UNITED STATES POSTAL SERVICE®

Classified National Security Information Program

Handbook AS-303

August 2007
Transmittal Letter

A. Explanation. This is a complete revision of Handbook AS-303, *National Security Information.* Immediately dispose of all copies of Handbook AS-303, with Transmittal Letter 2 (TL-2) dated January 30, 1987.

B. Purpose. This handbook provides Postal Service™ instructions and procedures for the management, accountability, and protection of classified national security information.

C. Scope. These instructions and procedures apply to all Postal Service officials, employees, and contractors who need access to classified national security information.

D. Policy. Postal Service policy about audits and investigations can be found in Chapter 2 of the Administrative Support Manual.

E. Questions and Comments. Send comments and questions to:

ATTENTION DMI-HS
CHIEF POSTAL INSPECTOR
INVESTIGATIONS AND SECURITY OPERATIONS
UNITED STATES POSTAL SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON DC 20260-3301

Al Lazaroff
Chief Postal Inspector
U.S. Postal Inspection Service

Special Notes

This handbook provides guidance to Postal Service employees for the proper handling and storage of classified national security information. Executive Order (EO) 12958, as amended, *Classified National Security Information* and the Information Security Oversight Office (ISOO) Implementing Directive Number 1 are the authorizing documents upon which this guidance is based. Nothing in this handbook should be construed as contradicting either of these two documents. Not all of the information in the EO or the ISOO directive is included in this handbook.

Questions relating to the guidance provided in this handbook, the executive order, and the implementing directive may be referred to the Inspector in Charge, Dangerous Mail Investigations - Homeland Security (INC, DMI-HS).

All references to EO 12958 mean the executive order *as amended.*

All references to "ISOO Directive Number 1" mean the ISOO Implementing Directive Number 1, as amended.

EO 12958 is available at: *http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html.*

The ISOO directive is available at *http://www.archives.gov/isoo.*

Forms cited in this handbook may be available on the General Services Administration Web site at *www.gsa.gov/forms* or on the Postal Service intranet (Blue) at *http://blue.usps.gov.* Questions about any forms cited in this handbook or how to obtain them should be directed to:

INSPECTOR IN CHARGE
DMI-HS
INVESTIGATIONS AND SECURITY OPERATIONS
UNITED STATES POSTAL SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON DC 20260-3301

This page intentionally left blank

Contents

This page intentionally left blank

Exhibits

This page intentionally left blank

1 Classified Information

1-1 Use

Classified national security information is transmitted to the Postal Service by other federal departments and agencies. This information is used by designated Postal Service officials, employees, and contractors who require access in the performance of their official duties according to Executive Order (EO) 12958, as amended, *Classified National Security Information.*

Access. The ability or opportunity to gain knowledge of classified information.

Classified information. Information determined according to EO 12958 as amended or any predecessor order to require protection against unauthorized disclosure. Classified information is marked to indicate its classified status when it is in documentary form. Categories of classified information are Top Secret, Secret, and Confidential.

Information. Any knowledge that can be communicated, including documentary material, regardless of physical form or characteristics that is owned by, produced by or for, or is under the control of the United States Government.

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

Postal Service official. An officer, manager, or other employee designated in charge of carrying out particular Postal Service functions.

1-2 Classification Conventions

National security information may be classified one of two ways: originally or derivatively.

The Postal Service does not have original classification authority but does, on occasion, classify derivative information supplied to it from other federal departments and agencies.

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.

Derivative classification. The act of incorporating, paraphrasing, restating, or generating in new form information that is already classified and marking the newly developed material consistent with the classification markings from the source information. The Postal Service does have occasion to derivatively classify information supplied to it from other federal agencies.

Original classification. The act of determining initially that information requires, in the interest of national security, protection against unauthorized disclosure.

Original classification authority. Authority for an individual authorized in writing either by the President of the United States or by agency heads or other officials designated by the President to classify national security information in the first instance. The Postal Service does not have original classification authority. See EO 12958, as amended, for additional information.

1-2.1 Levels

National security information may be classified at one of the following three levels:

a. ***Top Secret*** — Applies to information that, if disclosed without authorization, could reasonably be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to describe.

b. ***Secret*** — Applies to information that, if disclosed without authorization, could reasonably be expected to cause *serious damage* to the national security that the original classification authority is able to describe.

c. ***Confidential*** — Applies to information that, if disclosed without authorization, could reasonably be expected to cause damage to the national security that the original classification authority is able to describe.

d. No other terms may be used to identify classified national security information. The terms “Top Secret,” “Secret,” and “Confidential” should not be used to identify nonclassified U.S. Postal Service information. Terms such as “For Official Use Only,” “Sensitive But Unclassified,” “Law Enforcement Sensitive” etc., should not be used to identify classified national security information.

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

1-2.2 Categories

Information is not considered for classification unless the information concerns one or more of the following items:

a. Military plans, weapons systems, or operations.

b. Foreign government information.

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

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

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

f. United States Government programs for safeguarding nuclear materials or facilities.

g. Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism.

h. Weapons of mass destruction.

1-3 Original Classification

1-3.1 Standards

Information is originally classified only if *all* of the following conditions are met:

a. An original classification authority is classifying the information.

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

> **Control.** The authority of the agency that originates classified information or its successor in function to regulate access to the information.

c. The information falls within one or more of the categories of information listed in EO 12958 as amended (also see 1-2.2, Categories).

d. The original classification authority determines the following:

(1) The unauthorized disclosure of the information that reasonably could be expected to result in damage to national security, which includes defense against transnational terrorism.

(2) The identification or description of the damage that disclosure could cause.

1-3.2 Duration of Classification

Generally, information is classified for prescribed periods of time. One of the following, as prescribed in Section 1.5(b) of EO 12958 as amended must be applied:

a. The date or event for declassification.

b. The date that is 10 years from the date of original classification.

c. The date that is up to 25 years from the date of original classification.

If the original classifying agency does not extend the classification date, the information becomes declassified. Classification extensions may not exceed 25 years from the date of original classification. Information can remain classified for more than 25 years in certain defined situations as described in 3.3 of EO 12958 as amended.

1-3.3 Identification and Markings

The following will appear on the face of or applied in an appropriate manner to originally classified information:

a. One of the three classification levels described in 1-2.1, Levels.

b. The identity by name or personal identifier and position of the original classification authority.

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

d. Declassification instructions, which should indicate a date or event for declassification.

> **Declassification.** The authorized change in the status of information from classified to unclassified information. Information that has been declassified without proper authority remains classified.

e. A concise reason for classification that, at a minimum, cites the applicable classification categories listed in 1-2.2, Categories.

f. Exemption categories used previous to September 22, 2003, may no longer be used.

g. Information that has been properly exempted from automatic declassification shall include the symbol “25X” on the “Declassify On” line. A brief reference of the exemption category is also entered. (See 3.3(b) of EO 12958 as amended for the exemption categories.)

1-3.4 Overall Marking

a. The highest level of classified information contained in a document shall determine the classification level of the document.

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

c. Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation “Unclassified” when

it is applicable or with the highest overall classification of the document.

d. Working papers are defined as documents or materials, regardless of the media, that are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information are dated when created, marked with the highest classification of any information contained in the papers, protected at that level, and if otherwise appropriate, destroyed when no longer needed.

1-3.5 Portion Markings

Portion markings (see Exhibit 1-3.5 a and b) are required by EO 12958 as amended because they place recipients on alert about the sensitivity of information. The first step in the marking process is to identify the classification level of each portion. A portion is ordinarily defined as a paragraph. Subjects and titles are also treated as portions. Only in this way can the overall classification level be determined. Portion marking consists of the following combinations of letters and parentheses:

a. ***(U)*** — Unclassified.

Exhibit 1-3.5a
Portion Markings Before Each Portion

SECRET

[Security marking for illustration purposes only]

UNITED STATES POSTAL INSPECTION SERVICE

Chief Postal Inspector
June 25, 2006

TO: Postmaster General
FROM: Chief Postal Inspector
SUBJECT: **(U)** Portion Markings of Classified Documents

1. **(U)** This is paragraph 1 and contains unclassified information. Therefore, this portion of the document will be marked with the designation “U” in parentheses.

2. **(S)** This is paragraph 2 and contains “Secret” information. Therefore, this portion of the document will be marked with the designation “S” in parentheses. Note that since this is the highest classification in the document, the entire document will be marked “SECRET.”

3. **(C)** This is paragraph 3 and contains “Confidential” information. Therefore, this portion of the document will be marked with the designation “C” in parentheses.

SECRET

[Security marking for illustration purposes only]

Exhibit 1-3.5b
Portion Markings After Each Portion

SECRET

[Security marking for illustration purposes only]

UNITED STATES POSTAL INSPECTION SERVICE

Chief Postal Inspector
June 25, 2006

TO: Postmaster General
FROM: Chief Postal Inspector
SUBJECT: Portion Markings of Classified Documents **(U)**

1. This is paragraph 1 and contains unclassified information. Therefore, this portion of the document will be marked with the designation "U" in parentheses. **(U)**

2. This is paragraph 2 and contains "Secret" information. Therefore, this portion of the document will be marked with the designation "S" in parentheses. Note that since this is the highest classification in the document, the entire document will be marked "SECRET." **(S)**

3. This is paragraph 3 and contains "Confidential" information. Therefore, this portion of the document will be marked with the designation "C" in parentheses. **(C)**

SECRET

[Security marking for illustration purposes only]

b. ***(C)*** — Confidential.
c. ***(S)*** — Secret.
d. ***(TS)*** — Top Secret.

1-4 Changes in Classification Status

1-4.1 Downgrading and Declassifying Information

The federal department or agency originating classified information may change the level of classification and safeguarding for information by performing the following:

a. ***Downgrading*** — From the originally specified level to a lower level.
b. ***Declassifying*** — From classified to unclassified.

Postal Service officials, employees, and contractors must not declassify or downgrade the classification of national security information unless directed to do so by the originating federal department or agency. See Chapter 2, Declassification and Downgrading, for more information.

1-4.2 Challenging a Classification Status

Postal Service officials, employees, and contractors who are authorized custodians of classified information and who, in good faith, believe that the classification status is improper are encouraged and expected to challenge the classification status.

To challenge a classification status:

a. Prepare a statement of your rationale for challenging the classification status and attach a photocopy of the document in question.

b. Forward your challenge to the Office of the Chief Postal Inspector, who will submit the challenge to the head of the originating agency for review and decision.

Be assured that you:

a. Will not be subject to retribution for bringing such actions.

b. Will be provided an opportunity for review by an impartial official or panel of the originating agency.

c. Will be advised of your right to appeal the originating agency's decision to the Interagency Security Classification Appeals Panel.

1-5 Derivative Classification

1-5.1 Authority

Designated Postal Service employees are authorized by the Chief Postal Inspector to incorporate, paraphrase, restate, or generate in new form information that is already classified by another federal agency.

The duplication or reproduction of existing classified information does not constitute derivative classification.

1-5.2 Maintaining Original Classification Requirements

To maintain the security of derivatively classified information:

a. Observe and respect original classification decisions.

b. Carry forward to any newly created documents the pertinent classification markings.

c. Stamp or mark the overall classification at the top and bottom of the front and back covers, title pages, and the first page of the new document. The overall classification level is the highest classification level of information contained in the document. Each interior page must be stamped or marked according to the highest classification level of its content, including unclassified, when appropriate. For example, if one page is TOP SECRET, the entire document is TOP SECRET.

1-5.3 Identifying Derivatively Classified Information

To mark the face page of a derivatively classified document (see Exhibit 1-5.3):

a. Create a "derivatively classified by" line — Give the name and title of the Postal Service official, employee, or contractor creating the derivative document.

Example:

Derivatively classified by: *R.A. Martin,*
United States Postal Service
Program Manager, Inspection Service
DMI-HS

b. Create a "derived from" line — Give the identity of the sources used as the basis for classification.

Exhibit 1-5.3
Derivatively Classifying Documents

SECRET

[Security marking for illustration purposes only]

UNITED STATES POSTAL INSPECTION SERVICE

Chief Postal Inspector
June 25, 2006

TO: Postmaster General
FROM: Chief Postal Inspector
SUBJECT: **(U)** Derivatively Classifying Documents

1. **(U)** This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

2. **(S)** This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses. Note that since this is the highest classification in the document, the entire document will be marked "SECRET."

3. **(C)** This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Derived from: Memorandum dated November 24, 2006
Subject: Intelligence Report
Department of Homeland Security

Declassify on:November 24, 2021 *[Declassification date is the declassification date cited in the source document]*

SECRET

[Security marking for illustration purposes only]

Examples:

Derived from:	*Memo, "Funding Problems" June 25, 2006 Office of Administration Department of Good Works*
Derived from:	*Classification Guide No. 1 Department of Good Works Dated June 25, 2006*
Derived from:	*Multiple Sources*

c. Create a "Reason" line — Give, if you judge it necessary, the reason for classification from the source document or classification guide. The reason for the original classification decision is not required to be transferred to the derivatively classified document.

d. Create a "Declassify on" line — Give the duration of classification carried forward from the "Declassify on" line of the source document, or the duration instruction from the classification guide. If the document is based on more than one source document or more than one element of a classification guide, the "Declassify on" line must reflect the longest duration of any of its sources.

e. When a document is classified derivatively from a source document that contains the declassification instruction, "Originating Agency's Determination Required" or "OADR," unless otherwise instructed by the original classifier, the derivative classifier must carry forward:

(1) The fact that the source document was marked with this instruction.

(2) The date of origin of the most recent source document or specific information, as appropriate to the circumstances.

Example:

Declassify on:	*Source document marked "OADR" Date of source June 25, 2006*

This marking will permit the determination of when the classified information is 25 years old and, if historically valuable, subject to automatic declassification according to EO 12958, as amended.

> **Automatic declassification.** The declassification of information based solely on the following: (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 EO 12958, as amended.

1-5.4 Marking Information From Multiple Sources

To mark a derivatively classified document based on multiple sources (see Exhibit 1-5.4):

a. Mark the derivative document with the highest classification level of information found in any portion of the document.

b. If the document contains more than one page:

(1) Place the overall marking on the top and bottom of the outside of the front cover, the title page, the first page, and the outside of the back cover.

(2) Mark other internal pages either with the overall classification or with a marking indicating the highest classification level of information contained on that page.

c. Enter the standard notation "Multiple Sources" on the "Derived from" line to indicate that more than one source was used. The author must maintain a list identifying all the classified sources with the file or record a photocopy of the derivative document and, if practicable, include the list with all copies of the derivative document.

d. Mark the "Declassify on" line with the declassification instructions from the source document that requires the longest period of classification.

Exhibit 1-5.4
Derived From Multiple Sources

SECRET

[Security marking for illustration purposes only]

UNITED STATES POSTAL INSPECTION SERVICE

Chief Postal Inspector
June 25, 2006

TO: Postmaster General
FROM: Chief Postal Inspector
SUBJECT: **(U)** Derivatively Classifying Documents

1. **(U)** This is paragraph 1 and contains unclassified information derived from Document #1. Therefore, this portion will be marked with the designation "U" in parentheses.

2. **(S)** This is paragraph 2 and contains "Secret" information derived from Document #2. Therefore, this portion will be marked with the designation "S" in parentheses. Note that since this is the highest classification in the document, the entire document will be marked "SECRET."

3. **(C)** This is paragraph 3 and contains "Confidential" information derived from Document #3. Therefore, this portion will be marked with the designation "C" in parentheses.

Derived from: Multiple Sources
Declassify on:November 24, 2014 *[Declassification date is the date that requires the longest period of classification cited in the source documents.]*

SECRET

[Security marking for illustration purposes only]

1-6 Transmittal Documents

A transmittal document is used to transmit classified information. The transmittal document may or may not contain classified information.

To develop an unclassified transmittal document:

a. On the top and bottom of the transmittal document, mark the highest classification of the information being transmitted.

b. Mark the bottom of the transmittal document with an appropriate instruction, such as *Unclassified, when separated from classified enclosures*.

To develop a derivatively classified transmittal document (see Exhibit 1-6), portion mark it as required for all other classified information (see 1-3.5, Portion Markings), except:

a. Conspicuously mark the top and bottom of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures.

b. Mark the transmittal document with an appropriate instruction, such as *Downgrade to Confidential, when separated from Secret enclosures*, indicating its overall classification level when separated from its enclosures.

Exhibit 1-6
Transmittal Document

SECRET

[Security marking for illustration purposes only]

UNITED STATES POSTAL INSPECTION SERVICE

Chief Postal Inspector
June 25, 2006
TO: Postmaster General
FROM: Chief Postal Inspector
SUBJECT: **(U)** Transmittal of Classified Documents

1. **(U)** This exhibit illustrates the requirement for preparing a transmittal document used to reflect or transmit classified information. The highest classification of information in the enclosures is shown at the top and bottom of the document. The enclosures are listed, showing the number of copies and level of classification of each. If the transmittal document does not contain any classified information, it should contain an instruction indicating it is unclassified when separated from the enclosures.

2. **(U)** If the transmittal document does contain classified information, it should be marked with an appropriate instruction indicating its overall classification level when separated from its enclosures, e.g., "Downgrade to CONFIDENTIAL when separated from SECRET enclosures."

Enclosures:

a. Draft M-2 Handbook (U), 3 copies
b. Engineering Drawings (S), 2 copies
c. Draft International Agreement (C), 1 photocopy

[Unclassified When Classified Enclosure Is Detached]

SECRET

[Security marking for illustration purposes only]

2 Declassification and Downgrading

2-1 Declassification

2-1.1 Authority

Executive Order (EO) 12598, as amended, *Classified National Security Information,* directs departments and agencies to declassify information as soon as the information no longer meets the standards for classification under the order. Declassification normally rests with the originating agency; however, the Postal Service is required to work with the originally classifying agency in the declassification process. Foreign government information is declassified by the receiving agency in consultation with the U.S. Department of State.

Information that continues to meet the classification standards under the order will continue to be protected. In some exceptional situations, the need to protect such information may be outweighed by the public interest in disclosure of the information and should be declassified. In those situations, the question must be referred to the head or designated senior official of the classifying agency for determination.

Declassification decisions about information formerly classified by the Post Office Department and held by the U.S. Postal Service as the successor agency will be made by the Postal Service. Since the Post Office Department ceased in 1970, declassification of any remaining information must be coordinated with other agencies having an interest in the subject matter of the records, as must any records the Postal Service holds that were classified by an agency that has ceased to exist. Where the functions of an agency have been transferred to a successor agency, the successor agency will have the declassification authority.

2-1.2 Automatic Declassification

As of December 31, 2006, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under Title 44, *United States Code,* are automatically declassified whether or not the records have been reviewed. After that, all classified records will be automatically declassified on December 31 of the year that is 25 years from the date of original classification. Heads of agencies with original classification authority may exempt certain information with the approval of the President. Details regarding information that may be exempted and the process for exemption approval may be found in Section 3.3 of EO 12958, as amended.

2-1.3 Systematic Declassification Review

a. At the beginning of each calendar year, all classified information that is held by the Postal Service and that will have been classified for 25 years by the end of the year must be reviewed for declassification. This review can be performed during the annual inventory and must be completed by January 31.

b. Classified information that meets the criteria in item a above must be reviewed in concert with the original classifying agency in order to determine if the information warrants retention of the classification. The originating agency must make this determination and follow the exemption process under EO 12958, as amended, if the classification is to be retained.

c. By May 31, all Postal Service holders of classified information must advise the Inspector in Charge, DMI-HS, of the status of local declassification reviews. The following information must be reported:

- Number of documents eligible for declassification.
- Number of documents to be declassified by originating agency.
- Number of documents to be exempted or in exemption process.
- Estimated number of documents, if any, not yet reviewed for declassification decision.

d. By August 31, a final report on the status of all classified documents held locally by the Postal Service for which automatic declassification is required under EO 12958, as amended, must be submitted to the Inspector in Charge, DMI-HS.

e. Questions or assistance about declassification may be referred to the Inspector in Charge, DMI-HS.

2-1.4 Mandatory Declassification Review

a. Requests for information under the Freedom of Information Act, the Privacy Act of 1974, or for a declassification review must be forwarded to the agency originally classifying the document or information in question. Since the Postal Service does not have original classification authority, it cannot conduct a declassification review of information originally classified by another agency.

b. Requests for review must be submitted to the Chief Postal Inspector, U.S. Postal Inspection Service. Such requests will be processed in accordance with EO 12598 (Sections 3.5 and 3.6) and Information Security Oversight Office (ISOO) Implementing Directive #1 (Section 2001.33).

c. If the request for review concerns a derivatively classified document created by the Postal Service, the Postal Service must contact the agency(ies) of the source document(s) for assistance and declassification review.

d. If the fact that a record's existence or nonexistence is itself classified, the Postal Service must refuse to confirm or deny the existence or nonexistence of the requested record.

e. The Postal Service must consult with the originating agency before advising the requester of a referral. The requester will not be advised of the referral if the originating agency determines the association is itself classified. Further, if the originating agency determines in writing that a response under item c above is required, the Postal Service will respond in accordance with item c above.

2-1.5 Declassification Markings

The following markings shall be applied to records or copies of records regardless of media:

a. The word, "Declassified."

b. The name or personal identifier and position title of the declassification authority or declassification guide.

c. The date of declassification.

d. The overall classification markings that appear on the cover page or first page shall be lined with an "X" or straight line. An example might appear as:

~~SECRET~~

Declassified by R.A. Martin, Program Manager, DMI-HS, June 25, 2006

2-1.6 Records Originated by Other Agencies

When the Postal Service uncovers classified records originated by another agency that appear to meet the criteria for the application of the automatic declassification provisions of EO 12598, the Postal Service will alert the originating agency and seek instruction.

2-2 Downgrading

2-2.1 Postal Service Employees Not Authorized

Postal Service employees are not authorized to downgrade the classification level of a document. Such action can only be authorized by the originally classifying agency.

2-2.2 Derivative Documents

Care must be taken when applying an authorized downgrade to derivately classified documents, particularly those derived from multiple sources. Although a portion of the document may have been downgraded, the entire document must be reviewed to determine that it is classified at the same level as the portion with the highest level of classification.

This page intentionally left blank

3 Access

3-1 Authorized Access

Access to classified information is limited to Postal Service officials, employees, and contractors who meet all of the following conditions:

a. Have an official "need to know" about classified information in the performance of their official duties.

> **Official need to know.** A prospective recipient's need for access to specific classified information in order to perform or assist in a lawful and authorized government function as determined by an authorized custodian of that classified information.

b. Have the appropriate clearance for access to classified information.

c. Have received an initial security briefing from the Inspection Service, DMI-HS, that provides education on postal regulations, policies, and procedures and a basic understanding of the Classified National Security Information Program. This includes classification, declassification, access, accountability, safeguarding, transmission, disposition, loss or compromise, program review and reports, and disclosure of classified information.

d. Have executed Standard Form (SF) 312, *Classified Information Nondisclosure Agreement,* before they are provided access to classified information.

If you are authorized to receive classified information, you are responsible for ensuring that the information is disclosed only to individuals who meet criteria in items a through d above.

To determine whether a Postal Service official, employee, or contractor has an appropriate level sensitive security clearance, direct inquiries to the Inspector in Charge, Security, Postal Service Headquarters.

To acquire information on obtaining a sensitive clearance, see 272 of the *Administrative Support Manual.*

3-2 Security Clearance Certification

The Inspector in Charge, Security furnishes written verification and certification of security clearances for Postal Service officials, employees, or contractors to federal departments and agencies. The certification is furnished to allow those requiring clearance to attend meetings, conferences, seminars, or other activities where classified information may be presented, discussed, or released.

Postal Service officials, employees, or contractors requiring certification of their security clearance must provide the following information 48 hours in advance of the event to the Inspector in Charge, Security:

a. Name and title of Postal Service official, employee, or contractor.

b. Date and place of birth.

c. Social security number.

d. Name and address of requesting department or agency.

e. Department or agency point of contact.

f. Department or agency telephone number.

g. Department or agency fax number.

h. Date of event (if applicable).

i. Reason for clearance certification (i.e., to attend classified meeting).

3-3 Nondisclosure Agreement

A Postal Service official, employee, or contractor who occupies a position with official duties that require access to classified information is required to complete and sign SF 312.

To have authorized access to classified information, complete the following actions:

a. Obtain SF 312 from the General Services Administration (GSA), the GSA forms Web site, or from the Inspection Service DMI-HS at Postal Service Headquarters.

b. Send the signed and completed SF 312 to:

INSPECTOR IN CHARGE, INSPECTION SERVICE
DMI-HS
US POSTAL SERVICE
475 L'ENFANT PLAZA SW RM 3301
WASHINGTON DC 20260-3301

c. Upon its acceptance, the SF 312 is retained by the Inspection Service DMI-HS for 50 years according to Executive Order 12958, *Classified National Security Information,* as amended.

Anyone who refuses to sign a nondisclosure agreement must be denied access to classified information.

3-4 Security Education and Training

Postal Service officials, employees, and contractors who process or handle classified information or who are authorized to create derivatively classified documents must receive national security education and training to ensure a satisfactory knowledge and understanding of original classification, derivative classification, safeguarding classified information, and other program policies and procedures.

The Chief Postal Inspector establishes and maintains a security education and training program in accordance with Subpart F of the Information Security Oversight Office (ISOO) Directive #1, that provides for initial and refresher training for all Postal Service officials, employees, and contractors who are authorized access to classified information. Contact the Inspector in Charge, DMI-HS, to arrange for required training.

3-5 Observing Restrictions on Use of Accessed Information

To maintain security of classified information, do the following:

a. Do not disseminate or disclose classified information outside the Postal Service without the consent of the originating agency or its successor function.

b. If an employee needs to remove classified information from a designated work area for work elsewhere, the employee must:

   (1) Be authorized to do so by the Chief Postal Inspector. *All such requests and authorizations must be documented in writing.*

   (2) Prepare the classified materials for transmission (see Chapter 6, Transmission). A locked briefcase may serve as the outer wrapper.

   (3) Ensure that the information remains under your constant and continuous protection until secured in a GSA-approved security container.

c. When you leave Postal Service employment, do not remove classified information from Postal Service custody.

> **In Postal Service custody.** Transmitted to and held by the Postal Service for use by Postal Service officials, employees, and contractors. This does not apply to classified information transmitted by other federal agencies through the mail.

d. If you use automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information, you must ensure that such systems have controls that:

(1) Prevent access by unauthorized persons.

(2) Ensure the integrity of the information.

(3) Document each access to the information.

3-6 Termination Briefings

Termination briefings are required for Postal Service officials, employees, and contractors who no longer require access to classified information in the performance of their official duties or who are leaving Postal Service employment. A termination briefing serves to remind these individuals that (1) their responsibility to protect classified information, including that stored in their memory, does not end with their departure from government service, and (2) a person who no longer has a security clearance is still subject to criminal and civil liability for the unauthorized disclosure of classified information learned while he or she was cleared.

> **Unauthorized disclosure.** A communication or physical transfer of classified national security information to an unauthorized recipient.

A termination briefing can be arranged through the Inspector in Charge, DMI-HS.

3-7 Emergency Authority

The Chief Postal Inspector may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations

In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.

b. Limit the number of individuals who receive it.

c. Transmit the classified information via approved federal government channels by the most secure and expeditious method to include those required in Chapter 6, Transmission, or other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified and how it should be safeguarded. Physical custody of classified information must remain with an authorized federal government entity in all but the most extraordinary circumstances.

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement.

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

(1) A description of the disclosed information.

(2) To whom the information was disclosed.

(3) How the information was disclosed and transmitted.

(4) Reason for the emergency release.

(5) How the information is being safeguarded.

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

This page intentionally left blank

4 Accountability

4-1 Top Secret Information

The Inspector in Charge, DMI-HS, must be contacted immediately upon receipt of Top Secret information. The Inspector in Charge, DMI-HS, is designated as the Top Secret Control Officer (TSCO) of the Postal Service. The TSCO will ensure that:

a. The information is chronologically logged in a database system established to record the receipt, interoffice routing, transmission, handling, and final disposition by the Postal Service.

b. The information is delivered to or in the custody of the official, employee, or contractor having authorized access.

c. PS Form 1861, *Classified Document Accountability Record* (see Exhibit 4-1), is prepared and maintained.

4-2 Completing the Accountability Record

PS Form 1861 is an accountable, sequentially numbered control form that is disseminated by the Inspector in Charge, DMI-HS. PS Form 1861 must be completed for each classified document received. The Postal Service official, employee, or contractor with authorized access who first receives a classified document must complete PS Form 1861.

To establish the accountability record for a classified document:

a. Immediately complete the receipt enclosed by the sending or originating agency and return it to the sender to confirm delivery.

b. Complete and distribute PS Form 1861 whether the document is picked up or hand delivered (Top Secret) or received directly through the mail (Secret or Confidential). Distribute the colored pages of a completed PS Form 1861 as follows:

   (1) *White* — Attach to the original classified document. When the classified information is destroyed or returned to the originating agency, forward the original annotated PS Form 1861 to the Inspector in Charge, DMI-HS.

Exhibit 4-1
PS Form 1861, Classified Document Accountability Record

United States Postal Service
Classified Document Accountability Record

USPS Control No.

Incoming Control/Registered Mail No.	Classification	Originating Agency

Received By

Name *(Print or type)*			
Title	Organization		
Signature	Date Received	Time Received	No. of Copies Received

Description of Documents

Unclassified Subject or Title	Document Type *(Letter, memo, report, book, other)*	No. of Pages	Document Date	Copy Nos.

Record of Derivative Classification

Were Any Documents Derivatively Classified? ☐ Yes ☐ No	If Yes, How Many?	USPS Control No. on New Form 1861
List By Type *(e.g., transmittal letter)*		Date Derivatively Classified

Reproduction Record

No. of Copies	Date

Copies Made By

Name *(Print or type)*	Signature

Copies Authorized By

Name *(Print or type)*	Telephone No. *(Include area code)*
Title	Agency

Routing

Routed To:	Copy No.	Date	Registered Mail No.	Printed Name	Signature
1.					
2.					
3.					

Storage Record

Office Responsible for Storage	Date Transferred to Federal Records Center

Transfer Authorized By

Name *(Print or type)*	Title
Signature	

Disposition Record

Original (and Copies) Were: *(Check one)* ☐ Returned to Originating Agency ☐ Destroyed	Date of Disposition
Disposed By Name *(Print or type)*	Signature of Disposing Individual
Witness Name *(Print or type)*	Signature of Witness

PS Form **1861**, July 1995 **Original—File With Document**

(2) *Yellow* — File by Postal Service control number in the preparing office. Use to reconcile annual inventory (see 35, Annual Inventory).

(3) *Green* — Forward to the Inspector in Charge, DMI-HS.

(4) *Blue* — File this "extra" copy if needed or destroy it.

To establish the accountability record for a derivatively classified document:

a. Complete and attach a *new* PS Form 1861 to the derivative document.

b. Annotate the PS Form 1861 of the source documents in the section titled "Record of Derivative Classification."

c. Distribute copies as described above.

4-3 Receipt for Classified Information

PS Form 1266, *Receipt for Classified Communication*, (see Exhibit 4-3*)* must be completed when returning classified information to the originating agency or when routing classified information internally within the Postal Service. To return classified information to the originating agency or to route internally, the sender should do the following:

a. Complete PS Form 1266.

b. Attach the original and copy 1 to the document to be routed; retain copy 2 until copy 1 is returned by the addressee (see 6-3, Preparing Envelopes or Containers, for transmitting classified information).

c. Complete and sign the *Routing* section of the controlling PS Form 1861.

To receipt for classified information routed internally, the addressee should do the following:

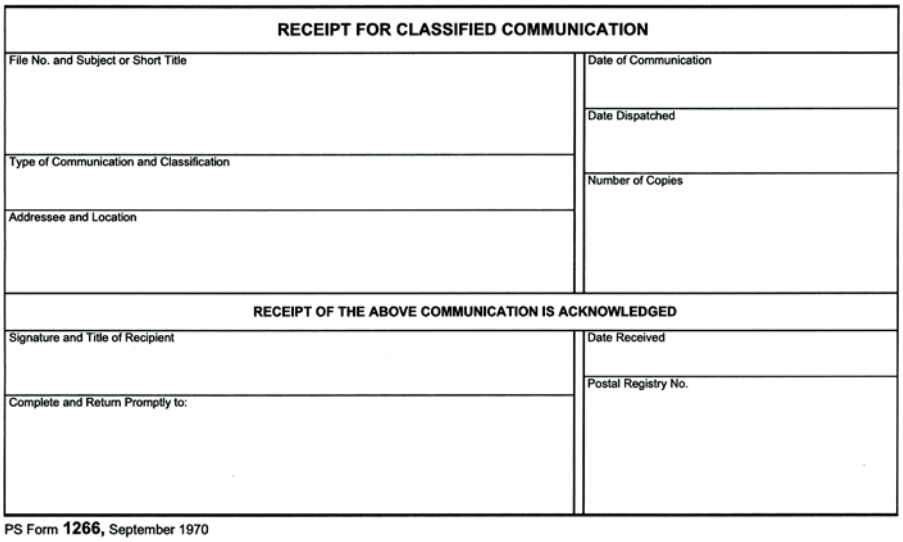
a. Complete and sign *Recipient Information* on PS Form 1266.

b. Return copy 1 to the sender within 10 days of receipt.

c. Attach original to the inside front cover and maintain with the classified document until the classified information is destroyed or returned to the originating agency.

To trace a classified document for which no PS Form 1266 has arrived within 10 days of transmission, the sender should do the following:

Exhibit 4-3
PS Form 1266, Receipt for Classified Communication



RECEIPT FOR CLASSIFIED COMMUNICATION

File No. and Subject or Short Title	Date of Communication
	Date Dispatched
Type of Communication and Classification	Number of Copies
Addressee and Location	

RECEIPT OF THE ABOVE COMMUNICATION IS ACKNOWLEDGED

Signature and Title of Recipient	Date Received
	Postal Registry No.
Complete and Return Promptly to:	

PS Form **1266,** September 1970

a. Telephone the addressee or forward a photocopy of the completed PS Form 1266, marking at the top: *Tracer – Addressee: Annotate Date Received and Return to Sender.* Include the registered or certified number if the original material was mailed.

b. Immediately notify the Inspector in Charge, DMI-HS if the addressee confirms that the classified information was never received.

4-4 Reproducing Classified Information

Reproduced copies of classified information are subject to the same accountability and controls as the original information. The following constraints apply:

a. Classified information may be reproduced to the extent necessary to satisfy operational needs as long as the reproduction process complies with any restrictions specified by the originating agency or any higher authority.

b. Only Postal Service officials, employees, and contractors who have the appropriate security clearance for handling classified information are authorized to reproduce it.

c. Only the original may be reproduced.

To account for a reproduced classified document, annotate the controlling PS Form 1861, “Reproduction Record” section, to indicate the number of copies, date, who made the copies, and if they required an authorization from the originating agency.

4-4 Annual Inventory

Classified information in Postal Service custody must be inventoried at least annually, with the objective of reducing holdings to a minimum. Custodians, individuals who possess or otherwise are charged with the responsibility for

safeguarding or accounting for classified information, must perform the annual review by January 31 of each year.

Classified information no longer needed for operational purposes may be destroyed or returned to the originating agency, if requested (see Chapter 7, *Disposal and Destruction)*. The inventory must include the following:

a. Visual verification of each document.

b. Reconciliation of the documents on hand to the documents included in the accountability records (see PS Form 1861 yellow copies).

Reporting discrepancies to the Inspector in Charge, DMI-HS.

This page intentionally left blank

5 Safeguarding

5-1 Custodian Responsibilities

Any person with custody of classified information is responsible for:

a. Protecting it from persons not authorized access to it.

b. Securing it in approved storage equipment or facilities whenever it is not under the direct control of an authorized person.

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

NATO Classified Information shall be safeguarded in compliance with U.S. Security Authority for NATO Instructions I-69 and I-70.

5-2 Protecting Information From Inadvertent Disclosure

To protect paper documents:

a. Use a protective document cover to protect classified information from inadvertent disclosure and to alert observers that such information is attached.

b. Use the following protective document covers to protect classified information in Postal Service custody:

(1) Standard Form (SF) 703, *Top Secret Cover Sheet* (see Exhibit 5-2a).

(2) SF 704, *Secret Cover Sheet* (see Exhibit 5-2b).

(3) SF 705, Confidential Cover Sheet (see Exhibit 5-2c).

Do not use plastic executive correspondence covers, which are subject to image transfer, to protect classified documents.

c. Keep the document cover attached to the top of the classified information from its receipt until its destruction.

Depending upon its condition, a document cover may then be reused.

Exhibit 5-2a
Standard Form 703, Top Secret Cover Sheet

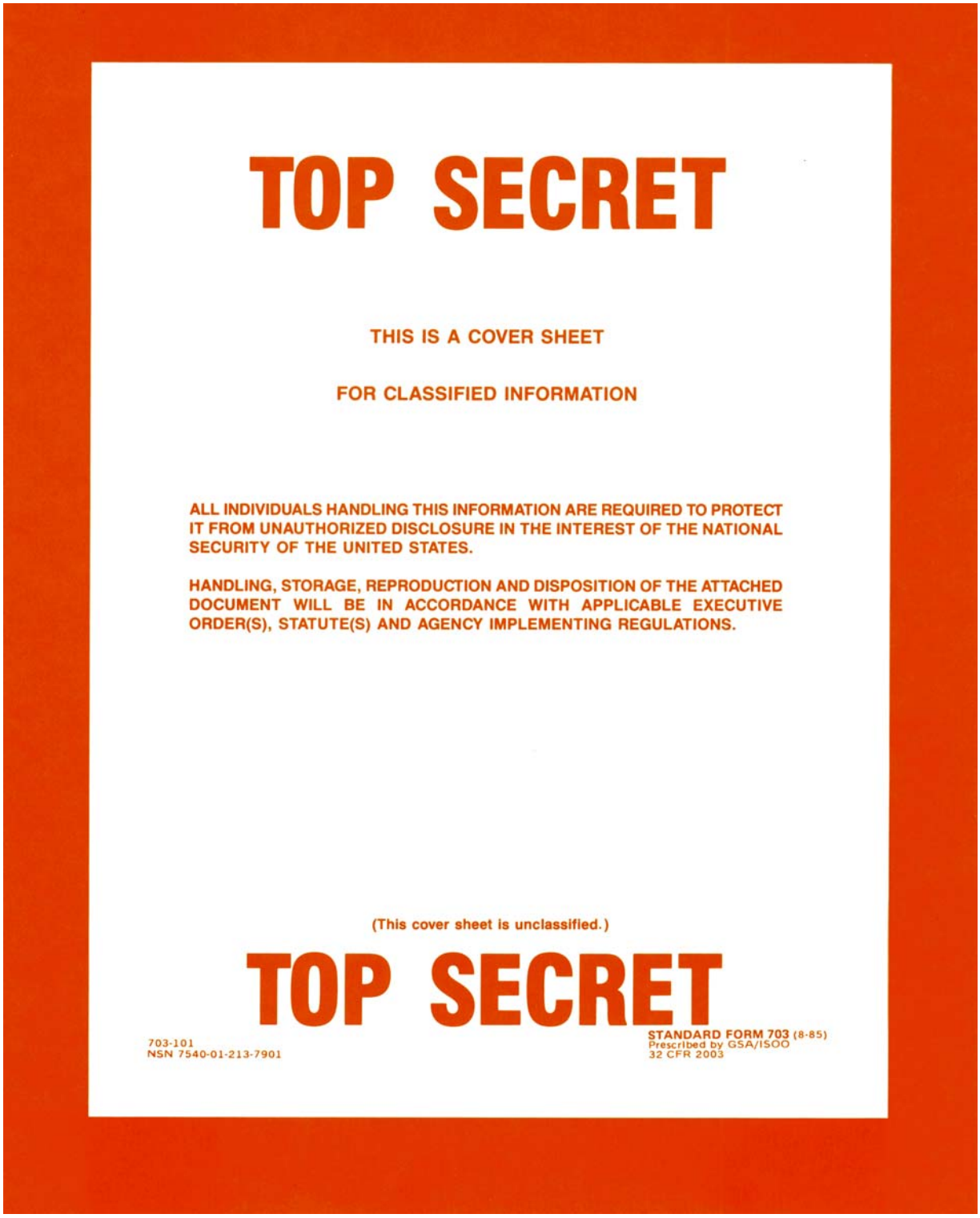


Exhibit 5-2b
Standard Form 704, Secret Cover Sheet

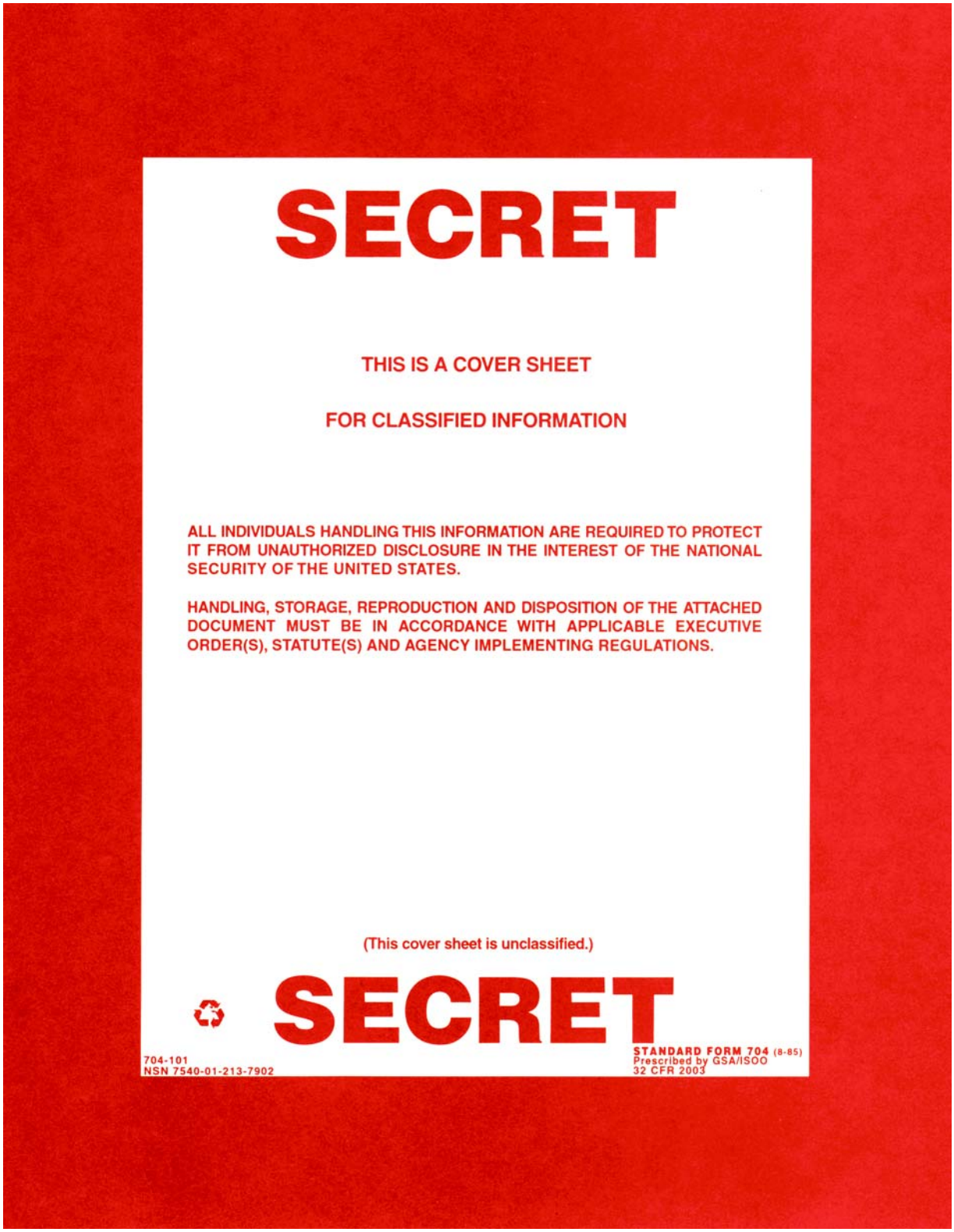
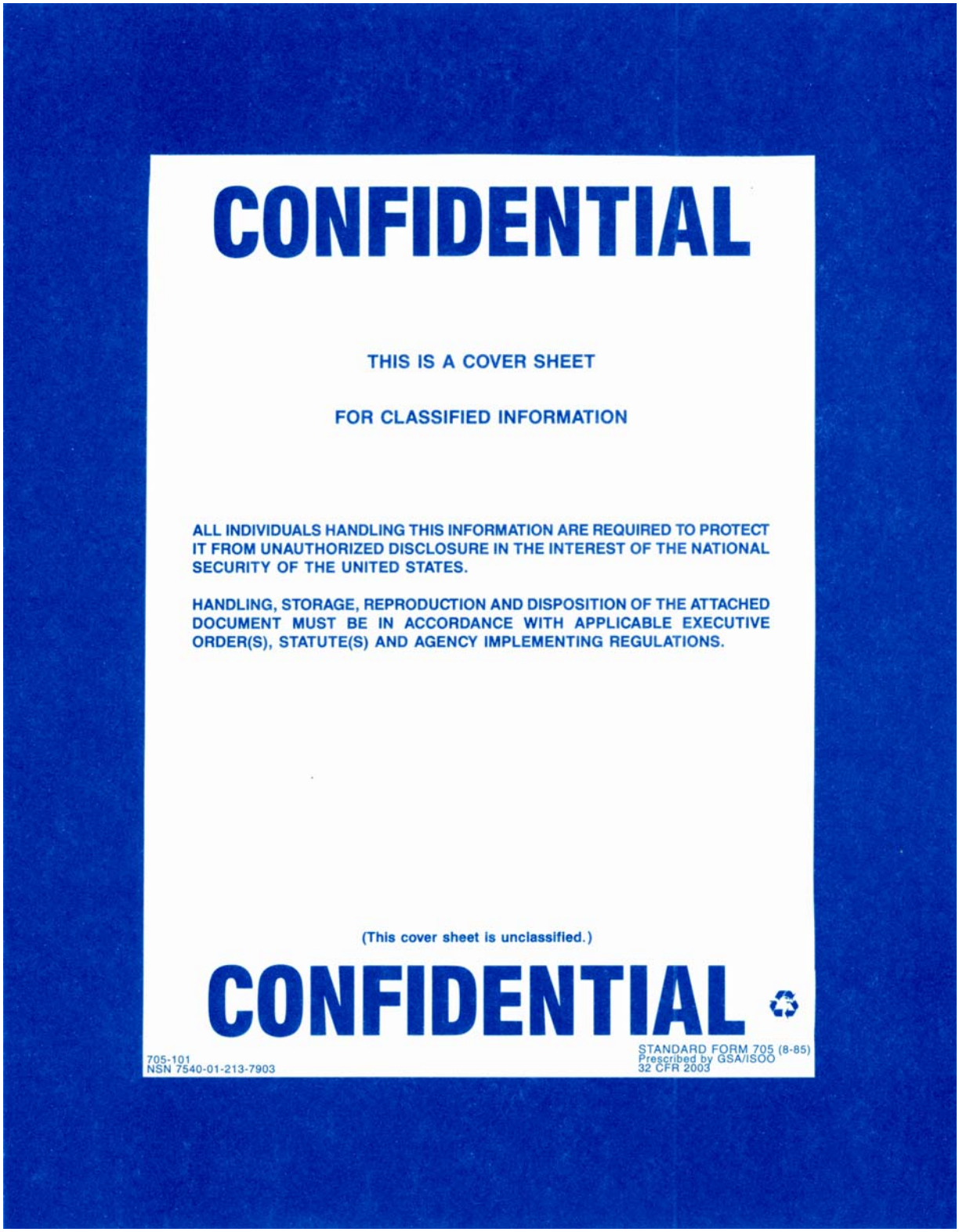


Exhibit 5-2c
Standard Form 705, Confidential Cover Sheet



To protect automatic data processing materials:

a. Use protective media labels to alert observers that classified information is contained in computer hardware and software and other media such as disks, charts, maps, drawings, CDs, tapes, photographs, and recordings.

b. Use the following protective media labels to identify electronic media containing classified information in Postal Service custody:

(1) SF 706, *Top Secret Label* (see Exhibit 5-2d).

(2) SF 707, *Secret Label* (see Exhibit 5-2e).

(3) SF 708, *Confidential Label* (see Exhibit 5-2f).

c. Affix these labels to the media in such a way that they will not adversely affect operation of the equipment in which the media are used. *Once the label has been applied, it cannot be removed.*

Exhibit 5-2d
Standard Form 706, Top Secret Label

Exhibit 5-2e
Standard Form 707, Secret Label

Exhibit 5-2f
Standard Form 708, Confidential Label

5-3 Physical Storage and Protection

Classified information, regardless of the media on which it is stored, must be stored and protected as described herein.

To store and protect Top Secret information, store the information using *one* of the following methods in items a or b as follows:

a. In a GSA-approved security container with *one* of the following supplemental controls:

(1) Continuous protection of the location housing the security container by a cleared guard or duty person.

(2) Inspection by a cleared guard or duty person every 2 hours.

(3) An approved intrusion-detection system (IDS) with personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(4) Security-in-depth, when the GSA-approved container is equipped with a lock that meets Federal Specification FF-L-2740. Security-in-depth involves additional safeguards to mitigate the vulnerability of alarmed, open-storage areas, and security-storage cabinets during nonwork hours. Examples include, but are not limited to:

- Perimeter fences.
- Employee and visitor access controls.
- IDSs.
- Guard patrols conducting random surveillance throughout the facility during nonwork hours.
- Closed-circuit video monitoring.

Security-in-depth. Layered and complementary security controls in a facility sufficient to deter and detect unauthorized entry and movement within the facility or other safeguards that mitigate the vulnerability of nonalarmed open storage areas and security storage cabinets during nonworking hours.

b. In either one of the following:

(1) In an authorized, open-storage area constructed according to requirements specified in Exhibit 5-3, Construction Standards for Approved Open-Storage Areas, which is equipped with an approved IDS with the

Exhibit 5-3
Construction Standards for Approved Open Storage Areas

The following construction standards for walls, floors, doors, vents, ducts, windows and other features are required to certify an area as an approved open storage area.

General Construction

a. The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other.

b. All construction must be done in a manner to provide visual evidence of unauthorized penetration.

Doors

a. Doors are to be constructed of wood, metal, or other solid material. Entrance doors are to be secured with a built-in, GSA-approved, three-position combination lock.

b. When special circumstances exist, the agency head may authorize other GSA- or military specification-approved locks on entrance doors for secret and confidential storage.

c. Other doors are to be secured from the inside with panic hardware, dead bolt, or rigid wood or metal bar extending across the width of the door or by other means approved by the agency head.

Vents, Ducts, and Miscellaneous Openings

All vents, ducts, and similar openings in excess of 96 square inches (and more than 6 inches in its smallest dimension) that enter or pass through a closed area are to be protected with either bars, expanded metal grills, commercial metal sound baffles, or an intrusion detection system.

Windows

a. All windows that might reasonably afford visual observation of classified activities within the facility are to be made opaque or equipped with blinds, drapes, or other coverings.

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

c. Approved open-storage areas located within a controlled compound or equivalent may obviate forced entry protection if windows are made inoperable by permanently sealing them or by equipping them with an inside locking mechanism and installing IDS (either independently or by the motion detection sensors within the area).

d. personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) An approved IDS-equipped vault with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

To store and protect Secret information, use one of the following methods:

a. In the same manner as prescribed for Top Secret information.

b. In a GSA-approved security container or vault *without* supplemental controls.

c. Until October 1, 2012, in a non-GSA-approved container having a built-in combination lock or in a non-GSA-approved container secured with a rigid metal lockbar and an agency head approved padlock.

To store and protect Confidential information, store in the same manner as prescribed for Top Secret or Secret information, except that supplemental controls are not required.

To observe storage restrictions:

a. *Do not* store classified materials with weapons, drugs, or valuables.

b. *Do not* store classified materials with unclassified materials unless access is limited to persons with an appropriate security clearance.

5-4 Security Container Combination Requirements

5-4.1 Changing Combinations

Combinations to security containers must be changed only by individuals designated that responsibility and having a favorable determination of eligibility for access to classified information and authorized access to the level of information protected unless other sufficient controls exist to prevent access to the lock or knowledge of the combination.

To maintain combination security:

a. Change a combination:

- When the combination is placed in use.
- Whenever an individual knowing the combination no longer requires access.
- When the combination has been subject to possible compromise.

When the combination is taken out of service.

b. When security equipment is taken out of service, it must be inspected to ensure no classified information remains. Reset built-in combination locks to the standard combination 50-25-50. Reset combination padlocks to the standard combination 10-20-30.

5-4.2 Maintaining Combination Records

A record must be maintained by classified custodians for each vault, secure room, or container used to store classified information, showing the location of the container and information about the individuals having knowledge of the combination.

To record information for a vault, secure room, or container:

a. Use Standard Form (SF) 700, *Security Container Information*, to record the names, home addresses, and home telephone numbers of individuals having knowledge of the combination.

b. Assign to the combination a security classification equal to the highest category of the classified information authorized to be stored therein. Mark this classification clearly on the SF 700.

c. Store the SF 700, observing the physical protection requirements appropriate to the classification.

d. Provide duplicates as follows for storage and safeguarding:

(1) Headquarters records are provided by to the Inspector in Charge, DMI-HS.

(2) Inspection Service field division records are provided to the Inspector in Charge.

(3) Postal Service Area office records are provided to the Vice President of Area Operations.

5-4.3 Key-Operated Locks

When special circumstances exist, the Chief Postal Inspector may approve the use of key-operated locks for the storage of Secret and Confidential Information. Whenever such locks are used, administrative procedures for the control and accounting of keys and locks shall be established.

5-5 Security Forms

The Postal Service Classified National Security Information Program has used Standard Forms since 1986. Standard Forms support the governmentwide security program for classified information, are available from the General Services Administration (GSA), and can be ordered through the Postal Service Material Distribution Center.

5-5.1 Standard Form 700, Security Container Information

The SF 700 must be used to maintain a record for each vault, secure room, or container used for storing classified information.

Description. SF 700 shows the location of the container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the security container to which the form pertains is found open and unattended. The form also includes a current record of the security container's combination and provides the envelope to be used to forward this information to the Chief Postal Inspector.

Postal Use. SF 700 must be maintained for all security containers.

A new SF 700 must be completed each time the combination to the security container is changed.

Classification. Parts 2 and 2A of each completed copy of Standard Form 700 must be classified at the highest classification level of the information authorized for storage in the security container.

Availability. The GSA National Stock Number (NSN) is 7540-01-214-5372.

5-5.2 Standard Form 701, Activity Security Checklist

SF 701, *Activity Security Checklist,* must be used by certain postal facilities designated by the Inspector in Charge, DMI-HS.

Description. SF 701 provides a systematic means to make a thorough, end-of-workday security inspection for a particular work area. It is used to document employee accountability in the event that irregularities are discovered.

Postal Use. SF 701 must be used in all situations that call for the use of an activity security checklist as specified by the Inspector in Charge, DMI-HS.

Availability. The GSA NSN is 7540-01-213-7899.

5-5.3 Standard Form 702, Security Container Check Sheet

SF 702, *Security Container Check Sheet,* is used with SF 701 above as part of the end-of-workday security check system for securing all vaults, secure rooms, and containers used for the storage of classified material.

Description. SF 702 provides a record of the names, dates, and times that persons have opened, closed, or checked a particular container that holds classified information.

Postal Use. SF 702 must be used in all situations that call for a security container check sheet as specified by the Inspector in Charge, DMI-HS.

Availability. The GSA NSN is 7540-01-213-7900.

6 Transmission

6-1 Secure Transmission

Classified information must be transmitted and received in a manner that ensures the following:

a. The information is handled only by authorized individuals.

b. Evidence of tampering can be detected and inadvertent access can be precluded.

c. Delivery to the intended recipient is timely.

6-2 Transmission Methods

6-2.1 Within the United States, Territories, or Possessions

Top Secret information must be transmitted by any one of the following:

a. An authorized Postal Service courier with a Top Secret security clearance.

b. The Defense Courier Service (DCS).

c. An authorized government agency courier service.

d. Electronic means using approved communications systems.

Under no circumstances will Top Secret information be transmitted via the mail.

Secret information must be transmitted by any one of the following:

a. Any methods established for Top Secret information.

b. Postal Service Express Mail® (the Waiver of Signature and Indemnity block must not be completed) or Registered Mail™.

c. Cleared commercial carriers or commercial messenger services.

The use of street-side mail collection boxes is prohibited.

Confidential information must be transmitted by any one of the following means:

a. Any methods established for Secret information.

b. Postal Service Certified Mail™.

c. Postal Service First-Class Mail® provided that the following two conditions are met:

(1) The recipient is located in a U.S. Government facility and approves its use.

(2) The envelope or outer wrapper is marked to indicate that the document is not to be forwarded but is to be returned to the sender if the intended recipient is not at the specified address.

The use of street-side mail collection boxes is prohibited.

6-2.2 Outside the United States

The transmission of classified information to a U.S. Government facility located outside the United States, its territories, or possessions must be by methods specified for Top Secret information or by methods outlined by the U.S. Department of State Courier System.

Postal Service Registered Mail through military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control or pass through a foreign postal system.

6-2.3 Internal Routing

Classified information must be hand delivered by an authorized individual within a Postal Service facility. Internal mail or distribution services must not be used for this purpose.

6-3 Preparing Envelopes or Containers

To transmit securely:

a. Complete PS Form 1266, *Receipt for Classified Communication* (see 4-3).

b. Enclose classified information in two opaque, sealed envelopes or similar wrappings that provide reasonable evidence of tampering and that conceal the contents (see also 4-3 and Exhibit 4-3).

c. Mark the inside wrapper:

(1) Clearly identifying your work address and that of the intended recipient. Identify intended recipients by name only as part of an attention line.

(2) Showing the highest classification level of the contents and any appropriate warning notices.

d. Attach PS Form 1266 to the inner envelope.

e. Address the *outer* wrapper the same as the inside wrapper, but do not include markings to indicate that the contents are classified.

When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer wrapper.

6-4 Using Couriers

6-4.1 Defense Courier Service

The DCS provides courier service to the Department of Defense and other U.S. government agencies, including the Postal Service. DCS provides secure transportation and delivery of national security material requiring handling by a courier.

To use a DCS courier, make arrangements through the Inspection Service DMI-HS, Postal Service Headquarters.

6-4.2 Postal Service Couriers

A list of authorized Postal Service couriers is maintained by the Inspector in Charge, DMI-HS. Proposed additions and deletions to this list must be submitted to the manager. The list is updated after clearance is granted by the Inspection Service. A copy of the list is provided to the Headquarters Communications Center.

To use a Postal Service courier:

a. Prepare PS Form 1266, *Receipt for Classified Communication,* for courier signature (see 4-3).

b. When the Postal Service courier picks up the package containing classified information, instruct him or her to do the following:

   (1) Complete and sign *Recipient Information on the PS Form 1266. [Sender will need to make a photocopy for his or her records.]* PS Form 1266 accompanies the classified information package to the addressee.

   (2) Obtain the addressee's *Recipient Information* on PS Form 1266.

   (3) Have the addressee retain copy 2 for his or her records.

   (4) Return the original to you; the courier retains copy 1.

c. When you receive the signed original PS Form 1266, relinquish the signed, copy 1 to the courier to relieve him or her of accountability for the classified information.

6-5 Using the Mail

When a courier is not used, Secret information must be sent by Registered Mail, and Confidential information must be sent by Certified Mail.

Top Secret information must not be sent through the mails. Always use a courier who has proper clearance and is authorized by the Inspector in Charge, DMI-HS.

To mail classified information:

a. Enter the Registered or Certified receipt number on PS Form 1861, *Classified Document Accountability Record.*

b. Prepare PS Form 1266 (see 4-3).

6-6 Electronic Transmissions

Facsimile (fax) transmissions:

a. Classified information transmitted via fax must utilize secure communications equipment. Such equipment includes a combination of secure telephone unit/equipment (STU/STE) and a secure fax machine.

b. When transmitting classified information via fax, the classification level of the information transmitted must not be higher than the classification of the sending or receiving equipment. TOP SECRET information must not be sent from or to STU/STE equipment rated at the SECRET level. It is permissible to send information classified at a lower level to equipment rated at a higher level.

c. Secure fax equipment must be located in a secure area rated for the highest level the equipment is capable of receiving.

Electronic data:

a. Classified information stored on electronic media must only be accessed by systems rated at the same level as the highest classification of the stored information.

b. U.S. Postal Service networks are not rated for storage or transmission of classified information; therefore classified information must not be stored or transmitted using those networks. Only stand-alone equipment may be used for storage of classified electronic media.

c. Generally, electronic storage media takes on the classification level of the hardware in which it is used. Further guidance on use of storage media may be obtained from the Chief Postal Inspector, U.S. Postal Inspection Service.

d. Care must be taken to separate classified hardware from hardware classified at a lower level or that is unclassified. Guidance for equipment placement must be sought from the Chief Postal Inspector.

e. The Chief Postal Inspector determines the need for technical countermeasures in accordance with applicable regulations as provided in ISOO Directive Number 1.

Classified systems: Classified stand-alone equipment must be used and stored in an area protected in accordance with the highest level classification used on the system or equipment. See 5-3 for additional information.

7 Disposal and Destruction

7-1 Secure Disposal

Classified information no longer needed for operational purposes may be destroyed or returned to the originating agency, if requested. Classified materials identified for destruction retain their sensitivity until actual destruction. These materials must be protected in the same way as other materials of the same classification level. A witness or witnesses must ensure that classified materials are really destroyed by verifying that the destruction process meets established standards and that the contents are no longer recoverable from the residue of the destruction process.

To destroy classified information:

a. Protect them in the same way as other materials of the same classification level until the contents are no longer recoverable from the residue of the destruction process.

b. Ensure that a witness or witnesses have verified that classified materials are destroyed using established standards for destruction and that no recoverable information is present in the residue.

7-2 Disposal Methods

The Postal Service is relieved of its accountability for classified information when the information is returned to the originating agency or destroyed. Disposal or destruction of classified information must be documented in the disposition record section of the controlling PS Form 1861, *Classified Document Accountability Record.*

When destroying classified information no longer needed for operational purposes, the following stipulations apply:

c. Make sure witnesses are available to witness destruction of the types of classified information as follows:

   (1) Top Secret — Only the Top Secret Control Officer (TSCO) or Alternate TSCO is permitted to conduct the destruction. The custodian or another appropriately cleared employee must serve as the destruction witness.

   (2) Secret — The custodian or any other appropriately cleared employee may destroy the material. One witness to the destruction is required.

(3) Confidential — The custodian or any other appropriately cleared employee may destroy the material. No witness is required.

To destroy classified information:

a. If it is paper, do *one* of the following:

(1) Shred it in a shredding machine capable of shredding material as specified by current National Security Agency standards. *(An approved shredder is available in the office of the Inspector in Charge, DMI-HS.)*

(2) Burn it in an incinerator approved by the Inspector in Charge, DMI-HS.

b. If it is electronic data, do *both* of the following:

(1) Clear, purge, and degauss the processing equipment containing the information.

(2) Pulverize, smelt, incinerate, disintegrate, shred, or use any other method that ensures the physical destruction of the data storage media.

c. Document the destruction by signing the PS Form 1861 and have the necessary witnesses sign the PS Form 1861.

d. Ensure that a photocopy of the annotated PS Form 1861 is maintained by the destroying office.

If the custodian of classified information does not have approved destruction methods available, contact the Inspector in Charge, DMI-HS for appropriate destruction arrangements.

If the originating agency requests the return of classified information, do the following:

a. Remove all copies of PS Form 1861.

b. Follow the transmission procedures (see Chapter 6) and return the original and all copies of classified information to the originating agency.

c. Document that action in the disposition record section of PS Form 1861.

Forward to the Inspector in Charge, DMI-HS, the signed Standard Form 1266, *Receipt for Classified Information,* returned by the originating agency and the annotated PS Form 1861.

8 Loss or Compromise

8-1 Reporting

The loss or compromise of classified information can present a threat to national security. Classified information, regardless of its form, must be afforded a level of protection against loss or compromise commensurate with its classification level.

To report the known or suspected loss or compromise of classified information:

a. Immediately report the incident to the Inspector in Charge, DMI-HS who will notify the appropriate investigative office.

b. When a loss or possible unauthorized disclosure involves the classified information or interests of another government agency or of a foreign government agency, advise the agency of the circumstances and findings that affect their information or interests. Foreign governments are not normally advised of any security system vulnerabilities that contributed to the compromise.

8-2 Investigation

Investigation of suspected loss or compromise of classified information in Postal Service custody is conducted by Postal Inspectors as directed by the field division Inspector in Charge at the request of the Inspector in Charge, DMI-HS or by the Inspection Service Special Investigations Division, as appropriate.

No incident is officially termed a loss or compromise until the investigation is completed.

8-3 Sanctions and Penalties

Officials, employees, and contractors of the Postal Service are subject to sanctions if they knowingly, willfully, or negligently disclose to unauthorized persons national security information properly classified under the current Executive Order (EO) 12958, *Classified National Security Information,* as amended, or predecessor orders. Sanctions may include reprimand, suspension without pay, removal, loss or denial of access to classified

information, or other sanctions in accordance with applicable law and postal regulations.

If action beyond a reprimand is contemplated against any Postal Service employee believed responsible for the unauthorized disclosure of classified information, the action must be coordinated between legal counsel offices in the Postal Service. If criminal prosecution is contemplated, the U.S. Department of Justice and the appropriate Postal Service legal counsel must coordinate their efforts.

Infraction. Any knowing, willful, or negligent action contrary to the requirements of EO 12958 or its implementing directives that does not comprise a violation as so defined.

Special access program. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Violation. Any knowing, willful, or negligent action (1) that could reasonably be expected to result in an unauthorized disclosure of classified information, (2) that results in classifying or continuing to classify information contrary to the requirements of EO12958 or its implementing directives, or (3) that results in creating or continuing a special access program contrary to the requirements of the EO.

9 Program Review and Reports

9-1 Self-Inspection Program

Self-inspection means an internal review and evaluation of individual agency activities and the agency as a whole regarding program implementation pursuant to Executive Order (EO) 12958, *Classified National Security Information,* as amended and the Information Security Oversight Office (ISOO) Implementing Directive Number 1. Such reviews will include the *Elements of Coverage* as provided in section 2001.61 of the ISOO Directive Number 1.

The Inspector in Charge, DMI-HS must establish and maintain an annual self-inspection program to include, but not be limited to, the following:

a. Reviewing relevant security directives, guides, and instructions.

b. Interviewing producers and users of classified information.

c. Reviewing access and control records and procedures.

d. Reviewing a sample of derivative documents.

e. Documenting findings and making recommendations.

f. Following up on implementation of recommendations.

9-2 Audit

9-2.1 Internal Audit

Periodic audits of the Classified National Security Information Program may be conducted at the discretion of the U.S. Postal Inspection Service, DMI-HS to ensure compliance with EO, program guidance issued by the ISOO of the National Archives and Records Administration, and Postal Service regulations, policies, and procedures.

9-2.2 External Audit

The ISOO conducts periodic audits of the Postal Service Classified National Security Information Program to ensure compliance with EO 12958 as amended and ISOO directives.

9-3 Information Security Oversight Office Report

Each year, the ISOO collects statistical data on how the Postal Service administers its classified information program. When requested by the Inspector in Charge, DMI-HS, custodians of classified information must provide information for this report.

The data collected include the following:

a. The number of derivatively classified documents categorized by classification levels.

b. Information on infractions involving the handling of classified information for the reporting period. *(Examples of infractions are classifying without authority; mismarking; providing unauthorized access; and storing, reproducing, transmitting, or disposing of or destroying classified information improperly.)*

Cost estimates associated with the implementation of EO 12958 as amended.

10 Disclosure

10-1 Requests for Release of Information

Public requests for disclosure of classified information in Postal Service custody, including the news media, that are made under the Freedom of Information Act (FOIA) or the Privacy Act, must be submitted to the:

USPS FOIA REQUESTER SERVICE CENTER
US POSTAL SERVICE HEADQUARTERS
475 L'ENFANT PLAZA SW RM 5821
WASHINGTON DC 20260-5821

10-2 Responding to Freedom of Information Act and Privacy Act Requests

In response to requests made under FOIA and under the Privacy Act, the Postal Service:

a. Must not refuse to confirm the existence or nonexistence of a classified document, *unless* the fact of its existence would itself be classifiable.

b. Must forward all requests for classified information in its custody (including information within records derivatively classified by the Postal Service) to the originating agency. The originating agency reviews the request, notifies the requester of the Postal Service referral, and responds to the request. If the originating agency needs to shield itself from association with the classified information, the Postal Service custodians must respond to the requester.

Mandatory declassification review. The review for declassification of classified information in response to a request.

To respond to receipt of a request for mandatory declassification review, submit requests to:

INSPECTOR IN CHARGE DMI-HS
US POSTAL SERVICE HEADQUARTERS
475 L'ENFANT PLAZA WEST SW RM 3301
WASHINGTON DC 20260-2186

This page intentionally left blank