



United States
Department of
Agriculture

Food Safety
and Inspection
Service

FSIS Directive
2620.2

Guidelines for Handling and Distributing Classified Documents

GUIDELINES FOR HANDLING AND DISTRIBUTING CLASSIFIED DOCUMENTS

TABLE OF CONTENTS

BASIC PROVISIONS

| | Title | Page No. |
|-------|--|----------|
| I. | PURPOSE | 1 |
| II. | (RESERVED). | 1 |
| III. | (RESERVED) | 1 |
| IV. | REFERENCES | 1 |
| V. | ABBREVIATIONS AND FORMS. | 1 |
| VI. | POLICY | 2 |
| | A. Original Classification | 2 |
| | B. Derivative Classification | 2 |
| VII. | DEFINITIONS | 2 |
| | A. Authorized for Release to (REL TO) | 2 |
| | B. Caution - Proprietary Information Involved (PROPRIN) or (PR) | 2 |
| | C. Communications Security (COMSEC). | 2 |
| | D. Confidential | 2 |
| | E. Critical Nuclear Weapons Design Information (CNWD) or (N). | 3 |
| | F. Cryptographic Material (CRYPTO) | 3 |
| | G. Dissemination and Extraction of Information Controlled by Originator (ORCON) or (OC) | 3 |
| | H. NOFORN | 3 |
| | I. Not Releasable to Contractors/Consultants (NOCONTRACT). | 3 |
| | J. Secret | 3 |
| | K. Sensitive Compartmented Information (SCI) | 3 |
| | L. Top Secret | 3 |
| | M. Warning Notice--Intelligence Services or Methods Involved (WNINTEL) | 3 |
| VIII. | RESPONSIBILITY | 3 |
| IX. | HANDLING FSIS CLASSIFIED INFORMATION | 4 |
| | A. General Guidelines | 4 |
| | B. Safe Handling | 5 |
| | C. Secure Containers | 6 |
| | D. FSIS Classified Information Distribution | 6 |
| | E. FSIS Classified Information Inventory | 8 |
| | F. Wrapping of Materials | 8 |
| | G. Mailing of FSIS Classified Information. | 9 |
| | H. Secure Computers | 10 |
| | I. Classified Document Reproduction | 11 |
| | J. Secure Telephone and Facsimile Transmission | 11 |
| X. | ADDITIONAL INFORMATION | 12 |
| | ATTACHMENT 1, Approved Overnight Carriers - U.S. Only | 13 |

UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

| | | |
|-----------------------|--------|--------|
| FSIS DIRECTIVE | 2620.2 | 9/7/06 |
|-----------------------|--------|--------|

**GUIDELINES FOR HANDLING AND DISTRIBUTING
CLASSIFIED DOCUMENTS**

I. PURPOSE

This directive prescribes procedures for handling and distributing classified documents.

II. (RESERVED)

III. (RESERVED)

IV. REFERENCES

Executive Order 12958, Classified National Security Information

V. ABBREVIATIONS AND FORMS

The following appear in their shortened form in this directive:

| | |
|------------|--|
| CD-ROM | Compact Disc Read Only Memory |
| CNWD | Critical Nuclear Weapons Design Information |
| COMSEC | Communications Security |
| CRYPTO | Cryptographic Material |
| E-mail | Electronic Mail |
| GSA | Government Services Administration |
| NSA | National Security Agency |
| NATO | North Atlantic Treaty Organization |
| NOCONTRACT | Not Releasable to Contractors or Consultants |
| NOFORN | No Foreign Nationals |
| OCIO | Office of Chief Information Officer |
| OFDER | Office of Food Defense and Emergency Response |
| ORCON | Dissemination and Extraction of Information Controlled by Originator |

DISTRIBUTION:

All Offices

OPI:

OFDER - Scientific and Technical
Support Staff

| | |
|---------|---|
| PDS | USDA Personnel and Document Security Division |
| STU III | Secure Telephone Unit Third Generation |
| SCI | Sensitive Compartmented Information |
| STSS | Scientific and Technical Support Staff |
| TS | Top Secret |
| WINTEL | Warning Notice – Intelligence Sources or Methods Involved |

| | |
|--------|-------------------------------------|
| AD-471 | Classified Material Control Receipt |
| SF-700 | Security Container Information |
| SF-702 | Security Container Check Sheet |
| SF-706 | Top Secret Media Label |
| SF-707 | Secret Media Label |
| SF-708 | Confidential Media Label |
| SF-709 | Classified Media Label |
| SF-710 | Unclassified Media Label |

VI. POLICY

FSIS policy protects national security information from unauthorized disclosure. Information classified as:

A. **Original Classification** is the initial determination that information requires protection. Only U.S. Government officials with this authority, delegated in writing, and trained in classification requirements has the authority for original classification.

B. **Derivative Classification** is the act of classifying a specific information item or material based on an original classification decision already made by an authorized original classification authority.

VII. DEFINITIONS

A. **Authorized for Release to (REL TO)**. Classified information that may be released through proper disclosure channels to the named foreign government or international organization.

B. **Caution – Proprietary Information Involved (PROPIN) or (PR)**. A term used with or without a security classification to identify information provided by a commercial firm or private source under an express or implied understanding that the information is protected as a trade secret or proprietary data with actual value

C. **Communications Security (COMSEC)**. A system to protect all telecommunication elements: encryption, transmission, emissions, and the physical security of equipment and materials.

D. **Confidential**. Information disclosed without authorization, could cause damage to national security.

E. **Critical Nuclear Weapons Design Information (CNWD) or (N).** Applies to information that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition, ammunition, or test device. Special handling procedures are required.

F. **Cryptographic Material (CRYPTO).** Identifies information or materials that must be handled through special cryptographic channels.

G. **Dissemination and Extraction of Information Controlled by Originator (ORCON) or (OC).** Additional distribution or inclusion in another document must be approved by the document's originator. It is used on intelligence information that could permit identification of a sensitive intelligence source or method.

H. **NOFORN.** Intelligence information that may not be passed to foreign nationals.

I. **Not Releasable to Contractors or Consultants (NOCONTRACT).** Has been discontinued but is still seen on older documents. The reviewer should check with the originator of the document regarding any ongoing controls on the use of such a document. This caveat was used on intelligence information that is provided by a source on the express or implied condition that it not be made available to contractors; or that, if disclosed to a contractor, would actually or potentially give them a competitive advantage or cause a conflict of interest with their obligation to protect the information.

J. **Secret.** Information, if disclosed without authorization, could reasonably be expected to cause serious damage to national security.

K. **Sensitive Compartmented Information (SCI).** Applies to certain intelligence sources, methods, or analytical processes that are subject to a formal access control system established by the Director of Central Intelligence. Special approval is required for access to SCI.

L. **Top Secret.** Information, if disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to national security.

M. **Warning Notice - Intelligence Sources or Methods Involved (WNINTEL).** Has been discontinued but is still seen on older documents. Used on intelligence information to identify or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness.

VIII. **RESPONSIBILITY**

A. The OFDER STSS Director maintains Agency document security responsibility. The Agency handles classified material in scientific vulnerability assessment and studies. These studies often originate in the OFDER or the Office of Public Health Science and are shared with other Federal agencies on a need-to-know basis which requires an appropriate security clearance.

B. Information is obtained from the USDA PDSD's Information Security Program website for proper classified document handling and distribution.

IX. HANDLING CLASSIFIED INFORMATION

A. **General Guidelines.** Always safeguard classified information to prevent loss or compromise, and unauthorized disclosure, dissemination, or duplication. Unauthorized classified material disclosure is punishable under the Federal Criminal Statutes or organizational policies.

1. Designated employee controls classified documents by:
 - a. Logging documents on an inventory sheet retained in a secure container with:
 - (1) Name.
 - (2) Date received.
 - (3) Received from whom.
 - b. Conducting and verifying classified document inventory quarterly.
2. Safeguard classified information in a GSA-approved secure container. Contact OFDER for information on approved containers. Classified information not safeguarded in an approved secure container must remain under the control of a person with the proper clearance level
3. Properly protect unattended classified material (**example**: on a desk). If classified material is compromised:
 - a. An employee with the appropriate security clearance level must remain with unattended classified material.
 - b. Notify the security office if possible.
 - c. Deliver documents or other material to the Security Office:
 - (1) Supervisor.
 - (2) Person authorized access to the information.
 - (3) Alternately lock the material in an approved secure container overnight.

B. Safe Handling.

1. Do not dispose of classified documents in a waste basket or recycle bag. Destroy classified documents by making arrangements to use an NSA-approved shredder. If one is not available, make arrangements with PDSD to have the information burned at an approved incinerator. Classified documents destruction is as follows:

a. TS information destruction requires:

- (1) Two people with TS level clearances for destruction.
- (2) One person acts as a witness.
- (3) Documentation.

b. Secret information destruction requires only one person and they must hold at least a Secret clearance.

2. E-mail and the Internet create many opportunities for inadvertent disclosure of classified information. Classified information is prohibited from unsecured electronic transmissions. Before sending an e-mail, posting to a bulletin board, publishing anything on the Internet, or adding to an existing Web page, one must be certain that none of the information is classified.

3. Classified working papers such as notes and rough drafts should be:

- a. Dated when created.
- b. Marked with the overall classification.
- c. Annotated with "Working Papers."
- d. Disposed of properly with other classified waste when no longer needed.

4. If classified information is stored on magnetic media such as, computer diskettes, magnetic tape, CDs, or used typewriter ribbons, they must be:

- a. Labeled with the highest classification level resident on the media. Obtain pre-printed label SF 707-710, through GSA at <http://www.gsa.gov>.
- b. Stored in an approved secure container.
- c. Maintained in the custody of an individual with the proper clearance level and "need to know" when not in use.

5. When classified material is stored in a secure container:

a. Label the folder on the top and bottom, front and back side with the enclosed material classification.

b. Attach a cover sheet labeled with the identified classification level.

C. Secure Containers.

1. Safeguard classified information in a GSA-approved secure container. Contact OFDER for information on approved containers.

2. Maintain a log sheet SF-702. Make a log entry each time the container is opened. Obtain log sheets at <http://www.gsa.gov>.

3. Safeguard all classified information in an approved secure container or under the control of a person having the proper clearance or need to know.

4. Record secure container combination on the SF-700. Follow the form instructions and provide the envelope to PDSD marked "Secret."

5. Change combinations to secure containers, secure rooms, or vaults when any one of the following events occurs:

a. Placed in use after procurement or moved to a new area of responsibility.

b. An individual knowing the combination is transferred, discharged, or reassigned; or if an individual's clearance is downgraded, suspended, or revoked.

c. The combination or record of combination is suspected of possible compromise.

d. Every three years, unless more frequent change is dictated by the material type stored therein (**example**: NATO and COMSEC material every six months).

e. A container is placed out of service.

D. FSIS Classified Information Distribution.

1. Different procedures exist for hand-carrying classified material via surface transportation, commercial air, government air, and transportation outside the United States. All hand-carried classified material requires a Courier Letter issued by PDSD (202) 720-7373.

2. A completed AD-471 must accompany classified material for recipient's signature; return a signed copy to the sender for filing in a secure container. Process AD-471 as follows:

- a. **TS** material requires a continuous chain of receipts, AD-471, documenting each individual who obtains custody and upon delivery.
- b. **Secret** material requires a classified AD-471 upon delivery.
- c. **Confidential** material requires a classified AD-471 upon delivery only if the sender deems it necessary or transmitting to a foreign government.
- d. **Return** a signed copy of AD-471 to sender.
- e. **Retain** a copy of AD-471 in secure container.

3. Protect all classified material transported by car or foot to another location from all foreseeable contingencies while in transit.

a. Automobile accident, theft and sudden illness are all foreseeable contingencies.

(1) Double wrap or package as though it were being sent by mail.

(2) Keep under constant control (**example**: not left in a car trunk).

(3) Deliver only to an authorized person.

(4) A briefcase may serve as the outer wrapper only if it is locked and approved for carrying classified material.

(5) Prepare a material inventory and retain a copy in the office. Provide an additional copy to a security officer or other responsible person.

b. Air travel requires a written authorization letter from the Agency's security office. Aircraft transportation may require advance airline notification due to security screening.

4. Loaning classified material requires:

a. "Need to know" and proper clearance level. PDSD must verify an external receiver's clearance level and need to know.

b. Ability to store it properly.

c. Recorded on a log sheet:

- (1) Requestor's name.
- (2) Check out date.
- (3) Document name and classification
- (4) Where it is to be kept.
- (5) Anticipated return date and actual return date.

5. **Top Secret** material transmission requires a continuous chain of receipts covering each individual who obtains custody.

6. **Secret** material requires a classified material receipt with all material transmitted outside the facility.

7. **Confidential** material transmission requires a receipt only if the sender deems it necessary; or if the transmission is to a foreign government.

8. Keep receipts in a secure container with a copy of the classified material.

9. Inventory all documents bearing the above classification levels and store in a GSA-approved secure container.

E. **FSIS Classified Information Inventory.** All documents that bear any of the above classification levels must be inventoried and stored in a GSA-approved secure container.

F. **Wrapping of Materials .**

1. Double-wrap all classified material with opaque inner and outer covers.

2. Mark the inner envelope top and bottom on both sides, preferably in red, with the classification in all capital letters. Mark boxes containing classified material with the classification on all inner wrapping surfaces.

3. Ensure complete mailing and return addresses are contained on the **inner** envelope along with a point of contact name. The address on the **inner** envelope should have the name of an appropriately cleared individual.

4. Attach or enclose in the inner envelope, a receipt identifying the sender, the addressee, and the document. Ensure that receipts do not contain classified information. Sign receipts and return to sender.

5. The outer envelope contains the complete mailing address and return address.
 - a. The **outer** envelope **does not** state that it contains classified information.
 - b. Address classified mail or shipments to the Administrator or other organization head by title, not by name, or to an approved classified mailing address of a federal activity or to a cleared contractor using the name and classified mailing address of the facility.
 - c. An individual's name should not appear on the outer envelope. Instead of a person's name, use office code letters, numbers, or phrases in an attention line to aid with internal routing.
 - d. When necessary to direct material to the attention of a particular individual, put the individual's name on an attention line in the transmittal letter or on the inner container or wrapper.

6. A briefcase or lockable pouch may serve as the outer wrapper only if it is locked and GSA-approved for carrying classified material.

G. Mailing FSIS Classified Information.

1. Do not send TS materials in the mail under any circumstances. All cleared TS material must be sent by DOD or State Department courier or hand-carried by a USDA employee.
2. Send Secret material via the U.S. Postal Service using registered mail or express mail within and between the United States and its territories. There are nine approved carriers for transporting secret material for urgent, overnight delivery. See Attachment 1 for a list of U.S. only approved overnight carriers. Contractors must receive approval from their government contracting authority to use this method.
3. Confidential material is subject to the same mailing procedures as Secret material, with the following exceptions:
 - a. Send Confidential material by U.S. Certified mail rather than by U.S. Registered mail.
 - b. Government agencies (but not contractors) may also send Confidential material by First Class mail between and among government agencies only. It cannot be sent to contractors via First Class mail.
4. Under all circumstances, mark the outer envelope "Do Not Forward. Return to Sender."
5. Mail classified material at the post office. Use of street mail collection boxes is prohibited.

H. Secure Computers.

1. Classified processing can only be done on an approved classified computer. An approved computer can be a computer that is located in a room approved for storage of classified material or on a computer that has a removable hard drive, which is stored in an approved secure container when not in use.
2. A laptop computer can be used for classified processing, but once it's used for classified processing, it must then be treated as classified equipment and stored in an approved secure container when not in use.
3. Classified computers cannot have a physical connection to the internet or intranet (**example**: local area network). Stand-alone systems are required.
4. Properly label computers (**example**: SECURE COMPUTER--used for processing classified information up to Secret. Property of USDA FSIS). Use proper authorization and connectivity procedures. Obtain labels from OFDER.
5. Do not enter into any secure computer system without authorization. Unauthorized entry into a protected or compartmented computer file is a serious security violation and considered as a basis for revocation of a secure clearance.
6. Do not store or process classified information on any system not explicitly approved for classified processing. Do not attempt to circumvent or defeat security or auditing systems without prior authorization from the system administrator, other than as part of a system test or security research authorized in advance.
7. Do not install computer software without the system administrator's approval.
8. Do not use another individual's user identification, password, or identity.
9. Do not permit an unauthorized individual (**example**: spouse, relative or friend) access to a secure computer system.
10. Do not reveal passwords to anyone including the computer system administrator.
11. Do not modify or alter the operating system or configuration of any system without first obtaining permission from the owner or system administrator.
12. Do not use the office computer system to gain unauthorized access to any other computer system.
13. Print classified documents using a secure laptop:
 - (a) Connect the laptop directly to the printer.

- (b) Run three clean sheets of paper after initial printing.
- (c) Power down the printer.
- (d) Turn the printer on.
- (e) Run one additional clean sheet of paper.

I. Classified Document Reproduction.

1. Upon legitimate request for a copy of a classified document, the designated document security employee provides that copy in one of two ways:

(a) If the document is stored on a diskette that is kept in an approved secure container, the employee prints a copy of the document from a secure laptop computer. When printing from a secure computer, it must be directly connected to the printer.

(b) If the document is not stored on disk, the employee carries the document, using appropriate safeguard procedures for classified documents, to the PDSD Office and makes a photocopy on the secure photocopy machine. **NOTE:** If located outside of the Washington, DC headquarters area, use a designated photocopier that is owned by USDA, not leased, and disabled from connection to a network or outside entities. The copier must be OCIO or PDSD-approved.

2. The OFDER employee numbers TS documents (#1, #2, etc.,) if multiple copies are made.

3. Employee returns the document to the approved secure container after making the copies.

4. Mark floppy disks and CD-ROM's containing classified documents, with the appropriate classification level. Obtain pre-printed SF 706-710 labels through GSA at <http://www.gsa.gov>.

J. Secure Telephone and Facsimile Transmission.

1. Transmit and receive classified information securely using a GSA-approved secure phone (**example:** STU III) which is required to discuss Secret and TS-level information.

(a) Send classified facsimiles over GSA-approved secure facsimile machine approved for the document classification level.

(b) TS documents require facsimile machines with TS-level clearance. USDA has a few of these machines and they are distributed based on the user's capability to properly store TS documents.

(c) All classified facsimiles must accompany a transmittal sheet marked top and bottom with the highest document classification level.

(d) The receiving facsimile machine must meet these requirements (**example**: a facsimile machine approved for Secret transmissions cannot receive a TS facsimile).

2. If unsure of the qualifications of an individual to participate in a secure telephone conversation or receive a classified facsimile, contact OFDER who contacts PSDS to verify the external receiver's security clearance and "need to know."

3. OFDER tests equipment quarterly for transmission capabilities by sending a transmission test from FSIS Headquarters to each FSIS location having a secure telephone and facsimile, (**example**: Agency's Athens laboratory or Continuity of Operations Plans sites).

X. **ADDITIONAL INFORMATION**

A. View additional information for handling and distributing classified information on the USDA PDSD's Information Security Program Website at:
<http://www.usda.gov/da/infosec/index.htm>.

B. Direct all questions to the FSIS OFDER at (202) 720-5643.



Assistant Administrator
Office of Management

Attachment

1 Approved Overnight Carriers - U.S. Only

APPROVED OVERNIGHT CARRIERS - U.S. ONLY

Airborne Express

AirNet Systems

Associated Global Systems

Cavalier Logistics

DHL Airways

Federal Express

Menlo Worldwide Forwarding (formerly Emergy)

United Parcel Service