NISP Operating Manual (NISPOM).

   a. Established by Executive Order (E.O.) 12829, the NISP provides for the protection of Classified National Security Information (CNSI).

   b. The NISP was created to develop a uniform program of baseline security requirements and standards that all agencies, departments, and contractors will adhere to and for which they will be measured.

   c. Through the NISP, the Department of Defense (DoD) as the Executive Agent, extends access to CNSI to contractors who have appropriate security clearances.

   d. The provisions of the NISPOM apply to all APHIS regions, laboratories, offices, contractors, licensees, certificate holders, or grantees that access CNSI through contractual obligations.

2. Requirements. The Federal Acquisition Regulation (FAR) requires a DD Form 254, Contract Security Classification Specification, be incorporated in each classified contract.

   a. The DD Form 254 provides to the contractor the security requirements and the classification guidance necessary to perform a classified contract.

   b. A classified contract is any contract, subcontract, purchase order, lease agreement, service agreement, etc. that requires or will require access to CNSI by a contractor or their employees in the performance of the contract (a contract may be classified even though the contract document is not classified). This term is used throughout the NISPOM because it is the most typical occurrence for a contractor to have access to or possession of CNSI.

   c. The requirements prescribed for a classified contract are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other government agency program or project that requires access to CNSI by the contractor.

3. USDA Senior Agency Official (SAO). The Personnel and Document Security Division (PDSD) serves as the SAO and will:

a. Furnish assistance and guidance to contracting and program personnel relating to the security requirements of any procurement action involving classified or sensitive information;

b. Receive and process requests for verification of Facility Clearances (FCL) for prospective contractors;

c. Assist the contractor, Contracting Officer (CO), and Contracting Officer Representative (COR) in the development of the DD-254; and

d. Represent APHIS in all NISP matters with other Federal departments, boards, or committees.

4. The CO, will:

a. Coordinate with the COR and the PDSD to ensure protection of CNSI in the possession of contractors and pertaining to contracts;

b. Approve DD-254, to include the following actions:

(1) Submit all DD-254s to the PDSD for certification;

(2) Issue a DD-254 (revised) whenever a modification or additional classification guidance is found necessary;

(3) Review the existing classification specification during the term of the contract and at least once every 2 years;

(4) Issue a final DD-254 upon completion of the contract. The final DD Form 254 will provide disposition instructions for any CNSI the contractor may possess pertaining to the contract; and

(5) Authorize release of CNSI by contractors at seminars, meetings, and symposiums when such authorization is required in the performance of the contract. Prior to authorizing release, coordinate with PDSD.

5. The COR will:

a. Verify the FCL.

(1) Prior to the disclosure of any CNSI to a contractor, the responsible COR must obtain verification that the contractor's facility is in possession of a valid FCL equal to or higher than the level of

classified information to be disclosed in the performance of the contract.

(2) Requests for certification will be submitted in writing to the PDSD and will contain the following information:

(a) Name and location of the contractor facility;

(b) Brief description of the work to be performed;

(c) Level of access to CNSI required;

(d) A statement whether the facility is to receive, generate, use, and/or store CNSI in the performance of the contract;

(e) The estimated volume of CNSI segregated by classification level, to be provided to, and/or generated by, the contractor; and

(f) The name and telephone number of the point of contact at the contractor facility who is knowledgeable and responsible for the contract.

b. Verify personnel security clearance. He/she will identify and certify contractors' security clearances and valid need-to-know prior to granting access to APHIS facilities where CNSI will be disclosed.

(a) A contractor with an active security clearance and a valid need-to-know may obtain access to CNSI at APHIS in the performance of their official duties.

(b) The contractor must provide visit certification, including the reason for the visit and verification of employee clearances.

(c) The COR will verify the clearance and valid need-to-know before granting the contractor access to any CNSI.

(d) The contractor is responsible for passing security clearances of its employees for visits to other classified facilities.

c. Process Requirements.

(1) For each classified contract, the COR must include a justification statement that the contractor will require access to CNSI and/or will generate CNSI in the performance of the contract.

(2) All classified contracts require positive verification of the FCL prior to release.

(3) The COR responsible for initiating the procurement request will prepare the DD Form 254 and forward it to the CO for review and approval.

(4) Supplemental instructions for preparation of the DD Form 254 are available from PDSD.

(5) This action will be taken sufficiently in advance to permit forwarding a copy of DD Form 254 with each Invitation For Bid (IFB), Request For Proposal (RFP), or Request For Quotation (RFQ).

6. PDSD will:

a. Maintain records of contractor/consultant personnel in his/her units subject to the NISP;

b. Provide assistance and guidance to the CO and the COR with respect to industrial security matters in APHIS;

c. Ensure that all contractor and consultant personnel who physically work within APHIS have been briefed on the procedures for handling and safeguarding CNSI. APHIS maintains the right to conduct an assessment of the contractors' ability to comply with the Federal requirements.

CHAPTER 11

LOSS, POSSIBLE COMPROMISE, OR UNAUTHORIZED DISCLOSURE OF CNSI

1. General Requirements.

   a. Any person who discovers Classified National Security Information (CNSI) improperly secured or unprotected will take custody of the information, safeguard it in an appropriate manner, and immediately report the incident to the APHIS Information Security Specialist (ISS).

   b. If CNSI appears in the public media, APHIS employees are cautioned not to make any statement or comment that would confirm the accuracy or verify the classified status of the information.

   c. If approached by a representative of the media who wishes to discuss information believed to be classified, individuals will neither confirm nor deny the accuracy of the information and will report the situation immediately to the ISS and a public affairs specialist in Legislative and Public Affairs.

   d. Any person who has knowledge that CNSI has been or may have been lost, possibly compromised, or disclosed to an unauthorized person(s) will immediately report the circumstances to their Information Security Controller (ISC) and/or the APHIS ISS.

2. Cases Involving Information Originated by a Foreign Government or Another U.S. Government (USG) Agency.

   a. Whenever a loss or possible unauthorized disclosure involves the CNSI or interests of a foreign government agency, or another USG agency, the activity in which the compromise occurred will advise their ISC or the ISS and/or who will, in turn, notify the other government agency or foreign government of the circumstances and findings that affect their information or interests.

   b. Foreign governments will not be advised of any security system vulnerabilities that may have contributed to the compromise.

3. The ISS will establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of CNSI, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

4. Reports to the Information Security Oversight Office (ISOO). In accordance with section 5.5(e)(2) of Execute order (E.O.) 13526, the APHIS ISS will notify the Personnel and Document Security Division (PDSD) who will, in turn, notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of E.O. 13526 that:

    a. Is reported to oversight committees in the legislative branch;

    b. May attract significant public attention;

    c. Involves large amounts of CNSI; or

    d. Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

5. Department of Justice (DOJ) and Legal Counsel Coordination.

    a. The APHIS ISS will establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of CNSI.

    b. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, the ISS will use established procedures to ensure coordination with the DOJ and the legal counsel of the agency where the individual responsible is assigned or employed.

6. To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, possible loss of CNSI, or an infraction of the safeguarding controls as established by this Directive.

    a. A formal investigation will be conducted into complex incidents or those of serious consequence. Initially these incidents are referred to as information security incidents. In the course of the inquiry or investigation, the incident will be categorized as a "Compromise," "Possible Compromise," "Inadvertent Access," or "Security Deviation."

    b. The purpose of an inquiry or investigation is to determine:

        (1) Whether or not a security incident has occurred;

        (2) The source and reason for the security incident;

        (3) Appropriate measures or actions to minimize or negate the adverse effect of the security incident;

(5) The seriousness of damage to U.S. interests; or

(5) The vulnerabilities in the security program that could result in similar incidents in the future.

7. Debriefings in Cases of Unauthorized Access. In cases where a person has had unauthorized access to CNSI, it may be advisable to discuss the situation with the individual to enhance the probability that he or she will properly protect it. Whether such a discussion ("debriefing") is held will be decided by the ISS. This decision must be based on the circumstances of the incident, what is known about the person or people involved, and the nature of the CNSI. The following apply:

a. If the unauthorized access was by a person with the appropriate security clearance but without a valid need-to-know, a debriefing is usually unnecessary. A debriefing may be required if the individual is not aware that the information is classified and needs protection.

b. If the unauthorized access was by a government employee or military member without the appropriate security clearance, a debriefing is appropriate.

(1) The person will be advised of his/her responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if he/she fails to do so.

(2) The debriefing official will make sure the individual understands what CNSI is and why its protection is important, and what to do if someone tries to obtain the information.

(3) If the person who had unauthorized access is an employee of a contractor participating in the National Industrial Security Program (NISP), the same Directives apply as for Government employees.

8. Appointment of a Preliminary Inquiry Officer (PIO).

a. Upon notification of a security incident or violation, the ISS will notify PDSD of the security incident or violation.

(1) The PDSD will request in memorandum format the details of the incident.

(2) The ISS will appoint a PIO in writing.

(3) The ISS will be provided the name, office identification code, and telephone number of the PIO within 5 working days from the date of the requesting memorandum.

b. The ISS will take the following actions after a security incident is reported:

(1) Appoint a PIO to conduct an expeditious, thorough inquiry or investigation whenever a security incident occurs. The person appointed to conduct the inquiry must:

(a) Have an appropriate security clearance and the ability and available resources to conduct an effective inquiry; and

(b) Must not have been involved, directly or indirectly, in the incident.

NOTE: Except in unusual circumstances, the activity security officer will not be appointed to conduct the inquiry.

(2) Approve, in writing, any extensions for completing the inquiry if the PIO cannot meet the established due date. A courtesy copy of the extension approval will be maintained by the ISS.

(3) Contact PDSD to determine whether the individual involved in the incident has any record of previous security violations. Any disciplinary action proposed against an employee is referred to Marketing and Regulatory Programs-Business Services, Human Resources Division, Employee Relations Branch.

c. The PIO will:

(1) Obtain a briefing from the ISS to receive initial facts and evidence surrounding the incident;

(2) Consult with PDSD for technical guidance in conducting the inquiry; and

(3) Prepare and forward, within 15 working days, a report that will include, as a minimum the following:

(a) When, where, and by whom the inquiry was conducted or requested;

(b) What specific CNSI or material was involved;

(c) A list of employees who were interviewed, including their grade, full name, title, home and work addresses, and security clearance level;

(d) A report of the facts including who, what, when, why, and how the incident occurred, describing exactly what happened in chronological order; and

(e) A brief summary of conclusions reached after a review of all pertinent information, facts, and evidence.

d. If the compromise of CNSI occurred and, if so, the damage to national security. Every inquiry into compromise or possible compromise of classified information must include a judgment about whether compromise occurred and about the potential damage to national security. One of the following alternatives must be chosen:

(1) Compromise of CNSI did not occur;

(2) Compromise of CNSI may have occurred;

(3) Compromise of CNSI did occur, but there is no reasonable possibility of damage to national security; or

(4) Compromise of CNSI did occur, and damage to national security may result.

9. Corrective Actions. Investigations often reveal gaps in security procedures, processes, or facilities. When corrective actions are required by an activity, they must report actions taken to date, and a timeline for further actions, within 30 days of the completion of a preliminary inquiry or security violation investigation.

10. Sanctions.

a. Employees will be subject to sanctions if they knowingly, willfully, or negligently:

(1) Disclose to unauthorized persons properly CNSI;

(2) Classify or continue the classification of information in violation of Federal regulations;

(3) Create or continue a Special Access Program (SAP) contrary to the requirements of a regulation; or

(4) Violate any other provisions of Federal regulations pertaining to CNSI.

b. Sanctions include, but are not limited to: warning, reprimand, suspension without pay, forfeiture of pay, removal, loss or denial of access to CNSI, and removal of classification authority. Action also may be taken under the applicable criminal law.

CHAPTER 12

PROGRAM MANAGEMENT

1. General. The Animal and Plant Health Inspection Service (APHIS) Information Security Program (ISP) requires that all APHIS locations where classified National Security Information (CNSI) is handled, processed or stored will be inspected and monitored to ensure that appropriate security measures, policies, and procedures are in place to ensure the highest degree of security for the protection of the information.

   a. Written documentation of inspections will be maintained and made available for a minimum of 2 years.

   b. Counterintelligence technical inspections will be conducted or scheduled on an "as needed" or recurring basis.

2. Requirements. Programs will appoint, in writing, an official to serve as the Information Security Coordinator (ISC) for the Program activities.

   a. ISCs are responsible for the administration of an effective ISP in their area of responsibility, emphasizing security education and training.

   b. The ISCs will serve as a focal point for their Program to provide advice and assistance regarding APHIS policy on classification, declassification, downgrading, marking, handling, and protection of national security and sensitive information.

   c. The ISCs will help coordinate the following actions with the ISS:

      (1) Ensure that indoctrination, refresher, threat, courier, foreign travel, and termination briefings are conducted as required, necessary, or requested.

      (2) Ensure an annual document review program is conducted in each program activity to reduce unnecessary classified holdings. The program will include downgrading, declassifying, destroying, or returning the documents to the originator.

      (3) Report all security incidents or violations to the ISS and serve as the point of contact on the status of ongoing preliminary inquiries or formal investigations.

      (4) Prepare or coordinate requests for designation letters.

(5) Maintain and report on all CNSI stored, handled, and processed in their program.

3. Policy. Entry and exit inspections will be conducted randomly on all persons and their property at the entry or exit points of Sensitive Compartmented Information Facilities, Secure Areas, or at other designated points of entry to the building, facility, or compound. The purpose of the inspection is to deter the unauthorized removal of sensitive or classified material. Failure to comply with inspections may result in loss of access or security clearance, and/or other administrative actions.

CHAPTER 13

SELF INSPECTIONS

1. General. The APHIS Information Security Specialist (ISS) is responsible for directing and administering APHIS' self- inspection program. The program will be structured to provide the ISS with information necessary to assess the effectiveness of the classified National Security Information (CNSI) program within activities and APHIS as a whole in order to enable the ISS to fulfill his/her responsibility to oversee APHIS' program.

   a. The ISS will determine the means and methods for the conduct of self-inspections.

   b. Self-inspections will evaluate the adherence to the principles and requirements of Executive order (E.O.) 13526 and 32 Code of Federal Register (CFR) and the effectiveness of APHIS' programs regarding original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight.

   c. Regular reviews of representative samples of APHIS' original and derivative classification actions will encompass all APHIS activities that generate CNSI.

      (1) They will include a sample of varying types of classified information (in document and electronic format such as e-mail) to provide a representative sample of APHIS' classification actions. The sample will be proportionally sufficient to enable a credible assessment of APHIS' classified product.

      (2) APHIS personnel who are assigned to conduct reviews of their original and Derivative classification actions will be knowledgeable of the classification and marking requirements of E.O. 13526 and 32 CFR, and have access to pertinent Security Classification Guide (SCG).

      (3) In accordance with section 5.4(d)(4) of E.O. 13526, the ISS will authorize appropriate agency officials to correct misclassification actions.

   d. Self-inspections will include a review of relevant security directives and instructions, as well as interviews with producers and users of CNSI.

2. Requirements. Self-inspections will be regular, ongoing, and conducted at least annually with the ISS setting the frequency on the basis of program needs and the

degree of classification activity. Programs that generate significant amounts of CNSI will include a representative sample of their original and derivative classification actions.

a. The ISS will establish self-inspection coverage requirements based on program and policy needs. Programs with special access programs will evaluate those programs in accordance with sections 4.3(b)(2) and (4) of E.O 13526, at least annually.

b. Programs will document the findings of self-inspections internally and provide copies to the ISS.

c. The ISS will provide the format for documenting self-inspection findings. As part of corrective action for findings and other concerns of a systemic nature, refresher security education and training will address the underlying cause(s) of the issue.

d. The ISS will provide a report annually to the PDSD on the agency's self-inspection program. This report will include:

(1) A description of APHIS self-inspection program to include activities assessed, Program areas covered, and methodology utilized;

(2) The assessment and a summary of the findings of the self-inspections in the following program areas: original classification, derivative classification, declassification, safeguarding, security violations, security education and training, and management and oversight;

(3) Specific information with regard to the findings of the annual review of APHIS' original and derivative classification actions to include the volume of classified materials reviewed and the number and type of discrepancies that were identified;

(4) Actions that have been taken or are planned to correct identified deficiencies or misclassification actions, and to deter their reoccurrence; and

(5) Best practices that were identified during self-inspections.

CHAPTER 14

AGENCY ANNUAL REPORTING REQUIREMENTS

1. Statistical Reporting. Each Animal and Plant Health Inspection Service (APHIS) Activity that creates or safeguards classified National Security Information will report annually to the ISS statistics related to its security classification program. The Director of the Information Security Oversight Office (ISOO) will instruct APHIS what data elements are required, and how and when they are to be reported.

2. Accounting for Costs.

   a. Information on the costs associated with the implementation of Executive order 13526 will be collected from the Activities. The Activities will provide data on the cost estimates for classification related activities. The APHIS Information Security Specialist will report these cost estimates to the Personnel and Document Security Division to compile a report for ISOO.

   b. Cost estimates will include classification-related activities of contractors, licensees, certificate holders, and grantees.