United States Department of Agriculture
Marketing and Regulatory Programs
Animal and Plant Health Inspection Service

Handbook **APHIS 3440** **5-2-06**

APHIS INFORMATION SECURITY HANDBOOK

This is the Animal and Plant Health Inspection Service (APHIS) Information Security Handbook. It is intended for all APHIS employees who have any duties and/or responsibility for safeguarding and using classified information (users, supervisors, contractors, management, and security).

The APHIS Information Security Handbook combines appropriate Federal regulations, Executive Orders, and Department Manual into one reference tool. The Handbook applies to all organizational levels and, ultimately, to all APHIS employees working in the United States and foreign locations. This Handbook contains specific procedures and instructions relating to information security issues.

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

Office of Emergency Management
and Homeland Security
4700 River Road, Unit 72
Riverdale, MD 20737

/s/
W. Ron DeHaven
Administrator

INFORMATION SECURITY PROGRAM
TABLE OF CONTENTS

CHAPTER 1 GENERAL

1.1 PURPOSE

This Handbook establishes the Animal Plant Health Inspection Service's (APHIS) Information Security Program (ISP), states APHIS policy and assigns responsibility in the classification, declassification, and safeguarding of national security information. The policy and procedures described within apply to all classified information in APHIS' custody, regardless of whether the material originated within APHIS or was released to the Agency by another Agency.

1.2 SCOPE

This Handbook applies to all APHIS employees and contractors utilizing, handling, and safeguarding classified information.

1.3 AVAILABILITY

Copies of this Handbook should be maintained in each office handling or storing classified information.

1.4 AUTHORITIES/REFERENCES

The authorities/references for this Handbook are published in accordance with the requirements of:

1. Executive Order (E.O.) 12958 as amended, Classified National Security Information, dated March 25, 2003.

2. Information Security Oversight Office (ISOO) Directive 1, Classified National Security Information, dated September 22, 2003.

3. Executive Order 12958, Title 3, Secretary of Agriculture Designation Authority, dated 26 September 2002.

4. Department of Defense (DoD) 5200.1-R, Information Security Program, dated 17 Jan 97.

5. DoD 5220.22.M, National Industrial Security Program Operating Manual (NISPOM), dated January 1995, and updates.

6. Department Manual (DM) 3440-001, Classification, Declassification, and Safeguarding Classified Information, dated August 10, 1983.

7. Department of Central Intelligence Directive (DCID) 6/9 Manual. Physical security Standards for Sensitive Compartmented Information Facilities, dated 18 November 2002.

These authorities prescribe a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

1.5 DELEGATION OF AUTHORITY

The APHIS Administrator has delegated to the Director of the Office of Emergency Management and Homeland Security (OEMHS) the responsibility for the establishment and administration of the Agency's Information Security Program. OEMHS will keep the Administrator apprised of the status of the information and document security program within APHIS and the status of ongoing investigations into security infractions and violations.

1.6 ACRONYMS

AD	**Agriculture Department (for forms use only)**
AIS	**Automated Information System**
AISSP	**Automated Information System Security Plan**
APHIS	**Animal and Plant Health Inspection Service**
CAGE	**Commercial and Government Entity**
CCI	**Controlled Cryptographic Item**
CNWDI	**Critical Nuclear Weapon Design Information**
CFR	**Code of Federal Regulations**
CIA	**Central Intelligence Agency**
CIPA	**Classified Information Procedures Act**
COMSEC	**Communications Security**
CONOP	**Concept of Operations**
CONUS	**Continental United States**
COOP	**Continuity of Operations Procedure**
CSA	**Cognizant Security Agency**
CSS	**Central Security Service**
CVA	**Central Verification Activity**
DCI	**Director of Central Intelligence**
DCID	**Director of Central Intelligence Directive**

DCS	**Defense Courier Service**
DIS	**Defense Investigative Service**
DISCO	**Defense Industrial Security Clearance Office**
DLSC	**Defense Logistics Services Center**
DoD	**Department of Defense**
E.O.	**Executive Order**
FCL	**Facility (Security) Clearance**
FGI	**Foreign Government Information**
FOCI	**Foreign Ownership, Control or Influence**
FRD	**Formerly Restricted Data**
FSO	**Facility Security Officer**
GCMS	**Government Contractor Monitoring Station**
GSA	**General Services Administration**
ISCAP	**Interagency Security Classification Appeals Panel**
ID	**Identification**
IDS	**Intrusion Detection System**
ISOO	**Information Security Oversight Office**
ISO	**Information Security Officer**
ISP	**Information Security Program**
ISS	**Information System Security**
LOC	**Letter of Notification of Personnel Clearance**
MOA	**Memorandum of Agreement**
NACC	**National Agency Check and Credit Check**
NDP	**National Disclosure Policy**
NISP	**National Industrial Security Program**
NISPOM	**National Industrial Security Program Operating Manual**
NISPOMSUP	**National Industrial Security Program Operating Manual Supplement**
NSA	**National Security Agency**
OADR	**Originating Agency's Determination Required**
OCA	**Original Classification Authority**
OEMHS	**Office of Emergency Management and Homeland Security**

OPM	**Office of Personnel Management**
PCL	**Personnel (Security) Clearance**
PDSD	**Personnel and Document Security Division**
PIN	**Personal Identification Number**
RD	**Restricted Data**
SAP	**Special Access Program**
SCI	**Sensitive Compartmented Information**
SCIF	**Sensitive Compartmented Information Facility**
SF	**Standard Form**
SIGINT	**Signals Intelligence**
SSBI	**Single Scope Background Investigation**
STE	**Secure Telephone Equipment**
TSCO	**Top Secret Control Officer**
UL	**Underwriters' Laboratories**
U.S.C.	**United States Code**
VAL	**Visit Authorization Letter**

1.7 BACKGROUND

E.O. 12958, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, 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, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation’s security remains a priority. Implementing guidance on these provisions is contained in ISOO directives.

1.8 DEFINITIONS

The following definitions are commonly used throughout the intelligence/security community. These definitions are provided for easy reference. The definitions may or may not appear in this Handbook. The definitions are meant to aid the user when such terminology is used in conversation or written correspondence.

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

2. Accredit. To certify as meeting a prescribed standard for the appropriate level of information being stored.

3. Agency. An organization within USDA, such as Foreign Agriculture Service, Food Nutrition Service, etc.

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

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

6. Automatic declassification. The declassification of information based upon: (1) the occurrence of a specific date or event as determined by the original classification authority; or (2) the expiration of a maximum time frame for duration of classification established under E.O. 12958.

7. Briefing. The act or process of giving or receiving concise preparatory instructions, information or advice.

8. Carve-Out. A classified contract for which the Defense Investigative Service has been relieved of inspection responsibility in whole or in part.

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

10. Classification Guidance. Any instruction or source that prescribes the classification of specific information.

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

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

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

14. Collateral Information. Information identified as National Security Information under the provisions of E.O. 12958, but which is not subject to enhanced security protection required for SAP Information for SCI.

15. Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

16. Compromise. An unauthorized disclosure of classified information.

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

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

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

20. Cryptanalysis. The analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the system key employed in the encryption.

21. Cryptography. The branch of cryptology which treats the principles, means, and methods of designing and using cryptosystems.

22. Cryptology. The branch of knowledge which treats the principles of cryptography and cryptanalytic; and the activities involved in producing signals intelligence (SIGINT) and maintaining COMSEC.

23. Custodian. An individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

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

25. Debriefing. To instruct not to reveal classified information after his/her employment has terminated.

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

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

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

29. Derivative Classification. The process of determining whether information has already been originally classified and, if it has, ensuring that it continues to be identified as classified by marking or similar means when included in newly created material.

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

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

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

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

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

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

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

37. Information Security. The system of policies, procedures, and requirements established under the authority of E.O. 12958 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.

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

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

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

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

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

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

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

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

46. Network. A system of two or more computers that can exchange data or information.

47. Nickname. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

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

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

50. Original Classification Authority. An individual authorized, in writing, either by the President, or by agency heads or other officials designated by the President, to originally classify information.

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

52. Re-Classify. The raising or lowering of the classification assigned to an item of information.

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

54. Restricted area. Area where classified information may be discussed but not stored. The location will normally be predetermined and designated in writing by the ISO.

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

56. Sanctions. Penalty for noncompliance. Acts to ensure compliance and uniformity for safeguarding classified information.

57. Secure Area. Area where collateral classified information is authorized to be stored. Required to be accredited for appropriate level of information. Predetermined and designated in writing

58. Security Clearance. A determination that a person is eligible under the standards of E.O. 12968 and Office of Personnel Management guidance for access to classified information.

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

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

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

62. Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence.

63. Special Access Program (SAP). Any Federal program or activity (as authorized in E.O. 12958), employing enhanced security measures (e.g., safeguarding, access requirements, etc.) exceeding those normally required for collateral information at the same level of classification. The Federal program/activity will be established, approved, and managed as an SAP.

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

65. Subject Matter Expert. A person with a high degree of skill in or knowledge of a specific subject.

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

67. Telecommunications. The preparation, transmission, or communication of information by electronic means.

68. Training. Required knowledge or briefing to work with classified information. Training occurs annually.

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

70. Upgrade. The raising of the classification of an item of information from one level to a higher one.

71. Vault. Approved area that is designed and constructed of masonry units or steel-lined construction to provide protection against forced entry. A modular vault approved by GSA may be used in lieu of a vault as prescribed in DCID 69 and/or the NISPOM.

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

1.9 POLICY

It is APHIS policy to:

A. Establish an Information Security Program to ensure a uniformed and coordinated policy at all levels of the organization, and

B. Ensure each individual who possesses or who has knowledge of such information regardless of how it was obtained will protect classified information.

1.10 RESPONSIBILITIES

Chapter 7, Code of Federal Regulations, requires each Department originating or handling classified information to designate a senior official to direct and administer its Information Security Program (ISP). Within USDA, the Deputy Assistant Secretary for Administration has the responsibility for the ISP. The Deputy Assistant Secretary for Administration has designated the Department Security Officer as having primary responsibility for providing guidance and oversight and for developing procedures governing the USDA's ISP. APHIS has designated the Information and Document Security Officer in OEMHS as having primary responsibility for implementing the ISP within APHIS. This position is responsible for actively overseeing the ISP, which includes establishing and monitoring policies and procedures to prevent unauthorized access to national security information and protecting classified information from unauthorized disclosure.

A. The Administrator has the overall responsibility for the establishment and maintenance of an effective ISP within APHIS.

B. Deputy Administrators and Program Directors are responsible for ensuring compliance with, and implementation of, all facets of the APHIS ISP as it relates to national classified information and sensitive security information. They are responsible for the effective application of information security policies and procedures within their organization. They must ensure that individuals who have access to classified information are:

- Appropriately cleared,
- Aware of their security responsibilities, and
- Indoctrinated and proficient in the security policy and procedures that apply to them in the performance of their duties.

C. Regional, Field, and Office Managers are responsible for ensuring that employees within their respective area of responsibility abide by and follow the ISP guidance outlined in this Handbook.

D. The Information and Document Security Officer, OEMHS, is the designated Information Security Officer (ISO) for APHIS and is responsible for coordinating compliance with the regulations for safeguarding national security information. The ISO is responsible for:

1. Monitoring and inspecting locations involved in the handling and storage of classified information to ensure appropriate security measures are being utilized. Written documentation of inspections will be maintained and be available for review for a minimum of 2 years. Counterintelligence technical inspections will be conducted or scheduled by USDA on an "as needed" or recurring basis.

2. Promulgating implementing instructions.

3. Establishing and maintaining security education and training programs.

4. Establishing and maintaining an ongoing self-inspection program, which will include the periodic review and assessment of classified documents and products.

5. Establishing procedures to prevent unnecessary access to classified information, including procedures that:

   (a) Require a need for access to classified information be established.

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

(c) Ensure classified information used in or near hostile or potentially hostile areas is safeguarded.

6. Establishing a method for accounting for the costs associated with securing classified information, which will be reported to the Director, ISOO, for publication.

7. Promptly assigning personnel to respond to any request, appeal, challenge, or complaint regarding classified information which originated in APHIS that no longer exists, and for which there is no clear successor in function.

E. Division Directors are responsible for ensuring that the ISP guidance is carried out within their respective Division, and assigning adequate resources to implement and maintain the program. Directors will appoint, in writing, an official to serve as the security contact for their Division. To ensure compliance with this Handbook, this official will be responsible for the administration of an effective ISP emphasizing security education and training.

F. Managers and Supervisors are responsible for effective program implementation and are accountable for the performance of their subordinates to ensure they handle and secure classified information in accordance with this Handbook. In addition, managers and supervisors must establish procedures for the accountability of Top Secret, Secret, and Confidential information and the control of such information. The procedures must provide for tracing the movement of classified information, the limited dissemination, the prompt retrieval of documents, the detection of the loss of information, and the prevention of excessive production or reproduction of documents.

G. Employees are responsible for the safekeeping, handling, and storing of classified material in approved storage containers, areas, or facilities when it is not in use or under the supervision of an authorized person. Before releasing classified information to another individual, the holder of the information must ensure that the individual has an appropriate clearance and the “need to know.” The holder is defined as a person who has classified material in his/her possession, regardless of whether he/she has signed a receipt for the material. Background checks and security badges do not verify the security clearance level or need-to-know. Verification of clearance will be made with the APHIS ISP.

H. The Top Secret Control Officer (TSCO) receives and maintains an accountability register of all Top Secret materials secured within a Top Secret accredited storage location. TSCOs, and alternates, will be designated within offices with approved areas for storage of Top Secret information. TSCOs will be responsible for receiving, dispatching, and maintaining accountability registers of all Top Secret documents in their possession. TSCOs will be selected on the basis of experience and reliability, and will maintain a Top Secret security clearance.

I. Escort Officials are responsible for escorting uncleared individuals visiting secured areas. The escort will ensure that areas are sanitized prior to entering the secured area. The escort must observe all security rules and regulations, and ensure classified information is safeguarded from unauthorized access. The escort official will maintain visual contact with escorted individuals at all times.

J. Couriers are responsible for requesting a courier authorization letter through the ISO prior to transporting classified information. Couriers will receive an initial and annual briefing on safeguarding classified information in their possession.

K. Guards are responsible for monitoring alarms, responding to annunciated alarms, conducting initial inquiries into the cause of alarms, and completing incident reports on alarms.

1. Guards will conduct checks of the secure areas after normal duty hours, and on weekends and holidays. These checks will be conducted every 4 hours for areas that store “Secret” and “Confidential” information, and every 2 hours for areas that store “Top Secret” information. The checks will be documented on SF-701, Activity Security Checklist. The SF-701 should be posted on the exterior side of the door.

2. Guards will conduct random entry and exit inspections on all persons and their property at the entry or exit points of Sensitive Compartmented Information Facilities, secure and restricted areas, or at other designated entry or exit points to and from the building, facility, or compound.

L. The Information Systems Security Program Manager (ISSPM), Information Technology Division, manages the Information System Security program on behalf of the Administrator. The ISSPM is responsible for ensuring effective ISS measures for general support systems that serve APHISwide missions and functions or application systems that transcend unit boundaries. The ISSPM ensures that implementation of established ISS requirements are in compliance with Federal, Departmental, and Agency policies and procedures.

CHAPTER 2 CLASSIFICATION MANAGEMENT

SECTION 1 CLASSIFICATION GUIDELINES

2.1.1 CLASSIFICATION STANDARDS

Classification standards are established in Executive Order (E.O.) 12958, as amended, which is restated below in part.

A. Information may be originally classified under the terms of E.O. 12958 only if all of the following conditions are met:

1. An original classification authority is classifying the information;

2. The information is owned by, produced by or for, or is under the control of the United States Government;

3. The information falls within one or more of the categories of information listed in Section 2.1.3 below; and

4. The original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

B. Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

C. The unauthorized disclosure of foreign government information is presumed to cause damage to national security.

2.1.2 CLASSIFICATION LEVELS

Information may be classified at one of the following three levels. Except as otherwise provided by statute, no other terms will be used to identify United States classified information. If information is under consideration of classification it will be safeguarded at the appropriate classification level.

A. TOP SECRET — will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **exceptionally grave** damage to the national security that the original classification authority is able to identify or describe.

B. SECRET — will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **serious** damage to the national security that the original classification authority is able to identify or describe.

C. CONFIDENTIAL — will be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **damage** to the national security that the original classification authority is able to identify or describe.

2.1.3 CLASSIFICATION CATEGORIES

To qualify for classification, information must meet one of the following criteria:

A. It must fall under one of the specified classification criteria listed below:

1. Military plans, weapons systems, or operations;

2. Foreign government information;

3. Intelligence activities, (including special activities) intelligence sources, methods, or cryptology;

4. Foreign relations or foreign activities of the United States, including confidential sources;

5. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

6. United States Government programs for safeguarding nuclear material or facilities; or

7. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defense against transnational terrorism; or

8. Weapons of mass destruction.

B. An official with original classification authority must determine whether the unauthorized disclosure of the information, either by itself or in the context of other information, could reasonably be expected to cause damage to national security.

2.1.4 CLASSIFICATION PROHIBITIONS AND LIMITATIONS

A. 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.

B. Basic scientific research information not clearly related to the national security will not be classified.

C. Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

1. The reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of national security;

2. The information may be reasonably recovered; and

3. The reclassification action is reported promptly to the Director of the Information Security Oversight Office (ISOO).

D. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of Section 3.5 of E.O. 12958.

E. Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

1. Meets the standards for classification; and

2. Is not otherwise revealed in the individual items of information.

2.1.5 CLASSIFICATION CHALLENGES

Authorized holders of information who, in good faith, believe that its classification status is improper, are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under E.O. 12958. APHIS will ensure that no retribution or other negative actions are taken against any individual initiating such a challenge. Those authorized holders wishing to challenge the classification status of information should present such challenges to an Original

Classification Authority who has jurisdiction over the information. Such a formal challenge should be made in writing, but does not have to be specific other than to ask why the information is or is not classified, or is classified at a certain level.

2.1.6 CLASSIFICATION CHALLENGE TRACKING SYSTEM

APHIS' Information Security Program (ISP) will maintain a system for processing, racking, and recording formal classification challenges made by authorized holders. The records of challenges will be subject to the attention of the Interagency Security Classification Appeals Panel (ISCAP), which is under the auspices of the ISOO. All classification challenges will be kept separate from Freedom of Information Act and Privacy Act requests with a separate recordkeeping system established to process and record the challenges.

CHAPTER 2

SECTION 2 CLASSIFICATION AUTHORITY

2.2.1 ORIGINAL CLASSIFICATION AUTHORITY (OCA)

The Secretary of Agriculture has been granted the authority to originally classify information as Secret and below. The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security, which includes defense against transnational terrorism, and is able to identify or describe the damage.

2.2.2 DERIVATIVE CLASSIFIER

The derivative classifier will carry forward the overall marking from the source document, or the classification level instruction from the classification guide, and mark the derivative document as described in Chapter 3. When a document is classified derivatively based on more than one source document or classification guide, the overall marking will reflect the highest level of classification of its sources. The derivative classifier will concisely identify the source document or the classification guide, including the agency and office of origin.

CHAPTER 2

SECTION 3 DECLASSIFICATION AND DOWNGRADING

2.3.1 DECLASSIFICATION AND DOWNGRADING

Information will be declassified as soon as it no longer meets the standards for classification under Executive Order (E.O.) 12958. It is presumed that information that continues to meet the classification requirements still requires continued protection.

2.3.2 PROCESSING REQUESTS AND REVIEWS

APHIS may refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or nonexistence is itself classified under E.O. 12958.

CHAPTER 3 CLASSIFICATION MARKINGS

3.1 IDENTIFYING AND MARKING BACKGROUND

A uniform security classification system requires that standard markings be applied to classified information. The marking of classified information created after October 16, 1995, will not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information, the originator will provide holders or recipients of the information with written instructions for protecting the information. 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. The overall marking must be conspicuous enough to alert anyone handling the document that it is classified. Overall, classification markings must be larger and **bolder** than other text on the page.

3.2 IDENTIFICATION AND MARKING

Identification and markings will be on the face of each classified document, or other classified media. Refer to The Information Security Oversight Office Marking National Security Information Marking Booklet, dated May 2005.

3.3 MARKING PROHIBITIONS

Markings other than “Top Secret,” “Secret,” “Confidential,” or “Unclassified” will not be used to identify information as classified national security information. No other term or phrase will be used in conjunction with these markings, such as “Secret Sensitive” or “Agency Confidential.” The terms “Top Secret,” “Secret,” and “Confidential” may not be used to identify unclassified information.

3.4 OVERALL MARKING

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

A. Conspicuously place the overall classification at the top and bottom of the outside of the front cover, on the title page, on the first page, and on the outside of the back cover.

B. For documents comprised of information classified at more than one level, the overall marking will be the highest level. For example, if a document contains some information marked “SECRET” and other information marked “CONFIDENTIAL,” the overall marking will be “SECRET.”

3.5 PAGE MARKINGS

At the time of either original or derivative classification, the document will be marked in capital letters (preferably in red ink) at the top and bottom of the page, and on the back of the last page if there is no outside cover page, with the overall classification of the information on the page. Within a classified document, the top and bottom of each page that contains no classified information will be marked "Unclassified" (preferably in black ink).

3.6 PORTION MARKING

Each portion of a document, usually a paragraph, but including subjects, titles, graphics, etc., will be marked to indicate its classification level by placing a parenthetical symbol immediately proceeding or following the portion to which it applies. Use the symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified.

3.7 ORIGINAL CLASSIFICATION MARKINGS

The following will appear on the face of each classified document, or will be applied to other classified media in an appropriate manner:

A. One of the three classification levels defined in Section 2.2 of this Handbook;

B. The identity, by name or personal identifier and position, of the OCA;

C. The agency and office of origin, if not otherwise evident;

D. Declassification instructions, which will indicate one of the following:

1. The date or event for declassification;

2. The date that is 10 years from the date of original classification; or

3. The date that is up to 25 years from the date of original classification; and

E. A concise reason for classification that, at a minimum, cites the applicable classification categories as defined in Section 2.3 of this Handbook.

3.8 DERIVATIVE CLASSIFICATION MARKINGS

Information classified derivatively based on source documents or classification guides will bear all markings except the classification authority line "Classified By" which will be replaced with "Derived From." Information for these markings will be carried forward from the source document or taken from instructions in the appropriate classification guide.

3.9 MULTIPLE SOURCE DOCUMENT

When a document is classified derivatively based on more than one source document or classification guide, the classification authority line will indicate "Derived From: Multiple Sources."

A. The derivative classifier will maintain the identification of each source with the file or record copy 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 documents on its classification authority line as "Derived From: Multiple Sources."

3.10 FOREIGN GOVERNMENT INFORMATION (FGI)

Documents that contain foreign government information will include the markings "Foreign Government Information," "FGI," or a marking that otherwise indicates that the information is of foreign origin. If the fact that the information is foreign government information must be concealed, the marking will not be used and the document will be marked as if it were wholly of U.S. origin.

3.11 WORKING PAPERS AND MISCELLANEIOUS MATERIAL

A. Working papers containing classified information will be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed

B. Unless immediately destroyed, classified carbons, rejected copy, typewriter ribbons, ribbons from word processors, toner cartridges, printers, and the like will be marked or labeled to indicate the level of classification and stored accordingly.

C. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, computer and typewriter ribbons, transfer medium, and other items containing classified information will be safeguarded according to the level of classified information they contain and will be accordingly destroyed after they have served their purpose. Transfer medium includes: drums, cartridges, belts, sheets, memory, and other materials in copiers, printers, facsimile and other devices or items that receive or come in contact with classified information.

3.12 MARKINGS ON SPECIAL CATEGORIES OF MATERIAL

A. SF-706, Top Secret Label; SF-707, Secret Label; and SF-708, Confidential Label; are color-coded adhesive labels that will be used, whenever possible, to mark special categories of classified material (i.e., non-document material, such as computers, removable hard drives, and CDs).

B. SF-709, Classified Label; SF-710, Unclassified Label; and SF-711, Data Descriptor Label; will be used in conjunction with the above labels to help identify unclassified materials and to record addition markings required.

CHAPTER 4 SAFEGUARDING

SECTION 1 SAFEKEEPING AND STORAGE

4.1.1 GENERAL POLICY

Classified information will be secured under conditions adequate to prevent access by unauthorized persons. These standards are established in Executive Order (E.O.) 12958; ISOO Directive 1; 32 CFR Parts 2001 and 2004; the National Industrial Security Program Operating Manual (NISPOM), dated January 1995 and updates; and the USDA Department Manual 3440-001. Exceptions to these requirements can be approved only by APHIS' Information Security Officers (ISO). Items not related to classified materials or documents will not be stored in the same container used to safeguard classified information. Security requirements for Sensitive Compartmented Information Facilities (SCIFs) are established by the Director of Central Intelligence Directives (DCIDs). Current holdings of classified material will be reduced to the minimum required for mission accomplishment.

4.1.2 PHYSICAL SECURITY

The USDA Personnel and Document Security Division (PDSD) requires all USDA agencies to follow the standards for the physical environment used to secure classified information as outlines in 32 CFR part 2001 for Government-owned facilities; and DoD 5220.22.M (NISPOM) for Government-leased facilities.

Classified information will not be stored or utilized in areas without approval from APHIS' ISP, in conjunction with USDA's PDSD. Additional requirements are imposed for the storage of SCI information and will require involvement and accreditation from the Central Intelligence Agency (CIA).

4.1.3 STANDARDS FOR STORAGE EQUIPMENT

The General Services Administration (GSA) establishes and publishes minimum standards and specifications for safes, containers, vault doors, and associated equipment suitable for the storage and protection of classified information.

4.1.4 PROCUREMENT OF NEW EQUIPMENT FOR SAFEGUARDING CLASSIFIED INFORMATION

New equipment will be procured from those items listed on the GSA Federal Supply Schedule, with approval of the ISO.

4.1.5 NUMBERING AND DESIGNATING STORAGE FACILITIES

No external mark will reveal the level of classified information authorized to be or actually stored in a given container or vault. Priorities for emergency evacuation and destruction of the contents of storage containers, vaults, or safes will not be marked or posted on the exterior of those containers.

4.1.6 CONTAINERS AND SAFES

A. The following two companies manufacture safes and containers which meet GSA-established standards. No other companies will be used to store classified information.

1. Diebold, Inc.

2. Hamilton Products Group, Inc.

B. Open/Closed Containers. Open containers will be identified by a standard issue "OPEN" sign displayed on the front of the container. Locked and checked containers will display the white reverse side of the sign marked "CLOSED." Containers with more than one built-in combination lock will have the "OPEN-CLOSED" sign displayed on each drawer having a combination lock.

C. The tops of security containers will be kept free of all material except for the SF-700, Security Container Information, instructions (see item h below).

D. 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 classified information will be accomplished only by authorized persons who have been the subject of a trustworthiness determination. Contact the APHIS ISO for guidance.

E. Moving or Excessing Safes. Safes being moved to another location will be locked before moving and escorted by appropriately cleared employees. Safes identified for excess will be inspected by the ISO, or designee, to ensure no classified material remains within.

F. Combinations to Containers and Vaults. Combinations to containers and vaults will not be recorded on pieces of paper or other material with the following exception: employees having access to a number of combinations may, with the approval of their staff supervisor, record all combinations on an 8 1/2" x 11" page. This page will be classified and marked with the highest classification of material stored in the security containers and filed in a master security container. The combination to the container in which the page is stored will be memorized.

Combinations to security containers, vaults, and secure rooms will be changed only by individuals having that responsibility and holding an appropriate security clearance. The combination will be recorded on the SF-700 and secured in a safe that is certified as equal to or at a higher classification level than the level of the documents in the safe. Combinations will be changed:

1. When a container is placed in use;

2. Whenever an individual knowing the combination no longer requires access;

3. When the combination has been subject to possible compromise;

4. At least once every year; and

5. When taken out of service. Built-in combination locks will then be reset to the standard combination 50-25-50.

    (a) Selecting Combinations. Combinations for each lock will be unique to that lock and will have no systematic relationship to other combinations used within a specific office. Combination numbers will not be derived from numbers otherwise associated with the specific office or its employees. The numbers within 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.

    (b) Classifying Combinations. The combination of a container, vault, or secure room used for the storage of classified information will be assigned a security classification equal to the highest category of the classified information stored within. Any written record of the combination will be marked with the classification. Declassification of combinations occurs at the time they are changed.

G. End-of-Day Security Checks. Each APHIS component that processes, handles, and stores classified information will establish a system of security checks at the close of each working day to ensure that the area is secured. Containers will be checked at the end of each workday or when a security container is closed. Containers will be checked using the physical locking procedures described in 3.(a) and (b) below.

H. Recording Storage Facility Data.

1. The SF-700 is a record that will be maintained for each vault or secure room door or container used for storage of classified information. The SF-700 will indicate the location of the door or container; and the names, home addresses, and home telephone numbers of the individuals having primary responsibility for the container.

   (a) SF-700, Part 1, will be completed and placed in an interior compartment of security cabinets or affixed on vault or secure room doors. To the extent practical, Part 1 will be on the inside face of the locking drawer of file cabinets, and on the inside surface of map and plan cabinets.

   (b) SF-700, Parts 2 and 2A, will be marked conspicuously on the front of the form with the highest level of classification and any special access notice applicable to the information authorized for storage in the container. Parts 2 and 2a and will be stored in a security container other than the one in which they apply.

2. SF-701, Activity Security Checklist, will be used to record the checks of all vaults, secure rooms, and containers used for the storage of classified material unless an access control system is used. A new SF-701 will be used each month.

3. SF-702, Security Container Check Sheet, is used to record each time a safe if opened, closed, or when an end-of-day check is conducted. The authorized employee will record the date and time and his/her initials when conducting the check. A new SF-702 will be used each month.

   (a) When opening a container, start turning the combination lock dial to the left (counter clockwise) until the (LCD) displays numbers. Continue turning the dial to the left until you reach your first number in the combination. Then turn the combination dial to the right until you reach the second number in the combination. Turn the dial back to the left until you reach the third. Once you have reached the third number, dial back right until the LCD displays (OP), and the dial stops turning.

   (b) When closing a container, the dial of the combination must be rotated at least four complete turns in the same direction and each drawer must be physically checked before the SF-702 is completed.

CHAPTER 4

SECTION 2 SAFEGUARDING AND CUSTODIAL PRECAUTIONS

4.2.1 RESIDENTIAL STORAGE ARRANGEMENTS

Removal of classified material from designated working areas for work at home is **NOT** authorized.

4.2.2 CARE DURING WORKING HOURS

Classified material removed from its storage container will be kept under constant surveillance by persons with authorized access and who are recognized as having a need-to-know. When not in use, the material will be protected from unauthorized view of its classified content until returned to storage. Such protection will be provided by the material's unclassified cover or by an appropriate cover sheet. Cover sheets to be used are Standard Forms 703, 704, and 705 for "Top Secret," "Secret," and "Confidential" documents respectively.

Normal working hours for secure areas are 8 a.m. to 4 p.m. Monday through Friday. Access after these hours will be requested through the Information Security Officer (ISO).

4.2.3 EMPLOYEES WORKING LATE

Working in a secured area beyond normal hours of operation will require approval from the ISO. The ISO will contact the guards and inform them of personnel working past normal hours.

When work is completed for the day, personnel will place classified materials back inside the secure containers and follow closing procedures stated above. They will conduct a check of the area to ensure no classified information is left out, turn off the light, ensure the door is securely closed, and contact the ISO to inform him/her that the room is secured. The ISO will contact the guards and they will conduct an exterior check of the area.

4.2.4 EMERGENCY PLANNING

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 material to ensure that the material does not come into the possession of unauthorized persons. 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 secure containers is the first priority. 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.

4.2.5 REMOVAL OF CLASSIFIED STORAGE AND INFORMATION PROCESSING EQUIPMENT

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 classified information remains within the equipment. Some examples of equipment that will be inspected are:

A. Reproduction or facsimile machines and other office equipment used to process classified information.

B. GSA-approved security containers used for safeguarding classified information.

C. Other items of equipment that may inadvertently contain classified information.

4.2.6 SAFEGUARDING U.S. CLASSIFIED INFORMATION LOCATED IN FOREIGN COUNTRIES

Except for classified information 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. 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.

4.2.7 NON-COMMUNICATION SECURITY (NON-COMSEC) CLASSIFIED INFORMATION PROCESSING EQUIPMENT

APHIS has a variety of non-COMSEC approved equipment to process classified information. This includes copiers, computers, and printers. Because much of this equipment has known security vulnerabilities, its use can cause unauthorized disclosure. Such vulnerabilities will be reported to the ISO.

A. Staffs must identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Security procedures must:

1. Prevent unauthorized access to classified information;

2. Ensure the equipment selected to perform the needed function presents the lowest acceptable risk to the classified information; and

3. Comply with guidance on security vulnerabilities.

B. Problems or vulnerabilities with COMSEC equipment and controlled cryptographic items must be reported to the ISO. The ISO will promptly coordinate these reports and take corrective action with the appropriate program or agency.

CHAPTER 5 ESCORTING

5.1 POLICY

Only authorized personnel with a valid APHIS Identification Card (ID), appropriate clearance, recognized need-to-know, and valid justification for access into secured areas will be authorized access into secure areas storing classified information. All other personnel must sign-in and be escorted.

5.2 BASIC RULES FOR ESCORTING

Only authorized APHIS personnel can be an escort. The escort must accept responsibility for the uncleared individuals visiting APHIS facilities. The escort must be knowledgeable of escorting requirements and guidelines, and assume control over the visitor at all times. The escort must observe all security rules and regulations and will ensure un-cleared individuals comply with APHIS instructions and directions to safeguard classified information from unauthorized access. 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 un-cleared persons. The escort must remain with visitors at all times until they are turned over to another authorized official / escort or leave the secure area.

A. The following are not authorized to conduct escorts: Non-APHIS employees, workers, contractors, maintenance personnel, and delivery personnel.

B. The ratio for escorting groups is one escort per five uncleared persons.

C. Escorts need to ensure the area is sanitized prior to allowing access by un-cleared personnel:

1. Repositories are locked or drawers closed.

2. Classified data is not visible on a computer screen.

3. Classified documents are secured.

4. Persons using classified material are advised to secure or shield classified information.

5. No classified discussions are held in the presence of uncleared employees.

6. Reproduction machines, facsimiles, secured telephones, and printers are free of classified data.

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

E. Visitors who have not yet had their security clearance passed by their security office will be treated as un-cleared.

5.3 CHALLENGES

It is the responsibility of all employees and contractors who observe an un-cleared/unescorted individual within a secure area, to become an escort to that person. The un-cleared person must be detained while the ISO or front lobby guard is called to respond to your location, or the individual must be escorted to the front lobby guard desk.

CHAPTER 6 CLASSIFIED DOCUMENT CONTROL

SECTION 1 ACCESS

6.1.1 GENERAL RESTRICTIONS ON ACCESS

Access is limited to individuals who hold the appropriate clearance and have the need-to-know.

6.1.2 POLICY

A. Classified information will remain under the control of the originating agency or its successor in function. Animal and Plant Health Inspection Service (APHIS) will not disclose information originally classified by another agency without its authorization. The Secretary of Agriculture may waive this requirement for specific information originated within the United States Department of Agriculture (USDA). An official, employee, or contractor leaving APHIS facilities, may not remove classified information from APHIS' control without proper authorization. A person may have access to classified information 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 SF-312, Approved Nondisclosure Agreement.

3. The person has a need-to-know the information.

B. Each staff will maintain control over the distribution of classified information under their control to ensure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information. All recipients will cooperate fully with distributors who are updating distribution lists and will notify distributors whenever a relevant change in document status occurs. When updates occur, outdated documents or information will either be destroyed by approved destruction methods or sent back to the originator. (See Chapter 7, Disposal and Destruction).

CHAPTER 6

SECTION 2 CLASSIFIED DOCUMENT CONTROL AND DISSEMINATION

6.2.1 CLASSIFIED DISCUSSIONS, MEETINGS, AND CONFERENCES

The APHIS Information Security Program is responsible for providing guidance and assistance to sponsoring APHIS organizations in developing and planning security measures for meetings and for monitoring meetings sponsored and conducted by APHIS organizations to ensure compliance with established security measures. The following procedures apply to hosting meetings or training sessions during which classified information is disclosed:

A. Before agreeing to sponsor a meeting, adequate security protective measures must exist.

B. Meetings will be held only at a U.S. Government installation or contractor facility that holds an appropriate Defense Security Service Office Facility Security Clearance.

C. Once an APHIS component accepts sponsorship of a meeting, it assumes overall security responsibility, ensuring that the invitations are unclassified; that all attendees have the appropriate level of clearances and the need-to-know has been certified; that access rosters are prepared, checked, and coordinated with APHIS' ISP; and that the subject matter, location, and other aspects of the meeting are coordinated with the appropriate Security employees.

D. The Information Security Officer or designated Security employees must be notified if loss or compromise occurs before, during, or after the meeting.

E. The APHIS component ensures that all participants are advised of their security responsibilities, and that classified presentations are appropriately marked and safeguarded for later compilation and distribution through secure channels.

F. Classified information to be presented must be authorized for disclosure in advance by the department or agency having classified jurisdiction over the information involved.

G. Before showing or presenting the material, the briefer will announce the overall classification level of the slides being presented. Slides will not be shown unless the classification level is first disclosed by the presenter, and all employees attending the meeting have appropriate equal or higher clearance and need-to-know.

H. Written approval must be obtained from the ISO prior to disclosing classified information to non-Governmental employees or foreign visitors.

I. If foreign nationals are invited, submit a list containing their names, and the dates and locations of the sessions they will attend to the appropriate local security office.

6.2.2 AUTHORIZATION FOR REPRODUCTION OF CLASSIFIED MATERIAL

A. Top Secret material can be reproduced only by the (TSCO). Alternate TSCO's must gain the approval of the TSCO before reproducing any Top Secret material.

B. Secret information reproduction will be kept to the minimum number of copies needed.

C. Designation of Copiers**.** APHIS will designate copiers approved for reproduction of classified material. All employees handling classified information will be notified where the copier is located, and will ensure that the equipment is under their control when copying classified materials.

D. Other agency information. Prior to making copies of classified information produced or transferred from another agency, you must receive permission from the initiating agency.

6.2.3 TRANSMITTAL DOCUMENT

A transmittal document will indicate on the cover sheet the highest classification level of any classified information attached or enclosed.

A. If the transmittal contains no classified information in the body of the letter, the following statement will be centered at the bottom of the page:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED

B. If classified information 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*)

6.2.4 FACSIMILE MACHINE CONTROLS

Some facsimile machines can be connected to the telephone system through a secure interface, such as the STE. These interfaces may be used for the transmission of classified faxes. The following controls are established for use of secure fax machines to transmit classified information:

A. The sender of a classified fax is responsible for verifying that the intended recipient has the appropriate security clearance and need-to-know.

B. Transmission details will be worked out before the actual transmission, by the sender, to ensure the fax is received by the intended recipient.

C. All Top Secret faxes received will be taken to the TSCO for accountability.

D. Form AD-471, Classified Document Accountability Record, will be used for all classified fax transmissions and will be prepared by the sender and included with the fax. The AD-471 also serves as the receipt for the classified information, and will be completed by the recipient and faxed back to the sender at the completion of the transmission.

E. Cover sheets affixed to classified documents will not be obscured by transmittal notes, routing sheets, etc.

F. Cover sheets will not be removed from the document when the document is returned to the safe.

G. All pages of a secure fax must be accounted for by the recipient. The user of the secure fax must ensure all classified material is cleared from the fax prior to exiting the room. Return the CIK to secure storage upon completion of the transmission.

CHAPTER 6

SECTION 3 TRANSMISSION

6.3.1 PREPARATION OF MATERIAL FOR TRANSMISSION, SHIPMENT, OR CONVEYANCE

When classified information is transported from one location to another, it must be properly packaged to ensure the material is protected from accidental exposure or undetected deliberate compromise. The following information provides instructions on how to package classified information for transmission:

A. Envelopes or Containers. Classified documents will be placed in an inner and an outer envelope:

1. Inner envelope will be:

(a) Made of opaque material.

(b) Marked with the highest level of classification as contained in the document. The markings will be placed on the top left and bottom (front and back) of the envelope.

(c) Wrapped to make detection of tampering easy to ascertain.

(d) Contain recipient's address.

(e) Contain complete return address.

2. Outer envelope will be:

(a) Made of opaque material.

(b) Wrapped to make detection of tampering easy to ascertain.

(c) Contain no classification markings.

(d) Contain recipient's address.

(e) Contain complete return address.

B. Addressing. Classified information must be addressed to an official Government agency or department, or a Government contractor with a facility clearance, and not to an individual. The attention line of the address on the outer envelope will

appear as follows: “Attention: Security Office” (or “Officer”) or “Document Control,” as appropriate. When directing Secret or Confidential material to the attention of a particular individual, the person’s name may be indicated in an attention line on the inner envelope or container.

C. Approved Methods of Delivery for Classified Information.

1. Top Secret materials can be transmitted only by an authorized courier.

2. Secret information can be transmitted by courier, registered mail, or approved overnight carriers.

3. Confidential information can be transmitted by courier, registered mail, first class mail, or approved overnight carriers.

D. Carriers for Overnight Delivery of Secret and Confidential Information.

1. The General Services Administration has approved nine contract carriers for overnight mail express delivery. The carriers listed below may be used for urgent overnight transmission of SECRET and CONFIDENTIAL material within the continental United States when overnight delivery cannot reasonably be accomplished by the U.S. Postal Service. However, classified Communications Security (COMSEC) information, North Atlantic Treaty Organization (NATO), and foreign government information may not be transmitted overnight.

(a) Airborne Express.

(b) AirNet Systems.

(c) Associated Global Systems.

(d) Cavalier Logistics Management.

(e) CorTrans Logistics.

(f) DHL Airways.

(g) Federal Express.

(h) Menlo Worldwide Forwarding (formerly Emery).

(i) United Parcel Service.

2. Carrier employees should not be notified that the package contains classified material.

3. Senders may not use a Post Office Box as the destination address. Instead, a street delivery address approved for overnight shipments by the recipient's security officer will be used. Contractors must first obtain approval from the Defense Security Service (DSS) and the street address must be listed in the Central Verification Authority (CVA) before shipments can be made to that address. Identification of a contractor's address in the CVA listing as an authorized overnight delivery address indicates (CSO) approval of the receiving facility's ability to securely accept such packages.

4. A release signature block on the receipt label will not be executed under any circumstances. The use of external (street side) collection boxes is prohibited.

5. As a general rule, packages may be shipped on Monday through Thursday only, to ensure that the package does not remain in the possession of the carrier service over a weekend. However, the CSO may grant local approval to ship material on a Friday provided the receiver can ensure that a cleared person will receive and sign for the package on Saturday, and that he / she is able to secure the package in approved storage.

6. The sender is responsible for ensuring that an authorized person will be available to receive the delivery, and for verification of the correct mailing address. The receiving contractor must have procedures detailing how incoming overnight shipments will be received, transferred within the facility, and protected.

7. Employees who handle incoming overnight shipments addressed to the "Security Office" or the "Facility Security Officer" must be cleared. Once the initial recipient notes that the package is addressed to the "Security Office" or "Facility Security Officer," the material will be turned over promptly to a cleared individual.

CHAPTER 6

SECTION 4 PROCEDURES FOR HAND-CARRYING CLASSIFIED INFORMATION

6.4.1 APPROVAL PROCESS

APHIS employees required to act as couriers of classified material will contact the Information Security Officer (ISO) 48 hours in advance to obtain approval to hand-carry classified information. A United States Department of Agriculture (USDA) Courier Authorization letter will be issued only to those individuals whose duties require routine hand-carrying of classified material. 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. All couriers will receive an initial briefing and will be re-briefed annually on their responsibilities if the need for authorization remains valid. As a minimum, the courier briefing will include information on the following:

A. Espionage and known terrorist threats;

B. Proper receipting and control procedures;

C. Physical protection, wrapping, and storage procedures; and

D. Procedures to be taken in an emergency.

6.4.2 PROCEDURES FOR HAND-CARRYING CLASSIFIED INFORMATION THROUGH BORDERS OR AIRPORTS

There is no assurance of immunity from search by the customs, police, or immigration officials of the United States 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. If the senior official still has questions and concerns, have them contact the Information Security Officer at 301-436-3158 or 301-526-4647. If the senior official demands to see the actual contents of the package, precautions should be taken to ensure compromise of the information does not occur. The outer envelope may be opened but should be done in an area out of sight of the general public. Precautions should be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item. The courier should ask the official to repack or assist in the repackaging of the material immediately upon completion of the examination. The senior official should 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. The addressee and the dispatching ISO will be informed, in writing, of the incident. Include the following information: Date and time of the incident, name of the senior official requiring the package to be opened, the official's organization, his/her supervisor's name and telephone number, and the location where the incident took place.

6.4.3 PROCEDURES TO BE FOLLOWED WHILE HAND-CARRYING CLASSIFIED INFORMATION

A. Individuals hand-carrying classified information must have in their possession their valid USDA identification.

B. Classified material must remain in the personal possession, and under the constant surveillance of the courier at all times.

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

D. When classified information 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.

E. When transporting classified materials, the route will be mapped out ahead of time to ensure door-to-door transport. If door-to-door transport is not possible, prior arrangements for proper storage of the classified materials must be made. Classified material will not be stored overnight in an individual's hotel room or private residence. Classified materials can be taken to the following facilities for storage:

1. An FBI field office. A list of all field offices can be found at: http://www.fbi.gov/contact/fo/fo.htm

2. A DoD military installation. Military installations by State can be found at: http://www.military.com/InstallationGuides/ChooseInstallation/1,11400,,00.html

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

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

CHAPTER 6

SECTION 5 CLASSIFIED DOCUMENT ACCOUNTABILITY AND CONTROL

6.5.1 COLLATERAL TOP SECRET CONTROL OFFICER (TSCO) PROGRAM

Top Secret information, if disclosed, could cause exceptional, grave damage to the security of the United States. A TSCO and at least one alternate will be appointed by APHIS that prepares, receives, stores, or handles Top Secret material. Material received by APHIS program offices must be logged in by the Agency TSCO, and then receipted to the appropriate APHIS Program. All TSCOs and alternates must possess a Top Secret clearance (interim clearance is not acceptable for this position). Such individuals will be selected on the basis of experience and reliability. Except in unusual circumstances, the TSCO will not be the person designated as the APHIS Information Security officer. Top Secret material must be taken to the TSCO or alternate for processing into the Top Secret account.

Top Secret Information.

1. Control Officers. TSCO and alternates will be designated within offices with approved areas for storage of Top Secret information.

2. Top Secret Registers. Top Secret accountability registers using the General Service Administration (GSA) Classified Document Register, Form 1567, will be maintained by the TSCO.

    (a) Top Secret Registers will be retained for 5 years from the date of the disposition of the last item on each sheet. As a minimum, the Top Secret Register will reflect the following:

        (1) Document Control Number. A control number identifiable with the Program receiving the document will be assigned to all Top Secret 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.

        (2) Date of Receipt. The date of the document or date the material was received.

        (3) Classification. The level at which the document is classified (Confidential, Secret, Top Secret).

(4) Unclassified Title or Description sufficient to identify adequately the Top Secret document or material. This description includes the unclassified title or appropriate short title, date of the document, serial number, and copy number(s).

(5) Originating Agency. Name of the originating agency and the agency the document was received from.

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

(7) Serialization and Copy Numbering. Top Secret documents originated and derivatively classified by USDA activities that are numbered serially. In addition, each Top Secret document will be marked to indicate its copy number, for example, copy 1 of 2 copies.

(8) Disclosure Records. A Top Secret Access Record, GSA Form 1566, appended to each Top Secret document or item of 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. Form 1566 should remain attached to the document until the document is downgraded, transmitted outside USDA, or destroyed. Form 1566 will be retained 5 years from the disposition date of the document.

(9) Inventories. All Top Secret documents and material inventoried semi-annually and more frequently where circumstances warrant. The inventory will reconcile the Top Secret accountability register with the documents or material on hand. At such time, each document or material will be examined for completeness. A report will be submitted to the APHIS ISO through 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.

(10) Retention. Top Secret information retained only to the extent necessary to satisfy current requirements. TSCOs will destroy copies of Top Secret documents when they are no longer needed. Record copies of documents that cannot be destroyed will be, when appropriate, retired to designated records centers.

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

(12) Reproduction. Top Secret documents, or portions of documents containing Top Secret information which must not be reproduced without the consent of the originator. Copies of documents containing Top Secret information must be kept to an absolute minimum. Records must be maintained of reproduced Top Secret documents to show the number, distribution, and authority for reproduction.

(13) Destruction. A Certificate of Destruction of Classified Material, Form AD-471 Classified Document Accountability Record, is required for Top Secret information. Please refer to Chapter 7 for more information on destruction.

6.5.2 CUSTODIANS DOCUMENTATION FOR SECRET AND CONFIDENTIAL INFORMATION

A. When Secret documents or material are transmitted or destroyed, Form AD-471 Classified Document Accountability Record, will be prepared to identify the material being transmitted. Form AD-471 will be maintained for 2 years from the date of the disposition of the last item on each sheet and will, as a minimum, reflect the following:

(1) Document Control. Keep only the receipt and disposition part of the form for all Secret and Confidential documents.

(2) Date of Receipt. The date the document or material was received or destroyed.

(3) Classification. The level to which the document is classified.

(4) Unclassified Title or Description. Sufficient information to adequately identify the document or material. This information is to include the unclassified title or appropriate short title, date of the document, and copy number(s).

(5) Originating Agency. Identify the originating agency and the agency the document was received from.

B. Inventories. All Secret and Confidential documents and material will be inventoried annually and more frequently when circumstances warrant. A report will be submitted to the APHIS ISP through the program TSCO within three working days from the requested date. This information should include the total number of documents for each classification derivatively classified during the previous 6 months.

C. Retention. Classified information will be retained only to the extent necessary to satisfy current requirements. Custodians will destroy non-record copies of classified documents when no longer needed. Record copies of documents that cannot be destroyed will be, when appropriate, retired to designated records centers.

D. Reproduction. The number of copies of documents containing classified information must be kept to an absolute minimum. Secret and Confidential documents that bear special dissemination and reproduction limitations will be reproduced only with the consent of the originator. Records must be maintained of reproduced documents with special limitations to show the number, distribution, and authority for reproduction.

CHAPTER 7 DISPOSAL AND DESTRUCTION

7.1 POLICY

Classified documents and other material will be retained only if they are required for effective operation of the organization or if law or regulation requires their retention. Documents that are no longer required will be destroyed or disposed of in accordance with the provisions of the Federal Records Act and this Handbook. Destruction of classified documents will be accomplished by means that eliminate the risk of reconstruction of the classified information they contain.

7.2 DESTRUCTION OF MATERIAL

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

A. Shredders. Approved crosscut shredders must be used to destroy classified information. Only shredders listed on the National Security Agency (NSA) Central Security Service (CSS) approved evaluated list will be used for destroying classified documents. These shredders must be able to crosscut shred at 5mm X 5mm or smaller. When shredding controlled documents, Form AD-471, Classified Material Receipt, must be completed.

(1) Signatures are required from two people who are authorized to handle the material (shredder and witness) when shredding Top Secret material.

(2) One signature is required when shredding Secret and Confidential material.

B. Computer Diskettes. Certain occasions may necessitate the destruction of classified or sensitive unclassified computer diskettes. This should be accomplished only when the diskette cannot be overwritten using NSA approved software or if degaussing is impractical or unavailable.

C. Destruction of material that cannot be shredded, such as Hard Drives etc., will occur at the NSA Physical Destruction Office, located at Fort Meade, Maryland. The destruction of this type of materials will be conducted by the Information Security Officer.

CHAPTER 8 SECURITY EDUCATION

8.1 POLICY

All APHIS offices will ensure that all employees who hold a security clearance will fulfill the security education requirements as indicated below.

8.2 SECURITY EDUCATION

The effectiveness of the APHIS Information Security Program is proportional to the degree employees understand their responsibilities within the program. An integral part of the program is security education. To ensure that employees become aware of their responsibilities, security education training is provided through the following briefings:

A. Initial Briefings. Employees granted a security clearance are not permitted access to classified information until they are briefed on the requirements of safeguarding classified information and sign a "Classified Information Nondisclosure Agreement." The USDA Personnel and Document Security Division (PDSD) will conduct the initial briefings for employees. A copy of the completed Certificate of Clearance and/or Security Determination will be sent to the APHIS Information Security Officer (ISO).

B. Refresher Briefings. The APHIS ISO conducts annual refresher briefings for employees with clearances. APHIS program field office employees can complete the web-based training briefings (if available). This training reacquaints employees with their responsibilities on the various requirements for handling classified information and other elements of the Personnel Security Program.

C. Termination Briefings.

1. Government and contract employees receive a termination briefing when:

(a) Assignment is complete or employment is terminated.

(b) A contemplated absence from duty or employment will last for 60 days or more.

(c) Access to classified or sensitive unclassified information is suspended.

2. Employees must contact USDA, PDSD, to receive a Security Termination Statement.

3. If an employee refuses to execute a Security Termination Statement, the refusal to sign will be recorded in the Defense Central Index of Investigations.

CHAPTER 9 LOSS, POSSIBLE COMPROMISE, OR UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

9.1 GENERAL

Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) must immediately report the circumstances to your local security office, the ISC or the ISB.

9.2 COMPROMISE OF CLASSIFIED INFORMATION

To determine the circumstances of occurrence, a preliminary inquiry is immediately initiated into incidents of compromise, possible compromise, possible loss of classified information, or an infraction of the safeguarding controls as established by this Handbook. 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.

9.3 INQUIRY OR INVESTIGATION

The purpose of an inquiry or investigation is to determine:

A. Whether or not a security incident has occurred;

B. The source and reason for the security incident;

C. Appropriate measures or actions to minimize or negate the adverse effect of the security incident;

D. The seriousness of damage to U.S. interests; or

E. The vulnerabilities in the security program that could result in similar incidents in the future.

9.4 DEBRIEFINGS IN CASES OF UNAUTHORIZED ACCESS

In cases where a person has had unauthorized access to classified information, 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 APHIS ISO. 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 classified information. The following guidelines apply:

A. If the unauthorized access was by a person with the appropriate security clearance but without a 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. The person should 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. The debriefing official should make sure the individual understands what classified information is and why its protection is important, and what to do should someone try to obtain the information. If the person who had unauthorized access is an employee of a contractor participating in the National Industrial Security Program, the same guidelines apply as for Government employees.

9.5 DISCOVERY

Any person who discovers classified information improperly secured or unprotected will take custody of the information, safeguard it in an appropriate manner, and immediately report the incident to the ISO. If classified information appears in the public media, Agency employees are cautioned not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. If approached by a representative of the media who wishes to discuss information believed to be classified, individuals should neither confirm nor deny the accuracy of the information and should report the situation immediately to the ISO and a Public Affairs specialist in the Legislative and Public Affairs staff.

9.6 APPOINTMENT OF PRELIMINARY INQUIRY OFFICER (PIO)

Upon notification of a security incident or violation, the ISO will notify the USDA Personnel and Document Security Division (PDSD) of the security incident or violation. The PDSD will request in memorandum format the details of the incident. The ISO will appoint a PIO in writing. The ISO 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. The following individuals will take action after a security incident is reported:

A. The ISO will:

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 have an appropriate security clearance, must have the ability and available resources to conduct an effective inquiry, and must not have been involved, directly or indirectly, in the incident. Except in unusual circumstances, the activity security officer should 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 ISO.

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 the Human Resources Division, Employee Relations Branch.

B. The PIO will:

1. Obtain a briefing from the ISO to receive initial facts and evidence surrounding the incident.

2. Consult with PDSD for technical guidance in conducting the inquiry.

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 classified information 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. He / she will describe exactly what happened in chronological order.

(e) A brief summary of conclusions reached after a review of all pertinent information. Conclusions must be supported by the facts. The evidence obtained during the inquiry process must support the facts.

(f) If the compromise of classified information 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 classified information did not occur.

(2) Compromise of classified information may have occurred.

(3) Compromise of classified information did occur, but there is no reasonable possibility of damage to national security.

(4) Compromise of classified information did occur, and damage to national security may result.

(g) Suggested corrective action to prevent future incidents.

4. Mark each page "FOR OFFICIAL USE ONLY" unless the report contains classified material, and then mark accordingly. The report will be routed through the ISO for a technical review and further processing.

9.7 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.

9.8 SANCTIONS

A. Employees will be subject to sanctions if they knowingly, willfully, or negligently:

1. Disclose to unauthorized persons properly classified information;

2. Classify or continue the classification of information in violation of federal regulations;

3. Create or continue a Special Access Program contrary to the requirements of a regulation; or

4. Violate any other provisions of Federal regulations pertaining to classified information.

B. Sanctions include, but are not limited to: warning, reprimand, suspension without pay, forfeiture of pay, removal, loss or denial of access to classified information, and removal of classification authority. Action also may be taken under the applicable criminal law.

CHAPTER 10 PROGRAM MANAGEMENT

10.1 PROGRAM MONITORING

The APHIS Information Security Program (ISP) requires that all APHIS locations where classified information is handled or stored, will be inspected and monitored to ensure that appropriate security measures are being followed. Written documentation of inspections will be maintained and made available for a minimum of 2 years. Counterintelligence technical inspections will be conducted or scheduled by the USDA Personnel and Document Security Division (PDSD) on an "as needed" or recurring basis.

10.2 HEADQUARTERS, REGIONAL AND FIELD PROGRAM MANAGEMENT

Programs will appoint, in writing, an official to serve as security contact for each of the program activities. Security contacts are responsible for the administration of an effective ISP in their area of responsibility, emphasizing security education and training. They will serve as a focal point for their Program to provide advice and assistance regarding APHIS policy on classification, declassification, downgrading, and marking of national security information. They will help coordinate the following actions with the Information Security Officer (ISO):

A. Ensure that indoctrination, refresher, threat, courier, foreign travel, and termination briefings are conducted.

B. Ensure a periodic document review program is conducted annually in each program activity to reduce unnecessary classified holdings. The program will include downgrading, declassifying, destroying, or returning the documents to the originator.

C. Report all security incidents or violations to the ISO and serve as the point of contact on the status of ongoing preliminary inquiries or formal investigations.

D. Prepare or coordinate requests for designation letters.

E. Maintain and report on all classified information stored, handled, and processed in their program.

10.3 ENTRY AND EXIT SECURITY CHECKS

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 and restricted 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, loss of security clearance, or other administrative actions.

CHAPTER 11 SELF INSPECTIONS

11.1 GENERAL

Self inspections are the internal review and evaluation of activities with respect to the implementation of the Information Security Program. These inspections can be accomplished by the Information Security Officer (ISO), local security officers, or Information Security Coordinators.

11.2 FREQUENCY

Self inspections should be conducted at least every 2 years. The ISO will conduct random inspections throughout APHIS in order to meet the requirements of Executive Order 12958, as amended. Self inspections also should be conducted when a pattern of security violations or infractions reveals a security weakness.

11.3 INSPECTION COVERAGE

Executive Order 12958 defines the coverage of a self inspection. The Self Inspection Checklist will be used as a guide for self inspections.