Department of Health and Human Services

NATIONAL SECURITY INFORMATION MANUAL

Material Transmitted

National Security Information Manual (in its entirety)

Material Superseded

This supersedes the prior HEW Security Manual, issued June 25, 1975, in its entirety.

Background

Most of the guidance in the 1975 Security Manual is obsolete. Information dealing with personnel security policy and procedures was superseded by HHS Personnel Instruction 731-1, dated August 4, 1988. The President issued Executive Order 12356 on April 2, 1982, prescribing a uniform system for classifying, declassifying, and safeguarding national security information. This Order also created the Information Security Oversight Office (ISOO) which subsequently issued an implementing directive to agencies on the control and safeguarding of classified national security information. This manual incorporates the Executive Order and ISOO requirements into HHS policy and provides specific guidance to those HHS employees and contractors who have security clearances for access to national security information.

Filins Instructions

Replace the entire obsolete 1975 HEW Security Manual with the current National Information Security Manual.

Thomas S. McFee
Assistant Secretary for
Personnel Administration

March 20, 1992
Date

Distribution: MS.HRF-119

Subject: NATIONAL SECURITY INFORMATION MANUAL

SCOPE AND ORGANIZATION

This manual provides specific guidance regarding classifying, declassifying, controlling, and safeguarding national security information. The manual addresses all aspects of the handling of national security information from the time the information is classified to the destruction of the information. While the national-security information is in possession of a HHS employee **or** contractor, various people have responsibilities for controlling and safeguarding it. This manual specifically indicates those responsibilities and provides detailed procedures to be followed when handling classified information.

National security information, also referred to as classified information, is treated very differently from other types of sensitive and official government information. Those individuals with security clearances should use this manual to guide their actions when dealing with classified information. This manual also provides security awareness guidance and sets forth certain foreign travel and contact requirements.

Throughout this manual references are made to specific HHS or Standard Forms. To allow for easy reference to them, copies are grouped together and included in the final chapter entitled, "Exhibits".

ISSUANCE MANAGEMENT

Although this manual covers security requirements and procedures, nothing in this manual is classified or sensitive so it should be shared with anyone needing guidance in this subject manner. This manual should be maintained in any office where classified material is kept or where classified information is handled.

HHS National Security Information Manual

TABLE **OF** CONTENTS

CHAPTER 4-00 - MARKING DERIVATIVELY CLASSIFIED DOCUMENTS

CHAPTER 5-00 - ACCESS AND DISSEMINATION

CHAPTER 6-00 - CUSTODY, ACCOUNTABILITY AND REPRODUCTION

CHAPTER 7-00 - STORAGE

CHAPTER 8-00 - TRANSMISSION

CHAPTER 9-00 - DISPOSAL AND DESTRUCTION

CHAPTER 10-00 - SECURITY AWARENESS, CONTACT WITH CERTAIN FOREIGN NATIONALS, AND FOREIGN TRAVEL

CHAPTER 11-00 - OTHER SPECIAL SECURITY PROGRAMS

CHAPTER 12-00 - EXHIBITS

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

AIS	Automatic Information Systems
ARFCOS	Armed Forces Courier Service
ASPER	Assistant Secretary for Personnel Administration
C	Confidential
CFR	Code of Federal Regulations
COMSEC	Communications Security
CUSR	Central United States Registry
DECL/DG	Declassification/Downgrading
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
GSA	General Services Administration
10s	Immediate Office of the Secretary
IS00	Information Security Oversight Office
LCO	Logging Control Officer
LCP	Logging Control Point
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NSDD	National Security Decision Directive
OADR	Originating Agency's Determination Required
OPDIV	Operating Division
OPS	Office of Personnel Services, ASPER
PA	Privacy Act
SDD	Personnel Security and Drug Testing Program Division
S	Secret
STAFFDIV	Staff Division
TS	Top Secret
U	Unclassified
U.S.C.	United States Code
USPS	United States Postal Service
USSAN	United States Security Authority for NATO Affairs
TSCO	Top Secret Control Officer

Subject: SAFEGUARDING NATIONAL SECURITY INFORMATION - GENERAL PROVISIONS

1-00-00 PURPOSE

The National Security Information Manual is the official Departmental medium for providing policy and procedural guidance to the Department of Health and Human Services **(DHHS)** employees and contractors who have access to classified national security information. This manual prescribes policy and responsibility for handling and safeguarding national security information in the possession of DHHS. The guidance provided is to be used mainly by those individuals who have security clearances or have security program responsibilities. This manual is a part of the DHHS Staff Manual System.

l-00-05 AUTHORITY

Executive Order (E.O.) 12356, National Security Information, dated April 2, 1982; Information Security Oversight Office **(ISOO)** Directive Number 1, (32 **C.F.R.2001),** concerning National Security Information, dated June 23, 1982; National Security Decision Directive (NSDD)-84, Safeguarding National Security Information, dated March 11, 1983; and NSDD-197, Reporting Hostile Contacts and Security Awareness, dated November 1, 1985.

l-00-10 POLICY

It is the policy of the DHHS to safeguard from unauthorized disclosure all national security information, also referred to as classified information, in the custody of the Department and its employees and contractors.

l-00-15 APPLICABILITY

A. The requirements of this manual apply to all HHS employees and contractors whose duties require access to national security information.

B. Heads of OPDIVS and STAFFDIVs are authorized to issue supplemental guidance and instructions to facilitate implementation of the requirements of this manual within their divisions. A copy of each supplement issued must be furnished to the Director, Office of Personnel Services (OPS), Office of the Assistant Secretary for Personnel Administration (ASPER).

l-00-20 REFERENCES

A. E.O. 12356 which prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

B. ISOO Directive No. 1 which implements the provisions of E.O. 12356, and further sets forth guidance relating to original and derivative classification, downgrading, declassification, and safeguarding of national security information.

C. NSDD-84 which establishes procedures to safeguard against the unauthorized disclosure of national security information.

D. NSDD-197 which requires the creation and maintenance of a formalized security awareness program designed to protect classified, proprietary, and sensitive information from foreign sources, whether overt or covert. NSDD-197 also requires that procedures be established for employees to report any contacts with certain individuals and foreign nationals of certain specific countries.

E. ISOO Briefing Booklet, undated, which provides information about the "Classified Information Nondisclosure Agreement," also *known as* the "SF 312."

F. HHS Instruction 731-1, Personnel Manual, dated August 4, 1988, which provides policy and guidance on personnel security and security briefings of individuals requiring security clearances for access to national security information.

G. U.S. Security Authority for NATO Affairs (USSAN) Instruction l-69, dated April 21, 1982, which provides policy and guidance for the safeguarding of NATO classified materials.

H. National Telecommunications and Information Systems Security Policy (NTISSP) No. 3, dated December 19, 1988, which was developed by the National Telecommunications and Information Systems Security Committee for the purpose of preventing the loss or unauthorized disclosure of U.S. classified **crytographic** information.

I. Other classified directives and manuals of national security agencies which provide policy and guidance for **HHS** personnel who are briefed into their special access programs.

l-00-25 DEFINITIONS

A. Access - The ability and opportunity to obtain knowledge of classified national security information.

B. Asencv - a Federal agency as defined in Title 5 **U.S.C.,** Section 552(e).

c. **Compromise** - The known or suspected exposure of classified information to an unauthorized person.

D. Controlled Area - Any area, entry to which is subject to restrictions for security reasons.

E. Custodian of Classified Files - An employee who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

F. Declassification - A determination, made by an original classification authority, that classified information no longer requires, in the interests of national security, protection against unauthorized disclosure under E.O. 12356 together with a removal or cancellation of the classification designation.

G. Derivative Classification - A determination that information is in substance the same as information currently classified. The newly developed information is marked consistent with the classified markings of the source material.

H. Downsrade - A determination made by the originating authority that particular classified information requires, in the interests of the national security, a lower degree of protection than currently provided. This determination requires changing of the classification designation to reflect such lower degree of protection.

I. Inadvertent Access - An incident in which an employee had access to classified information to which the employee was not authorized.

J. Logging Control Officer (LCO) - An employee responsible for the proper maintenance of records relating to the safeguarding and storage, accountability, transmission and destruction of national security information.

K. Logging Control Point (LCP) - A central place within an office or organization where all classified information is received, recorded, stored, transmitted or destroyed.

L. Multiple Sources - The term used to indicate that a document that is derivatively classified contains classified information derived from more than one source.

M. National Security - The national defense and/or critical foreign relations of the United States.

N. National Security Information - Information that has been determined pursuant to E.O. 12356, or any predecessor E.O. concerning national security, to require protection against unauthorized disclosure. National security information is also referred to as classified information. Such information must be appropriately marked TOP SECRET, SECRET, or CONFIDENTIAL, according to contents, by an official possessing the original classification authority under E.O. 12356.

0. Orisinal Classification - An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

P. Oriainal Classification Authority - The authority vested in a designated executive branch official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. DHHS does not have this authority.

Q. Personnel Security Representative (PSR) - A senior management official designated, in writing, the responsibility for his/her organization's personnel security program. PSRs maintain lists of those individuals within their organization who have security clearances and keep current information on their organization's LCPs and LCOs.

R. Security Classification Levels - National Security Information is classified at one of the following three levels:

1. "TOP SECRET" is applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

2. "SECRET" is applied to information, the unauthorized disclosure of which could reasonably be expected *to cause serious* damage to the national security.

3. "CONFIDENTIAL" is applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

S. Security Clearance - An administrative determination based upon the results of a favorably adjudicated investigation that an individual is trustworthy and may be granted access to a specified level of national security information as required in the performance of assigned duties (see HHS Instruction 731-l for clearance procedures).

T. Special Access - That special compartmented category of national security information accessible to selected individuals on a must know basis. It requires a current Top Secret clearance, a recent Special Background Investigation (SBI), specific justification to the agency responsible for the special access program, and a unique security briefing,

U. Unauthorized Disclosure - A communication or physical transfer of specific classified information to a person not authorized access to that level of classified information or not having met need-to-know requirements.

V. TOP SECRET Control Account - An approved method within an established LCP for the storage, receipt, and transmission of Top Secret documents, when authorized in accordance with section **1-00-30C.**

W. TOP SECRET Control Officer **(TSCO)** - An official who has a Top Secret clearance and is designated in writing to be responsible for receiving, safeguarding, controlling, accounting for, and destroying all Top Secret documents within the **TSCO's** assigned area of responsibility.

1-00-30 RESPONSIBILITIES

A. The Assistant Secretary for Personnel Administration **(ASPER)** is the senior Department official responsible for the overall implementation of E.O. 12356, **ISOO** Directive No. 1, **NSDDs-84** and 197, and similar future directives. Specific responsibilities include:

1. Issuing Department guidance to implement the provisions of E.O. 12356, **ISOO** Directive No. 1, NSDDs-84 and 197, and future national security information directives.

2. Maintaining active oversight of the Department's Information Security Program for the safeguarding of national security information.

3. Making the final determination on a denial of a security clearance and/or access to classified information, based upon specific unfavorable information regarding the trustworthiness or loyalty of an **HHS** employee or contractor.

B. The Heads of OPDIVS, STAFFDIVS, and **DHHS** Regional Directors are responsible for assuring that the requirements of this manual are implemented for their respective organizations. Specific responsibilities, which **can** be delegated, include:

1. Ensuring that all national security information received-or handled-within their organizations is properly safeguarded and controlled.

2. Ensuring that **classified** documents which are no longer required are properly destroyed in accordance with chapter **9-00.**

3. Designating a senior management official to serve as the primary Personnel Security Representative (PSR) for his/her respective organization to handle national security information responsibilities, in addition to personnel security responsibilities. (To further handle their security responsibilities in the Regions, **OPDIVs** and **STAFFDIVs** may designate their own regional **PSRs** or may request that the PSR designated by the Regional Director handle certain responsibilities for their organization.)

4. Establishing **a** Logging Control Point (LCP) for any major office or organization which needs to store classified information and designating, in writing, a Logging Control Officer (LCO) or a separate Custodian of Classified Files, as needed.

5. Establishing additional written procedures, as necessary, to prevent unauthorized access to national security information and reduce the opportunity *for* the negligent or deliberate disclosure of the information.

c. The Director of the Office of Personnel Services (OPS) is responsible for:

1. Overseeing the development of policy and procedures for the Department's classified information security program for the safeguarding of national security information.

2. Providing consultation and advice on the classified information security program to OPDIV, STAFFDIV, and other management officials.

D. The Director, Personnel Security and Drug Testing Program Division (SDD), OPS, **ASPER,** is responsible **for:**

1. Developing Department regulations to implement E.O. 12356, ***1800*** Directive No. 1, **NSDDs-84** and 197, and other similar directives.

2. Developing and publishing security education material for us8 by PSRs, and employees and contractors who have been granted access to national security information.

3. Processing required personnel security investigations, in accordance with the HHS Personnel Manual, and granting or denying security clearances to HHS employees and contractors.

4. Conducting national security information program reviews, assistance visits, inspections, and surveys within HHS to ensure compliance with this manual and authorities.

5. Receiving reports relating to the unauthorized disclosure and mishandling of national security information, and coordinating these, as necessary, with HHS and other Federal agency officials.

6. Providing security guidance and assistance to PSRs and contractors as needed or requested.

7. Furnishing any required reports to the Director, ISOO.

8. Designating a Headquarters Top Secret Control Officer (TSCO) who shall be responsible for the control and accountability of all Top Secret documents in the custody of the Headquarters Top Secret Control Account.

9. Approving requests for the establishment of a Top Secret Control Account and the assignment of a TSCO, whenever Top Secret information is routinely stored and received.

10. Designating a Logging Control Officer (LCO) and establishing a Logging Control Point (LCP) to service the Immediate Office of the Secretary.

11. Appointing a Subregistry Control Officer and alternate(s) to be responsible for the Department's NATO Subregister.

12. Serving as the principle Personnel Security Representative for the Office Of the Secretary.

E. Each Personnel Security Representative (PSR) has the following national security information responsibilities:

1. Providing security advice on the handling of classified information to officials and employees of the organization, some of whom may be designated as regional security representatives.

2. Ensuring that an employee or contractor has a legitimate need for a security clearance before signing the Request for Security Clearance, HHS Form 207, (see Exhibits), and forwarding it to SDD.

3. Conducting security inspections of all offices that store or handle classified information. The purpose of these inspections is to assure that office managers, supervisors, and employees, who are responsible for classified material, are in compliance with this manual.

4. Furnishing to the Director, SDD, when requested, a completed DHHS Annual Status Report on Classified National Security Information and any other reports, as needed.

5. Conducting preliminary inquiries relating to an unauthorized disclosure or loss of classified information.

6. Maintaining an up-to-date alphabetical list of all employees and contractors granted clearance for access to national security information. The list should include the level of clearance and the date of the last investigation on the cleared person.

7. Coordinating with Director, SDD, security matters affecting other Federal agencies (e.g., FEMA, DOD, and DOE access clearances).

8. Ensuring that initial, refresher, and termination security briefings are conducted as required by the HHS Personnel Manual and that required nondisclosure agreements and debriefing acknowledgments are signed and returned to SDD.

F. Supervisors. while certain employees may be assigned specific security responsibilities, it is nevertheless the basic responsibility of their supervisors to ensure that national security information entrusted to their employees is safeguarded according to the policies and procedures contained in this manual. Supervisors whose employees routinely handle or store classified information are responsible for taking the following actions:

1. Assuring for the proper accountability, control, and storage of classified information as outlined in Chapters 6-00 and 7-00.

2. Designating, in writing, any employees authorized to *receive* and open outer and inner covers (envelopes) of security mail which is addressed to other cleared employees.

3. Assuring that no employee is permitted to have access to classified information until it has been officially determined that the employee has been granted the appropriate level of security clearance and has a bonafide need-to-know for the information in the performance of his/her duties.

4. Assuring that the LCO, Custodian of Classified Files, and any Of their employees, who have been granted access to classified information, are made aware of others in the organization (e.g., division) who have security clearances and meet the "need-to-know" requirement.

5. Promptly reporting any violation of security procedures to their PSR.

6. Establishing a system of security checks at the close of each working day to assure proper safeguarding of classified information.

G. Logging Control Officer (LCO). Each LCO has the following responsibilities:

1. Receiving all incoming accountable communications containing classified information.

2. Inspecting sealed envelopes or similar wrappings containing classified information for any evidence of tampering, damage, or unauthorized disclosure.

3. Matching the actual contents of an incoming package of classified material with the enclosed receipt.

4. Signing and returning to the sender enclosed receipts for classified material.

5. Maintaining an up-to-date Classified Document Accountability Record, **HHS** Form 208 (see Exhibits), and other documents showing disposition of classified materials.

6. Verifying through the PSR the security clearance level of recipients of classified information, including the clearance level of the Custodian of Classified Files who will store the information.

7. Assuring prompt delivery of classified information to intended recipients who have the appropriate security clearance.

8. Handling the responsibilities of the Custodian of Classified Files (see next page), unless there is a separately designated Custodian of Classified Files.

9. Taking prompt action on any downgrading and/or declassification notices received and coordinating with PSR action taken.

10. Assuring that the appropriate secure method of transmission is selected, and that the material is properly prepared for transmission.

11. Designating, either orally or in writing, an employee with a security clearance to act as a courier of classified documents and assuring the courier is properly briefed.

12. Destroying any unneeded classified documents in accordance with Chapter **9-00.**

13. Completing an audit of classified documents and reporting that data and other information on the DHHS Annual Status Report on Classified National Security Information.

H. Custodians **of** Classified Files. when it is considered an absolute necessity that classified documents be stored in offices other than the LCP, separate Custodians **of** Classified **Files shall** be designated, in writing, to carry out the required duties.

Employees appointed as Custodians **of** Classified Files are responsible for:

1. Providing protection for all classified information entrusted to their care.

2. Locking **classified** information in approved security containers whenever it is not in use or under the direct control of an authorized and cleared person.

3. Verifying the security clearance level of any person prior to giving that person access to classified information.

4. Returning to the LCP classified material designated for destruction.

5. Providing periodic inventory reports to the LCO.

I. Employees. My employee who obtains access to national security information is responsible for the protection of that information, regardless of how it was received. Employees also are responsible for reporting to their supervisor and/or their PSR the loss, or temporary loss, of control or possession of national security information.

Every employee or contractor who has a security clearance must be familiar with and adhere to the provisions of this manual. Employees whose official duties involve contacts with representatives of the public media are to ensure that any classified **information** to which they may have access is never divulged, under any circumstances, to the media or other uncleared individuals (see Restrictions, Section 5-00-15).

l-00-35 REPORTING A SECURITY INCIDENT

A. Any employee who **has** *knowledge* of the loss or possible compromise **of** classified information, or who discovers that a classified document is not being properly safe-guarded, must immediately report the known circumstances to his/her immediate supervisor and PSR. The report may

be made orally or by memorandum. This security incident must be immediately reported by the PSR to the Director, SDD, who will report this to the agency that originated the information if there is reason to believe classified information has been lost or compromised.

B. The PSR must conduct a preliminary inquiry to fully determine the circumstances surrounding the reported security incident. The preliminary inquiry report must be in writing and sent to the Director, SDD, within ten workdays from the date of the incident, the inquiry report must not contain any classified information, however, it should include all relevant facts concerning the incident, including all steps taken to recover any missing classified documents.

C. The agency that originated the classified information must be promptly notified by the Director, SDD, of the loss or possible compromise, after relevant facts are gathered, so that a damage assessment can be conducted and measures are taken to negate or minimize any adverse effect of the compromise.

D. Normal due process procedures must be followed whenever an administrative action is contemplated against any HHS employee or contractor believed responsible for the compromise of classified information. Whenever a violation of criminal law appears to have occurred, the agency responsible for the damage assessment will coordinate with the Department of Justice to determine whether there will be criminal prosecution.

E. If there is no loss or possible compromise or unauthorized disclosure of classified information, the report of preliminary inquiry will be sufficient to resolve any procedural infraction, and when appropriate, support the taking of any administrative action. A procedural infraction is an incident which involves the misuse or improper handling of classified information where the action does not result in a possible compromise of classified information.

F. Additional procedures may be required when reporting a security incident involving special access program materials. The Director, SDD, will provide those procedures and coordinate that inquiry.

l-00-40 ADMINISTRATIVE AND CRIMINAL SANCTIONS

A. HHS employees may be subject to various administrative sanctions, including reprimand, termination of security clearance, or suspension or termination of employment, as appropriate, if they:

1. Refuse to cooperate in the conduct of a preliminary inquiry or formal investigation regarding a national security issue.

2. Knowingly, willfully, or negligently cause an unauthorized disclosure of classified information.

3. Display a lack of security responsibility relating to the proper handling and safeguarding of national security information.

B. In addition to the administrative sanctions stated above, criminal sanctions may also be imposed. HHS employees may be subject to criminal sanctions as described under Sections 641, 793,. 794, 798, and 952 of Title 18, U.S.C., Section 783 (b) of Title 50, U.S.C. or other appropriate statutes. Such sanctions may include penalties of up to $10,000 fine, or imprisonment for ten years, or both (refer to 1800 Briefing Booklet).

l-00-45 REPORTING REQUIREMENTS

PSRs are responsible within their respective organizations for the submission of an annual National Security Information Data Report to the Director, SDD. The format for the report will be furnished to the PSRs by the Director, SDD, typically near the end of each fiscal year, to request data needed for oversight responsibilities. Some of the data requested is used to report to ISOO and other agencies with national security responsibilities.

l-00-50 SUGGESTIONS

Suggestions about the HHS National Security Information Program, as set forth in this manual, should be directed in writing to the Director, OPS. Suggestions for program improvement may be discussed with the Director, SDD, at any time.

Subject: **CLASSIFICATION**

2-00-00 PURPOSE

This chapter tells how to classify information which requires protection in the interest of national security.

2-00-05 ORIGINAL CLASSIFICATION

A. No official of the DHHS is authorized under E.O. 12356 to originally classify information as TOP SECRET, SECRET, or CONFIDENTIAL. However, if in an evolving sensitive situation any employee originates or develops national security information which is believed to require original classification, that employee must safeguard the information in the manner prescribed by Chapter 7-00. The information must be promptly transmitted to the Director, SDD, in the manner provided by Chapter 8-00, unless advised differently by the Director, SDD. The Director, SDD, must contact ISOO for guidance on further steps to determine if the information is classifiable.

B. Under no circumstances shall information be considered for classification to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security. Basic scientific research information not clearly related to the national security shall not be considered for classification.

2-00-10 DURATION OF CLASSIFICATION

A. Information shall be classified as long as required by national security consideration. such determinations shall only be made by the original classification authority.

B. Documents classified by other agencies under predecessor **E.O.s** that are marked for automatic downgrading or automatic declassification on a specific date or event shall be downgraded and declassified according to the instructions on the face of the documents.

C. Documents, classified by other agencies under predecessor **E.O.s,** that are not marked for automatic downgrading **or** declassification on a specific date or event must **not** be downgraded or declassified without authorization, in writing, from the original classification authority.

2-00-15 DRRIVATIVR **CLASSIFICATION**

A. Derivative classification is (1) the determination that information is, in substance, the same as information currently classified, and (2) the application of the same classification markings. Employees who only reproduce, extract, or summarize classified information, or who apply classification markings derived from source material, or as directed by a classification guide, need **not** possess original classification authority.

B. The application of derivative classification markings is a responsibility of those who incorporate, paraphrase, restate, **or** generate in new form, information that is already classified by an authorized original classification authority, or in accordance with an authorized classification guide.

c. The overall classification markings and portion (paragraph) markings of the source document should supply adequate classification guidance to the person marking the extraction. If portion markings or classification guidance are not found in the source document, and no reference is made to an applicable classification guide, guidance must be obtained from the originator of the source document.

D. Employees who are authorized to apply -derivative classification markings must:

1. Be **designated,** in writing, by the supervisor who has responsibility for the classified information, and possess the **appropriate** level of security clearance. A copy of the designation shall be furnished **to the** PSR and Director, SDD.

2. Respect and comply with the classification decisions reflected in the source document or classification guide.

3. Carry forward to newly created documents the markings and information prescribed by Section 4-00-05.

4. Maintain a copy of the source document or pertinent identifying information from the source document with the record or file copy of the derivatively classified document.

2-00-20 **CLASSIFICATION** GUIDES

A classification guide is written guidance that is issued by an official exercising **original** classification authority over particular programs, projects, or classes of documents. The primary purpose of a classification guide is to ensure that proper and uniform classification markings are applied to derivatively classified information.

Subject: DECLASSIFICATION AND DOWNGRADING

3-00-00 PURPOSE

The purpose of this chapter is to provide guidance relating to the declassification and downgrading of information which was originated by other agencies and predecessor DHHS agencies who had original classification authority under prior Executive Orders.

3-00-05 DECLASSIFICATION AND DOWNGRADING AUTHORITY

A. Classified information originated by other agencies shall only be declassified and downgraded by the official of the originating agency who authorized the original classification, if that official is still serving *in* the same position; by a successor; or by a supervisory official of either.

B. All classified documents originated by a DHHS predecessor agency and being retained for some official reason, may be declassified by the Director, SDD, following the coordination with the IOS, OPDIV, or STAFFDIV that has subject matter interest in the documents. If it is determined that some information meets the *current* criteria of Section 2-00-10, or there is some doubt concerning its classification, the information must be promptly transmitted in the manner required by Chapter 8-00, to the Director, SDD, for review and transmittal to an agency that has appropriate subject matter interest and original classification authority. That agency shall decide whether to declassify, upgrade, downgrade, or to extend the initial classification level of the document.

C. PSRs of each organization should require the annual review of all classified documents in their possession and control to identify documents which require declassification, downgrading, or destruction. This review should be accomplished prior to completion of the DHHS Annual Status Report on Classified National Security Information.

The following review guidelines shall be followed:

1. All old and obsolete classified documents which have served their purpose must be destroyed in the manner prescribed by Chapter 9-00.

2. All classified documents originated by another agency, as most are, and being retained for some official reason, should be reviewed for declassification and downgrading in accordance with the specific instructions contained on the cover or first page of the documents. If there are no specific instructions, the originator of the documents should be requested to provide the necessary information.

3-00-10 MANDATORY REVIEW FOR DECLASSIFICATION

A. Classified information originally classified by the DHHS predecessor agencies, under prior E.O.s, must be reviewed for declassification upon receipt of a written request by a U.S. citizen or permanent resident alien, a Federal agency, or a state or local government. For release of the information, a valid request need not identify the requested information by date or title, but must be of sufficient particularity to allow HHS employees to locate the information sought with a reasonable amount of effort. Requests should be submitted to the Director, SDD.

B. The Director, SDD, will coordinate the request with the office in charge of Freedom of Information (FOI)/ Privacy Act (PA) requests, Office of the Assistant Secretary for Public Affairs, in an attempt to locate the requested classified information. Responses to requests shall be governed by the amount of search and review time required to process the request. However, in the interest of being responsive to such requests, the 106, STAFFDIV or OPDIV office which has primary interest in the subject matter must be contacted in an attempt to locate and review the requested information. Results of the review, including recommendations and a copy of the requested information, or a request for additional time, must be furnished to the Director, SDD. E.O. 12356 requires that agencies make a final declassification determination within one year from the date of receipt except in unusual circumstances.

C. The IOS, STAFFDIV, or OPDIV office should make a prompt recommendation to the Director, SDD, for the requested information or portions **to be** declassified. When the requested information cannot be declassified in its entirety, reasonable efforts shall be made to release those declassified portions that constitute a coherent segment. If the information may not be released in whole or in part, the action office must provide the reasons for denial. When the classification of the requested information is a derivative decision based on classified source material of another agency, the information must be provided to that agency for review and comment.

D. Upon receipt of the declassification review recommendation, the Director, SDD, must make the declassification determination after contacting the originating **agency,** when necessary, and furnish any declassified information to the office handling FOI/PA requests **for** a determination regarding release of the information.

E. Declassification of all or any information must be accomplished by the Director, SDD, **by** marking it to reflect the change as well as the authority for, and date **of,** the declassification action. If the request for declassification is denied, in whole or in part, the Director, SDD, must notify the **requestor** of the information of the right to appeal the determination within 60 days of receipt of the denial.

F. A **requestor** may appeal to the **ASPER** when the requested information is not declassified and released in whole. Appeal review procedures are as follows:

1. The **ASPER** shall normally make a determination within 30 work days following the receipt of an appeal. If additional time is required to make a determination, the **ASPER** shall notify the **requestor** of the additional time needed and provide the **requestor** with the reason for the extension. If continued classification of the information is required, the **ASPER** shall notify the **requestor** in writing of the final determination and of the reason for any denial.

2. During the appeal review,.the **ASPER** may overrule any previous determination in whole **or** in part when, in his/her judgment, continued protection of information is no longer required in the interest of the national security. If the **ASPER** determines that the information no longer requires classification it shall be declassified and, *unless it* is otherwise exempt from disclosure under the **FOIA/PA,** released to the **requestor.** The **ASPER** shall advise the original DHHS reviewing office of his/her decision.

Subject: MARKING DERIVATIVELY CLASSIFIED DOCUMENTS

4-00-00 PURPOSE

This chapter provides specific guidance for marking documents containing derivatively classified information.

4-00-05 IDENTIFICATION AND MARKINGS

A. Classified information must be marked at the time of original classification to inform and warn the holder of the information about its sensitivity. An official who exercises original classification authority under E.O. 12356 is responsible for ensuring that the proper classification markings are applied. These markings are also applied to derivatively classified documents when such action is taken in accordance with Section 2-00-20.

B. Derivatively classified documents shall be marked as follows:

1. The highest level of security classification (TOP SECRET, SECRET, or CONFIDENTIAL), extracted from a source document or determined from an originating agency's classification guide, must be marked or stamped at the top and bottom on the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover or page.

2. Each interior page must be marked at the top and bottom according to the highest classification of the extracted information, i.e., TOP SECRET, SECRET, CONFIDENTIAL, or UNCLASSIFIED.

3. Each section, part, paragraph, subparagraph, or similar portion of a derivatively classified document must be marked to show the level of classification assigned to the specific information.

4. The following information shall also be brought forward and reflected on the face of a derivatively classified document.

   a. Classification Authoritv. The "CLASSIFIED BY" line must show a description of the source document or classification guide. If a document is derivatively classified on the basis of more than one source document or classification guide, the "Classified By" line shall contain the notation "CLASSIFIED BY MULTIPLE SOURCES." In these cases the derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. A document derivatively classified on the basis **of** a source document that is marked "CLASSIFIED BY MULTIPLE SOURCES" must cite the source document in its **"CLASSIFIED BY"** line rather than the term "MULTIPLE SOURCES." For example, CLASSIFIED BY: JCS-J3, or CLASSIFIED BY: Department of State MCN ooooo/ooooo. The MCN (Message Control Number) is cited at the top of each message/cable.

   b. Declassification and Downurading Instructions.

   Dates or events for automatic declassification or downgrading, or the notation **"OADR"** (Originating Agency's Determination Required) to indicate that the document is not to be declassified automatically, must be carried forward from the source document, or as directed by a classification guide, and shown on the "DECLASSIFY **ON"** line.

C. Transmittal Documents

1. A transmittal document shall be marked to show the highest level of classification of the derivative information contained in the transmittal itself, if applicable, and in the material attached. A transmittal document which does not contain classified information shall-be-marked with the highest level of classification of the attachments. The marking shall appear at **the top** and bottom, of the first page only. In. addition to the classification marking, type the statement, "UNCLASSIFIED **WHEN**

CLASSIFIED ATTACHMENT IS **REMOVED," at** the bottom margin of the first page.

2. A transmittal document containing derivatively classified information shall be marked in the manner prescribed by Section **4-00-05** above, and contain a legend showing the classification of the transmittal document standing alone. For example, if the removal of the transmittal material will change the classification of the transmittal document itself, it shall be marked: UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS (enter highest classification of information contained in the transmittal document).

Subject: ACCESS AND DISSEMINATION

5-00-00 PURPOSE

This chapter provides general guidance for granting access to classified information.

5-00-05 SECURITY CLEARANCE AND ACCESS

A. An employee is eligible for access to classified information provided the employee has been determined to be trustworthy and access is essential to the accomplishment of lawful and authorized Government purposes. The Director, SDD, is responsible for processing personnel security investigations and the granting of security clearances. A need for access to classified information must be demonstrated before a Request For Security Clearance, HHS Form 207, can be initiated. The number Of employees cleared and granted access to classified information must be maintained at the minimum number that is consistent with operational requirements and needs.

B. No one has a right to have access to classified information solely by virtue of title, position, or level of security clearance. The final responsibility for determining whether the individual has been granted the level of security clearance needed, and whether an individual requires access to classified information, rests with the individual who has possession, knowledge, or control of the classified information, and not upon the prospective recipient. Verification of a security clearance may be made through the individual's PSR or the Director, SDD.

C. In addition to a security clearance, a person must have a need-to-know the classified information in connection with the performance of official duties. Persons who disclose classified information must advise recipients of the classification level of the information.

5-00-10 ADMINISTRATIVE DOWNGRADE OR WITHDRAWAL OF ACCESS

A. A PSR or the Director, SDD, in coordination with the appropriate office manager or supervisor, may determine that a currently cleared individual no longer requires access to classified information or requires access at a lower clearance level. After notification to the individual, the Director, SDD, may administratively withdraw or downgrade the clearance. If the clearance is withdrawn, the individual should be debriefed and asked to sign the Security Debriefing Acknowledgment on the lower portion of the back of Standard Form (SF) 312, Classified Information Nondisclosure Agreement (see Exhibits). The SF-312 with original signature must be sent to the Director, SDD, for maintenance.

B. The Director, SDD, also may administratively withdraw a clearance whenever a previously cleared individual refuses to comply with reinvestigation requirements. The clearance, subsequently, may be reissued based upon compliance with reinvestigation requirements and a redetermination of the individual's trustworthiness and identifiable need for access.

C. A security clearance may be revoked by the ASPER when it is determined that such clearance or access is no longer consistent with the interests of national security due to a question regarding the individual's trustworthiness or loyalty. Due process procedures must be followed when processing a revocation of a security clearance for cause. Guidelines published in Federal Personnel Manual Chapter 732, Personnel Security, should be followed.

D. Whenever a security clearance is administratively withdrawn or revoked the employee shall receive the termination briefing prescribed by the HHS Personnel Manual. The Director, SDD, will notify the employee's PSR about the termination of the security clearance so that the PSR can inform the employee's supervisor, LCO, and others who have a need to know.

5-00-15 RESTRICTIONS

A. Classified information must be discussed only with persons who are properly identified, have the proper security clearance, and have a valid need-to-know the information in performance of official duties. Discussion of classified information in homes with relatives or friends, in public places, on public conveyances, or any place where unauthorized persons may have access, is strictly prohibited. Classified information must not be released to employees or other persons for their private use.

B. Employees must not comment on published news articles concerning information that they know or think to be classified. Publication by a news media does not constitute proper authority for declassification, and is often the product of astute guessing.

C. Standard telephones, inter-office communication systems, and unsecured mobile radio telephones must not be used for purposes of discussing classified information. A number of secure telephones are available throughout DHHS for use by cleared employees. The Director, SDD, can provide their location.

5-00-20 DISSEMINATION OF OTHER AGENCY INFORMATION

Classified information originated in another agency must not be disseminated outside the DHHS without the consent of the originating agency. Such consent must be maintained in writing as a matter of record. This restriction does not apply to the authorized dissemination within the DHHS unless such a limitation is stated on a specific classified document.

5-00-25 DISSEMINATION OF DHHS INFORMATION

Classified information originated by this Department, under the authority of prior Executive Orders, must not be disseminated outside of the Department until the information is reviewed for downgrading or declassification in accordance with Chapter 3-00.

5-00-30 ACCESS BY FOREIGN NATIONALS, FOREIGN GOVERNMENTS, AND INTERNATIONAL ORGANIZATIONS

No HHS official or employee is authorized to discuss or make available any classified information to foreign nationals, foreign governments, or international organizations. Refer requests for such information to the originating agency, or to the Director, SDD, for information originally classified by the Department under predecessor Executive Orders.

Subject: CUSTODY, **ACCOUNTABILITY,** AND REPRODUCTION

6-00-00 PURPOSE

The purpose of this chapter is to provide instructions relating to the custody, accountability, and reproduction of classified information in the possession **of** the Department.

6-00-05 CUSTODY OF CLASSIFIED **INFORMATION**

A. Any employee who has possession **of**, or is charged with the responsibility for classified information, is responsible for protecting and accounting for that information. The following measures shall be taken to properly protect classified information:

1. While in use, classified documents must be kept under observation of a cleared person or properly stored in accordance with Chapter **7-00.**

2. An employee who receives a classified document and has no authorized storage container available must either return the document, arrange with another office to store the document in a manner that will meet the storage requirements as outlined in Chapter 7-00, or destroy it by an approved method in accordance with Chapter **9-00.** Under no circumstances shall classified information be left unattended, be left in an unauthorized storage container, or be left in the custody of a person who does not have the proper security clearance and a need-to-know the information.

3. Classified information must only be delivered to or left with cleared recipients.

4. Occupants of an office must ensure that uncleared persons assigned to or **visiting** the office do not take or read classified information, overhear classified **discussion, or** have visual access of classified information.

5. Classified information must be discussed only with cleared **persons** who have the need-to-know, and must not be discussed in public or other places where it may be heard by unauthorized persons.

6. Classified information must not **be checked with** baggage or left in such places as private residences, locked or unlocked automobiles, hotel rooms, hotel safes, aircraft, train compartments, buses, public lockers, etc.

7. Classified information must not be read, studied, displayed, used or discussed in any manner in a public conveyance **or** place.

6-00-10 ACCOUNTABILITY OF CLASSIFIED INFORMATION

A. Office managers and supervisors whose employees handle or store classified information must ensure that procedures are established for the accountability of Top Secret and Secret information. Such procedures shall provide for tracing the movement of classified information, limited dissemination, prompt retrieval of documents, detection of the loss of information, and prevention **of** excessive production and reproduction **of** documents. At a minimum, the following accountability procedures shall be established for each level of classification.

1. Top Secret Information.

a. A TSCO, designated in accordance with Section **1-00-30C,** shall administer each authorized Top Secret Control Account by using a Classified Document Accountability Record, **HHS** Form 208 (see Exhibits), to track each Top Secret document. Only Top Secret documents shall be accounted for on this **HHS** Form 208.

b. A Classified Document Receipt, HHS Form 25 (see Exhibits), must be used each time Top Secret documents are transmitted from one individual, office, organization, or agency to **another. HHS** Forms 208 and 25 should be **destroyed five years** after the Top Secret **documents are destroyed,** transferred, or downgraded.

2. Secret and Confidential Information.

   a. A separate HHS Form 208 must be used to account for all Secret documents received by an HHS office. HHS Form 25 must be used as a receipt for Secret documents whenever they are transmitted from one individual, office, organization, or agency to another. These HHS Forms 208 and 25 should be destroyed two years after the related documents are destroyed, transferred, or downgraded.

   b. Accountability records and document receipts are not required for Confidential information, although their use is a good security practice to aid in controling these classified documents. However, Confidential information must be handled, stored, and transmitted in accordance with the provisions of this manual. Confidential documents can be accounted for on the same HHS Form 208 that is used for Secret documents and the same HHS Form 25 can be used when Confidential documents are being sent with Secret ones.

3. Working Papers. Working papers are documents, including drafts, that are created to assist in the formulation and preparation of a finished document. Working papers containing classified information must be handled and safeguarded like normal classified information.

4. To prevent the inadvertent or unauthorized disclosure of Top Secret, Secret, and Confidential classified information, it must be protected by a cover sheet. Standard Form (SF) 703 (Top Secret Cover Sheet), SF 704 (Secret Cover Sheet), or SF 705 (Confidential Cover Sheet) must be used for this purpose (see Exhibits). A SF 703, 704, or 705 cover sheet must be affixed to the front of the classified document and remain attached until the document is destroyed. At the time of destruction the forms- should be removed and, depending upon their condition, reused. If an office routinely receives numerous Confidential cable messages, e.g. those from the State Department, they can be kept in separate -file -folders with a SF 705 attached to the front of each folder.

5. Limited Official Use (LOU) information is not classified national security information and therefore is not covered by E.O. 12356. However, the information, which usually involves sensitive State Department activities, should be tightly controlled and stored in a secure room like Confidential information (See Section 7-00-20). No security clearance is required to handle LOU information (for guidance regarding handling LOU or For Official Use Only (FOUO) information contact your OPDIV records management officer).

6-00-15 PRODUCTION AND REPRODUCTION OF CLASSIFIED INFORMATION

A. Only SDD approved automated information systems may be used to produce classified information derived from other classified sources. Word processors or computers must not be *used to* process classified information without authorization, in writing, from the Director, SDD.

B. Typewriter ribbons used in typing classified information must be treated as classified material'and safeguarded . after use or properly destroyed.

C. All classified documents shall be subject to the following reproduction restrictions:

1. The designated LCO shall be the only person authorized to reproduce classified documents.

2. The number of copies shall be kept to a minimum to decrease the risk of compromise and reduce storage costs. Any stated prohibition against reproduction must be strictly observed.

3. Reproduction equipment used by LCOs to reproduce classified documents must be specifically designated, and the following rules shall apply:

a. Make sure that the number of copies programmed actually are delivered.

b. Reproduce only the number authorized.

c. Account for all copies including originals before leaving the machine.

d. Ensure that all classification and any special markings appear on reproduced copies.

e. If the machine malfunctions, stay with it and send for any needed help. Correct the malfunction and verify that no classified pages remain in the machine.

4. All copies of classified documents reproduced for any authorized purpose are subject to the same controls prescribed for the document from which the reproduction is made.

5. HHS Form 208 (see Exhibit), must show the number and distribution of reproduced copies of all Top Secret and Secret documents, and any Confidential documents that bear special dissemination and reproduction limitations.

Subject: STORAGE

7-00-00 PURPOSE

This chapter provides instructions relating to the storage of classified information.

7-00-05 POLICY

Classified information must be stored under conditions that will provide adequate protection and prevent access by unauthorized persons. Whenever classified information is not under the personal control and observation of a cleared employee who has been authorized access to information based on a need-to-know, the information must be stored in a locked security container approved for such storage.

7-00-10 STANDARDS

A. The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information. Safe-type filing cabinets conforming to Federal specifications bear a Test Certification Label on the locking drawer attesting to the security capabilities of the container and lock.

B. The Director, SDD, may establish additional supplementary controls to prevent unauthorized access. The imposition of such additional controls should be based on the volume, nature, and sensitivity of the information to be protected in relation to other factors such as types of containers, presence of guards, vault-type space, and intrusion detection alarms.

7-00-15 STORAGE OF TOP SECRET INFORMATION

A. When not in use, Top Secret information must be stored in a GSA approved security container with a built-in, three-position, dial-type changeable combination lock. The security container shall be protected by an alarm system backed up by an armed response force.

B. In addition to the requirement specified above, admittance to the area in which Top Secret information is stored must be limited to cleared employees assigned to the area and to cleared persons who have been authorized access to the area. Persons not authorized access, but whose presence in the area is temporarily required, must be escorted and kept under constant observation.

7-00-20 STORAGE OF SECRET AND CONFIDENTIAL INFORMATION

When not in use, Secret and Confidential information must be stored in a manner and under the conditions prescribed for Top Secret information or in a non-alarmed, safe-type filing cabinet having an approved, built-in, three-position, dial-type changeable combination lock, or in a steel filing cabinet equipped with a steel lock bar secured by a GSA approved three-position, dial-type changeable combination. LOU information should be stored like Confidential information.

7-00-25 COMBINATIONS TO SECURITY CONTAINERS

A. Combinations to security containers may be changed by PSRs, LCOs, Custodians of Classified Files, other cleared employees authorized access to the information being stored, or by a bonded commercial locksmith or contractor. Combinations must be changed:

1. When the container is placed in use;

2. When an employee knowing the combination no longer requires access to the combination;

3. When a combination has been subjected to possible compromise:

4. At least once every 12 months: or

5. When the container is taken out of service.

B. Records of the combination of a lock used for the storage of classified information must be afforded protection equal to that given the highest level of the classified information stored therein. Combinations must be memorized, recorded on Standard Form (SF) 700, Security Container Information (see Exhibits), and stored in another approved security container. PSRs must establish procedures for the secure storage of the SF 700 combination envelope.

C. SF 700 must be completed to show the names, addresses, and telephone numbers of employees who are to be contacted if the security container, to which the form pertains, is found open and unattended by an authorized person. Part 1 of the form must be attached to the inside of the container so it is visible if the container is open. Parts 2 and 2A of the SF 700 are used to record the security container's combination which is inserted into the envelop portion for secure storage. Part 2 and 2A of each completed copy of SF 700 must be classified at the highest level of classification of the information in the security container. A new SF 700 must be completed each time the combination to the security container is changed.

D. Access to the combination shall be given only to those employees who are cleared and authorized access to the classified information stored in the container. Knowledge of combination must be limited to the minimum number of employees necessary for operating purposes.

7-00-30 RELOCATION OF SECURITY STORAGE CONTAINERS

When an office having custody of classified information physically moves from one office or building to another, the classified information may be retained in the approved security container. However, the custodian or other cleared employees must maintain constant supervision of the container during the move. The PSR must be notified prior to relocating a security container used for the storage of classified information and may decide to temporarily store the classified information in another approved container.

7-00-35 RESTRICTIONS ON USE OF STORAGE CONTAINERS

A. Security containers used for the storage of classified information should not be routinely used for the storage of cash, checks, weapons, controlled drugs, precious metals, personal items, or other items susceptible to theft.

B. Security storage containers should be located in an office occupied by an LCO or Custodian of classified Files but must not be located in office storage areas, corridors, hallways, or in the vicinity of unsupervised exits.

7-00-40 SAFE OR CABINET SECURITY RECORD

A. SF 702, Security Container Check Sheet (see Exhibits), must be placed on the outside of each container holding classified information to record each time the container is opened and closed. The person opening and closing the container must write in the time of each operation and initial the form. There is also space on the SF 702 for the initials of the person performing the daily check for closure of the container. Someone must perform this check at the end of each work day to assure the container is locked.

B. Each SF 702 can be used for four months and should be destroyed whenever a new one is put into use.

c. SF 701, Activity Security Checklist (see Exhibits), also can be used to provide for additional assurance that security containers have been locked and other end of the day security measures have been taken. This form must be used in a security office or other locations where there are a number of security containers holding a large quantity of national security information.

Subject: TRANSMISSION

8-00-00 PURPOSE

The purpose of this chapter is to provide instructions governing the transmission of classified information.

8-00-05 TRANSMITTAL OUTSIDE DHHS BUILDING

A. All classified information transmitted outside a DHHS building must be enclosed in opaque inner and outer covers (e.g. sealed envelopes or wrappings). The inner sealed opaque cover must show the completed forwarding and return address and be clearly marked on both sides, top and bottom, with the highest security classification of its contents. The outer sealed opaque cover must be addressed in the same manner but must not bear any classification markings or other indication that classified information is enclosed. Markings on the inner cover must not show through the outer cover. Classified information must be addressed to a person known to have a security clearance. The identity of the intended recipient must be indicated on an attention line on the inner cover or on an attention line placed in the letter/memorandum of transmittal.

B. Material used for packaging must be of such strength and durability so as to provide protection in transit and to prevent items from breaking out of the covers. Bulky packages must be sealed with tape laminated with asphalt and containing rayon fibers or nylon filament tape, or equivalent.

8-00-10 TRANSMITTAL WITHIN DHHS BUILDING OR BUILDING COMPLEX

A. All classified information transmitted between offices within a DHHS building or complex of buildings should be placed in a sealed opaque cover marked with the level of classification. All documents must have cover sheets attached, i.e., Standard Forms 703, 704, or 705.

Classified information carried in these covers must be promptly hand-carried by employees possessing a security clearance commensurate with the highest level of classification of the information being hand-carried.

B. Whenever security mail is opened in error by employees not authorized to open such mail, the envelope or container must be immediately resealed and marked "OPENED IN ERROR" (time and date) by (employee's name), and then promptly hand-carried to the proper recipient or LCP. In any such circumstances, it is the responsibility of the employee to ensure that the envelope or container is properly stored in the manner prescribed by Chapter 7-00 until personal delivery can *be* accomplished.

8-00-15 RECEIPT FOR CLASSIFIED INFORMATION

HHS Form 25, Classified Document Receipt (see Exhibits), must be completed for all transmissions of Top Secret and Secret information. The receipt shall be attached to or enclosed in the inner cover. The sender must retain his/her returned copy signed by the recipient as proof of the official transfer of the document(s): Top Secret receipts have a five year retention period, with two years for Secret. The transmission of Confidential information does not require a receipt but may be used for further accountability.

8-00-20 ACCOUNTABILITY PROCEDURES PRIOR TO TRANSMISSION

All classified material designated for transmission, regardless of designation, must be processed through the LCP, to include the TSCO if the information is Top Secret. The LCO must ensure that document accountability is maintained on HHS Form 208, that required receipts are attached and correct, and that the packaging meets requirements.

8-00-25 METHODS *OF* TRANSMISSION

A. Top Secret Information. Top Secret information must only be transmitted by one of the following methods:

1. Hand-carried by Top Secret cleared and designated employee (courier) within the United States and its territories provided the information is delivered before the close of business on the same day;

2. Cryptographic systems (automated information systems, secure telephone, secure facsimile systems, etc.) approved for the transmission of classified material at the appropriate level by the Director, NSA and authorized by the Director, SDD;

3. The Armed Forces Courier Service (ARFCOS); or

4. Diplomatic pouch through the Department of State Diplomatic Courier System,

B. Secret Information. Secret information must be transmitted by:

1. Any of the means approved for the transmission of Top Secret information, except that the courier only needs to be cleared at the *Secret* level;

2. United States Postal Service (USPS) reaistered mail within and between the United States and its territories;

3. U.S. registered mail through Military Postal Service facilities outside the United States and its territories provided that the information does not at any time pass out of the control of the United States Government and does not pass through a foreign postal system or any foreign inspection;

4. A cleared and designated employee (courier) on scheduled commercial passenger aircraft within and between the United States and its territories subject to the procedures and restrictions set forth in Section 8-00-30B, below;

5. Information classified up to Secret may be transmitted by a DHHS messenger provided the classified document is in a double envelope, as specified in Section 8-00-05 above, and handled like U.S. registered mail with a receipt attached to the outer envelope.

c. Confidential Information. Confidential information may be transmitted by the means approved for the transmission of Top Secret or Secret information and by the USPS certified mail within and between the United States and its territories. Outside of these areas, Confidential information must be transmitted

only as is authorized for Top Secret or Secret information.

8-00-30 HAND-CARRYING CLASSIFIED INFORMATION BY COURIERS

A. Restrictions. Designated employees (couriers) may be authorized to hand-carry classified information outside of DHHS buildings subject to the following conditions:

1. The employee's security clearance must be the same or higher than the classification of the material being carried.

2. The storage provisions of Chapter 7-00 shall apply at all stops en route to the destination, unless the information is retained in the personal possession and constant surveillance of the employee at all times. The hand-carrying of classified information on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage in a Federal Government installation or a cleared United States contractor's facility:

3. When classified information is carried in a private, public, or Government conveyance, it must **not** be left in automobiles, hotel rooms, hotel safes, aircraft or train compartments, private residence, or public lockers;

4. Employees must carry their DHHS identification card or badge whenever carrying classified information outside of DHHS buildings.

5. The LCO must be informed each time classified information is to be carried by an employee so that the LCO can designate that employee as a courier. The LCO shall authorize, orally or in writing, the use of the designated employee as a courier and assure the employee has been briefed in courier responsibilities as detailed in this chapter.

B. Aboard Commercial Passenger Aircraft.

1. Classified information may be hand-carried aboard commercial passenger aircraft within and between the United States and its territories only in an emergency when the information is not available at the destination and because of an urgent situation

there is neither time nor means available to properly transmit the information by other methods stated in Section 8-00-25. Permission to hand-carry classified information aboard such aircraft shall be granted on a case-by-case basis by the the Director, SDD.

2. Under no circumstances will any level of classified information be hand-carried across international boundaries.

3. Procedures for hand-carrying classified information aboard commercial passenger aircraft is as follows:

   a. All the provisions of Section 8-00-30 will be strictly complied with.

   b. The person hand-carrying the classified information will be designated as a courier, in writing, by the Director, SDD.

   c. The classified information being hand-carried will contain no metal binding and will be doubled-wrapped, addressed and sealed as out lined in Section 8-00-05. The envelope will be placed in a briefcase or other piece of carry-on luggage.

   d. The person authorized to hand-carry the classified information will process through the routine airline ticketing and boarding procedures. The briefcase or carry-on *luggage* will be routinely offered for opening for inspection, if requested. The screening officials may check envelope by x-ray machine, *flexing,* feel and weight, without opening the sealed envelope. Airport screening officials may be shown proper identification and the courier authorization documentation to avoid having the envelope opened.

e. If airline screening officials still insist on opening the envelope, the person will ask to see a **Federal** Aviation Administration **(FAA)** field office representative. If the FAA representative still insists on opening the envelope after being shown proper identification and the courier authorization documentation, the person will not attempt further boarding but shall make alternate arrangements for completing the travel. Under **no** circumstances should the courier allow the envelope to be opened.

Subject: DISPOSAL AND DESTRUCTION

9-00-00 PURPOSE

The purpose of this chapter is to provide instructions governing the disposal and destruction of classified information.

g-00-05 DISPOSAL OF CLASSIFIED INFORMATION

A. Early disposal/destruction of unnecessary classified information can assist in preventing security violations, reducing security costs, and providing better protection for classified information that needs to be retained for some official purpose.

B. Because DHHS does not have original classification authority, most of the DHHS classified holdings are non-permanent or non-record classified information, such as copies of classified documents from other agencies intended solely for reference purposes. These documents should be destroyed as soon as they have served their official intended purpose, have been superseded, or are obsolete. Retain those classified documents which contain current policy information. other documentary record materials which are classified must be disposed of in accordance with General Records Schedule published by the National Achieves and Records Administration.

C. Since almost all classified information in possession of HHS employees is originated by another agency, the originating agency will probably have a copy of the classified document if our copy is later Uestroyed and we subsequently have a need to review it. Proper documentation in the accountability records, HHS Form 208 (see Exhibits), will allow for tracking the document back to the originating agency.

9-00-10 DESTRUCTION OF CLASSIFIED INFORMATION

A. Documents containing classified information must be destroyed in a manner to preclude recognition

or reconstruction of the classified information in whole or in part. Heads of offices or organizations **(e.g.,** division directors) in possession of classified information must establish internal procedures for the proper destruction of classified information. Such procedures must ensure that adequate destruction methods are used, classified information is protected during transport to the destruction area, adequate records are maintained, and the destruction is properly witnessed.

B. 'Destruction of classified information must be accomplished by one of the following methods:

1. **Shredders** may be used for the destruction of classified information provided the shredders are listed on the GSA Federal Supply Schedule as approved security destruction devices. These approved shredders cross-cut the strips to a size of approximately **1/32"** in width and **1/2"** in length.

2. The burning method, when approved by the PSR, may be used for the destruction of classified information. The documents containing the information must be burned completely and no unburned pieces shall remain or be allowed to escape by wind ***or*** draft.

3. Classified information may be destroyed also by the pulping, disintegration, or pulverizing method. Such methods of destruction and the equipment used for such must be approved by the PSR.

C. Classified material awaiting destruction must be properly stored in an approved security storage container. Boxes, bags, sealed envelopes, or other like containers used for the collection and transportation of classified material must provide adequate safeguards to prevent the loss of the material. When transporting classified material to a destruction area such containers must not be left unattended.

D. The lower portion of **HHS** Form 25 is the official Certificate of Destruction and must be used as a receipt to indicate the destruction of Top Secret

and Secret information. The form must include a full unclassified description of the material, the date of actual destruction, and witness to the actual destruction. For Top Secret information two employees must sign the form, one as the destruction official and the other as the witnessing official. Just the destruction official is required to sign for Secret information. Employees who conduct and witness the destruction of classified information must possess a security clearance commensurate with highest level of information being destroyed. Destruction certificates are not required for Confidential information unless prescribed by the agency that originated the information.

HHS Form 25, used for the destruction of Secret or Confidential information, must be maintained for a minimum of **two** years. When used for the destruction of Top Secret information, the form must be maintained for five years and then destroyed. These destruction certificates can be maintained at any location approved by the PSR.

E. Classified waste material must be destroyed as soon as practical by one of the approved destruction methods. This applies to all waste material containing classified information, such as preliminary drafts, carbon sheets, fabrics or plastic typewriter ribbons, stencils, stenographic notes, working papers, and similar items. Employees who are designated to destroy classified waste material must possess the appropriate security clearance and the need-to-know the information. Destruction certificates are not required for classified waste material. Pending destruction, all classified waste material must be stored in an approved security container.

F. Typewriter and automated information systems equipment ribbons used in transcribing classified material must be stored in an approved security container when *not* in use or until the ribbon is cycled through the typewriter or printer a sufficient number of times to obliterate information contained thereon. Normally this can be accomplished if the ribbon is completely overprinted five times in all ribbon typing or printing positions. **Any** ribbon which remains substantially stationary (that is, receives at least five consecutive impressions) shall be treated as unclassified. Ribbons which are not obliterated must be destroyed as other classified materials.

G. Classified messages, which are generated during a classified exercise, need not be processed into an accountability system or brought under control if they are destroyed within 30 *calendar* days after Completion Of the exercise. Certificates of destruction are not required for these messages. However, classified exercise messages that are retained beyond the 30-day period will be controlled and destroyed in the same manner as other accountable classified messages. These classified messages, awaiting destruction, must be safeguarded and stored in the manner stated in Chapter 7-00.

g-00-15 EMERGENCY PROTECTION, REMOVAL, AND DESTRUCTION

A. In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, classified information must be protected either by placing it in a locked approved security container, relocating it to another office/organization for proper storage, or by properly destroying the information. Employees who are away from their office and have classified information in their possession at the time of an emergency must assure that such information is properly safeguarded or destroyed.

B. Only the Secretary or designee may order the Safe removal *or* emergency destruction of U.S. and NATO classified material. Upon receipt of the order, the Director, SDD, Will immediately notify the LCOs Of all affected offices and inform them of the emergency plan. In all situations, highest priority for removal or destruction will be given to the highest level of classified material, e.g., Top Secret Special Access is first priority, then *regular* Top Secret, then NATO Secret, then regular Secret, etc.

C. The PSR must ensure that all offices in possession of classified information must have plans for the emergency protection, removal, and destruction of the information. The location and identity of the information to be destroyed, priorities for destruction, persons responsible for destruction, and recommended place and method of destruction must be predetermined and persons fully indoctrinated. The Director, SDD, can assist in the preparation of such plans.

D. A copy of the written plans for emergency handling of classified information should be filed in a readily accessible location inside each security container being used for the storage of classified information.

Subject: SECURITY AWARENESS, CONTACT WITH CERTAIN FOREIGN NATIONALS, AND FOREIGN TRAVEL

10-00-00 PURPOSE

This chapter provides PSRs and employees with instructions relating to security awareness concerns regarding contact with certain foreign nationals and specific foreign travel requirements..

10-00-05 SRCURITY AWARENESS AND REPORTING CONTACT WITH CERTAIN FOREIGN NATIONALS

A. NSDD 197, signed by the President on November 1, 1985, calls for the establishment of procedures which will:

1. Create and maintain a formalized security awareness program designed to ensure that employees are aware of the potential threat to the Department's classified, proprietary, and sensitive information from foreign sources, whether overt or covert. This program must include a periodic formal briefing of the threat posed by hostile intelligence services.

2. Provide for the reporting, under defined circumstances, of the employee contacts with nationals of certain designated foreign countries or political entities.

B. The reporting requirements of NSDD 197 specifically apply only to HHS employees who, through their job functions or access to national security or sensitive information or technology, invite targeting or exploitation by foreign intelligence services. The unauthorized release of sensitive information or technology and contacts with foreign nationals of high risk designated countries must be reported in accordance with subparagraphs C and D below.

C. HHS employees, who have a security clearance or who could be targeted for exploitation because of their position or access to sensitive information, have certain reporting requirements. They must report all contacts with individuals of any nationality, either within or outside the scope of the their official activities, in which:

1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

2. They are concerned that they may be the target of an attempted exploitation by a foreign entity.

D. These employees must also report all contacts with nationals of high risk designated countries (see Section 10-00-15) which appear to:

1. Indicate an attempt or intention to obtain unauthorized access to classified, proprietary, or sensitive information;

2. Offer a reasonable potential for such access; or

3. Indicate the possibility of continued professional or personal contacts.

E. Employees subject to these reporting requirements must submit a written report to the PSR within five days of the occurrence. Employees in doubt as to whether a written report is required should call their PSR or the Director, SDD. The report should be as specific as possible regarding the facts about the contact, including the identity of the hostile or potentially hostile source. The PSR must promptly notify the Director, SDD, about the employee's report and the Director, SDD, will notify the FBI, if deemed necessary.

F. Definitions of Certain Words and Terms.

1. "Contact" means any form of meeting, association, or communication regardless of who initiated the contact or whether it was for social, official, or private purposes. This includes any contact in person, by telephone, letter, radio, or any form of communication, even if no official information was discussed or requested.

2. "Proprietary information" is that business information which was developed by the private sector, and furnished to the Department with the expectation or *condition* that it be protected. Information of this type referred to as trade secret material requires protection against unauthorized disclosure under Title 18, U.S.C., Section 1905 and Title 21, U.S.C., Section 3315.

3. "Sensitive information" is that unclassified information the loss, exploitation, or unauthorized disclosure of which could impair the national security or foreign relations of the U.S., or affect the ability of the Department to meet stated goals and/or objectives of national interest. Sensitive information also includes that privileged information which qualifies as an exemption under the Freedom of Information and the Privacy Act of 1974, and other information provided by another U.S. Department or Agency with the expectation or condition that the information will be protected. Sensitive information does not include information in the public domain or that given out under the auspices of bilateral agreements.

G. None of the reporting requirements contained in this chapter is intended to replace existing agreements between the Department of State and DHHS components to report suspicious activities. These requirements are in addition to those already established. Employees in Special Access Programs have additional reporting requirements (See *Section* 10-00-10 below).

10-00-10 FOREIGN TRAVEL REQUIREMENTS

A. HHS employees who travel to foreign countries to attend international, scientific, technical, medical, or other professional meetings or conferences may come into contact with representatives of high risk designated countries. These contacts must be reported in accordance with Section 10-00-05 above.

B. KHS employees, who have Top Secret clearances for participation in a highly sensitive Special Access Program, must report to the Director, SDD, their intent to travel to or through *any* of the high **risk** designated countries listed in Section **10-00-15.** They must report this information, orally or in writing, in advance of the planned trip, whether on private or official business, so that they can **be** afforded a defensive security briefing. Other **HHS** employees may request such a briefing from their PSR who can obtain briefing materials from the Director, SDD.

C. This defensive security briefing is in addition to any normal Department of State briefing provided to government employees traveling on official business. The briefing will cover safeguarding requirements for classified and other sensitive information and will include security awareness guidelines.

D. When any employee in a Special Access Program returns *from* travel to or through any of the high **risk** designated countries, he/she must contact the Director, SDD, for **a** security debriefing. Other employees traveling to these designated countries should report any incidents or concerns to their PSR. The employees should be advised that it is essential to report any suspected attempts to **obt** in classified, proprietary, or sensitive information, or efforts to recruit, compromise, harass, or entrap the employee. such information received by a PSR must be promptly reported to the Director, SDD.

10-00-15 DESIGNATED COUNTRIES

A. These are the high risk designated countries for which there are certain reporting and travel requirements (current as of date of issuance of this manual):

Afghanistan
Albania
Angola
Armenia*
Azerbaijan*
Belarus*
Bulgaria
Cuba
Estonia*
Ethiopia
Georgia*
Iran
Iraq
Kampuchea (formerly Cambodia)
Kazakhstan*
Kurile Island and south Sakhalin (karafuto)
Kyrgystan*
Laos
Latvia*
Libya
Lithuania*
Moldova*
Mongolian People's Repulic (Outer Mongolia)
Nicaragua
North Korea
People's Republic of China (including Tibet)
Romania
Russia*
South Yemen
Tadjikistan*
Turkemistan*
Ukraine*
Uzbekistan*
Vietnam
Yugoslavia (including Croatia and Serbia)

* Formerly part of the Union of Soviet Socialist Republics (USSR)

Subject: OTHER SPECIAL SECURITY PROGRAMS

11-00-00 PURPOSE

The purpose of this chapter is to provide general information and instructions regarding other special security programs that could be of interest to some Department officials who have national security responsibilities.

11-00-05 POLICY

It shall be the policy of the Department to establish, where an identifiable need exists, the special security programs described in this chapter and to fully comply with security directives issued by the Federal agencies identified for each program area.

11-00-10 COMMUNICATION SECURITY (COMSEC) AND SECURE VOICE

A. COMSEC means protective measures taken to deny unauthorized persons information derived from telecommunications or to assure its authenticity. Such protection results from the application of various security measures, including crypto-security, transmission and emission security, and certain physical security measures needed for protection of COMSEC information and materials. The Director, National Security Agency (NSA), is responsible for issuing COMSEC instructions for all approved cryptographic systems.

B. National security information must not be discussed over, or otherwise transmitted or processed by, any form of telecommunications unless approved measures are taken to protect the information. COMSEC is the only system of security measures used to protect classified information utilizing cryptographic keying material and equipment.

C. The Secure Telephone Units (STU) III developed by the NSA provide, by use of COMSEC measures, secure voice transmission capability during discussions involving the highest levels of classified national security information and other highly sensitive/proprietary information.

D. Upon determining the need for any COMSEC support or secure voice transmission system capability, the PSR should submit a request to the Director, SDD. The request shall contain all pertinent circumstances relating to the type of support or system needed.

E. Specific cryptographic access requirements are required for some HHS employees, such as COMSEC Custodians, because of their on-going need to handle certain classified cryptographic information. The Director, SDD, is responsible for processing and issuing crytographic accesses which meet the policy requirements of the National Telecommunications and Information Systems Security Committee.

11-00-15 NORTH ATLANTIC TREATY ORGANIZATION (NATO)

A. The U.S. national security authority responsible for the security of NATO classified information is the "United States Security Authority for NATO Affairs (USSAN)." The USSAN is the Secretary of Defense. The USSAN has established under the Secretary of the Army a U.S. national registry known as the Central United States Registry (CUSR). The Chief, CUSR, is authorized to establish and disestablish U.S. NATO subregistries, release NATO documents to U.S. departments and agencies, and to conduct inspections of all subregistries and control points.

B. NATO security procedures governing the protection and handling of NATO classified information in the possession of this Department are contained in USSAN Instruction l-69, Implementation of NATO Security Procedures. The instruction, which contains some NATO classified information, has been assigned an overall classification of CONFIDENTIAL.

C. A NATO SECRET subregistry, established in accordance with USSAN Instruction l-69, is located in the Office of the Director, SDD. The Director, SDD, is authorized to establish NATO SECRET Control Points where an operational need exists to maintain certain NATO SECRET, CONFIDENTIAL, or RESTRICTED information.

Written justification relating to the need of a control point shall include a description of the classified NATO documents needed, and be furnished to the Director, SDD. Formal access to NATO classified information may be authorized only when the Department has authorized an employee access to U.S. information of an equivalent classification, and the employee has been given a NATO security briefing.

11-00-20 SPECIAL ACCESS PROGRAXS

A. A Special Access Program is a program imposing "need-to-know" or access controls beyond those normally provided for access to Top Secret, Secret, or Confidential information. Such a program includes, but is not limited to, special clearance, investigative and adjudication requirements, special designation of officials authorized to determine "need-to-know", and special classified lists of persons granted Sensitive Compartmented Information (SCI) clearance.

B. Special Access Programs are created only by a Federal agency that possesses original classification authority. The programs are compartmentalized to further restrict access to those who "need-to-know" certain national security information. The Director, SDD, is responsible for processing all requests for access to Special Access Programs and assuring that special security requirements are met.

Exhibit 12-00-A
National Security Information Manual
HHS Transmittal 92.01

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICE:. CLASSIFIED DOCUMENT RECEIPT				DATE	
TO:	FROM: (Return Address)				
. DESCRIPTIONS OF DOCUMENT(S)	CLASS.	DATE OF DOCUMENT	CONTROL NUMBER	NO. OF CYS	CY NO.
RECEIPT OF ABOVE DOCUMENT(S) IS ACKNOWLEDGED				DATE	
PRINTED NAME AND TITLE	SIGNATURE				
CERTIFICATE OF DESTRUCTION					
I CERTIFY THAT THE DOCUMENT(S) LISTED ABOVE WERE DESTROYED				DATE	
PRINTED NAME, TITLE AND SIGNATURE OF DESTRUCTION OFFICIAL	PRINTED NAME, TITLE AND SIGNATURE OF WITNESSING OFFICIAL				

HHS FORM 25-(RC 12-85) 1 RETURN TO SENDER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

OFFICE OF THE SECRETARY

REQUEST FOR SECURITY CLEARANCE

For Access to Classified National Security Information

DATE

☐ CRITICAL-SENSITIVE POSITION ☐ NONCRITICAL-SENSITIVE POSITION

INSTRUCTIONS: Submit in duplicate for headquarters employees, and in triplicate for employees located in the field, with a cover memorandum. Any security, loyalty or misconduct information, and any information tending to show that this employee may be other than completely reliable and entirely trustworthy, must be brought to the attention of the Director, Office of Investigations and Security

It is requested that a security clearance be granted to permit access to information and material classified up to and including *(Check one)*

☐ Confidential ☐ Secret ☐ Top Secret for the following:

Name	Title, Division, Bureau, Agency	
		DOB
		GRADE

Justification:

	Signature	Title
RECOMMENDED BY		
CONCURRENCE		Security Representative

CERTIFICATE OF SECURITY CLEARANCE

This is to certify that the following named individual has been cleared for access to classified material or information up to and including _____ on a need-to-know basis.
Clearance is based on

NAME	DATE

The Security Representative is responsible for Physical Security Indoctrination of employee upon notification of clearance.

SIGNATURE OF DIRECTOR, PERSONNEL SECURITY AND DRUG TESTING PROGRAM DIVISION, ASPER

HHS-207 (Rev. 3/75)

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD

CONTROL NUMBER	NO. OF CYS.	CLASS	CLASSIFIED BY	DATE OF DECL/DG	DATE OF DOCUMENT	DATE RECEIVED	RECEIVED FROM	DESCRIPTION OF DOCUMENT(S)	DISPOSITION

HHS Form 208 (Rev. 12/85)

Page ____ of ____ Pages

(BLANK)

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN AND THE UNITED STATES

(Name cl Individual - Printed or typed)

1 Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Execuuve order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such informauon in the interest of national security I understand and accept tha: by being granted access to classified information, special confidence and trust shall be placed in me by the United Stales Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information. including the procedures to be followed in ascertaining *whether* other persons to whom I contemplate disclosing this informauon have been approved for access to it. and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified informauon to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it: or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the informauon is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. 1 have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthonred disclosure of classified information by me may constitute a violation, or violations. of United States criminal laws, including the provisions of Sections 641. 793, 794. 798, and '952, Title 18, United States Code. *the provisions of Section 783(b), Title SO, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982.1 recognize that nothing in thls Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties. remunerations. and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including. but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the propeny of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security ckarance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request. I understand that this may be a violation of Section 793. Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government. I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality. waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (SO U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents). and the statutes which protect against disclosure that may compromise the national security. including Sections 641. 793. 794. 798. and 952 of Title 18. United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling

(Continue on reverse.)

1 1. I have read this *Agreement* carefully and my questions. if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See Notice below)

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or print)

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or print)		NAME AND ADDRESS (Type or print)	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE

NAME OF WITNESS (Type or print)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S C 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397 Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT

SECURITY CONTAINER INFORMATION INSTRUCTIONS	1 AREA OR POST (if required)	2 BUILDING (if required)	3 ROOM NO
1. COMPLETE PART 1 AND PART 2A (ON END OF FLAP) 2 DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER 3 MARK PARTS 2 AND 2A WITH THE HIGHEST CLASSIFICATION STORED IN THIS CONTAINER 4 DETACH PART 2A AND INSERT IN ENVELOPE 5 SEE PRIVACY ACT STATEMENT ON REVERSE	4 ACTIVITY (DIVISION, BRANCH, SECTION OR OFFICE)		5 CONTAINER NO
	6 MFG & TYPE CONTAINER	7 MFG & TYPE LOCK	8 DATE COMBINATION CHANGED
	9 NAME AND SIGNATURE OF PERSON MAKING CHANGE		

10 Immediately notify one of the following persons, if this container is found open and unattended

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE

1. ATTACH TO INSIDE OF CONTAINER

700-101
NSN 7540-01-214-5372

STANDARD FORM 700 (8-8
Prescribed by GSA/ISOO
32 CFR 2003

WARNING

WHEN [illegible] THIS ENVELOPE MUST BE SAFEGUARDED IN ACCORDANCE WITH APPROPRIATE SECURITY REQUIREMENTS

DETACH HERE

COMBINATION

[illegible]

WARNING

[illegible]

2A INSERT IN ENVELOPE

SF 700 (8-8[illegible]
Prescribed by GSA/ISOO
32 CFR 2003

ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR

Irregularities discovered will be promptly reported to the designated Security Officer for corrective action

Statement

I have conducted a security inspection of this work area and checked all the items listed below

TO (If required) FROM (If required) THROUGH (If required)

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1 Security containers have been locked and checked.																															
2 Desks, wastebaskets and other containers are free of classified material																															
3 Windows and doors have been locked (where appropriate)																															
4 Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored																															
5 Security alarm(s) and equipment have been activated (where appropriate)																															

INITIAL FOR DAILY REPORT

TIME

701-101
NSN 7540 01 213 7899

*U.S. GPO: 1987-181 247/60090

STANDARD FORM 701 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

SECURITY CONTAINER CHECK SHEET

TO (if required) | THRU (if required)

CERTIFICATION

I CERTIFY. BY MY INITIALS BELOW. THAT I HAVE OPENED. *CLOSED OR CHECKED THIS SECURITY CONTAINER* IN ACCORDANCE *WITH PERTINENT* AGENCY *REGULATIONS AND OPERATING INSTRUCTIONS.*

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE—REVERSE FOLD FOR FULL USE OF BOTH SIDES—FOLD HERE

SECURITY CONTAINER CHECK SHEET

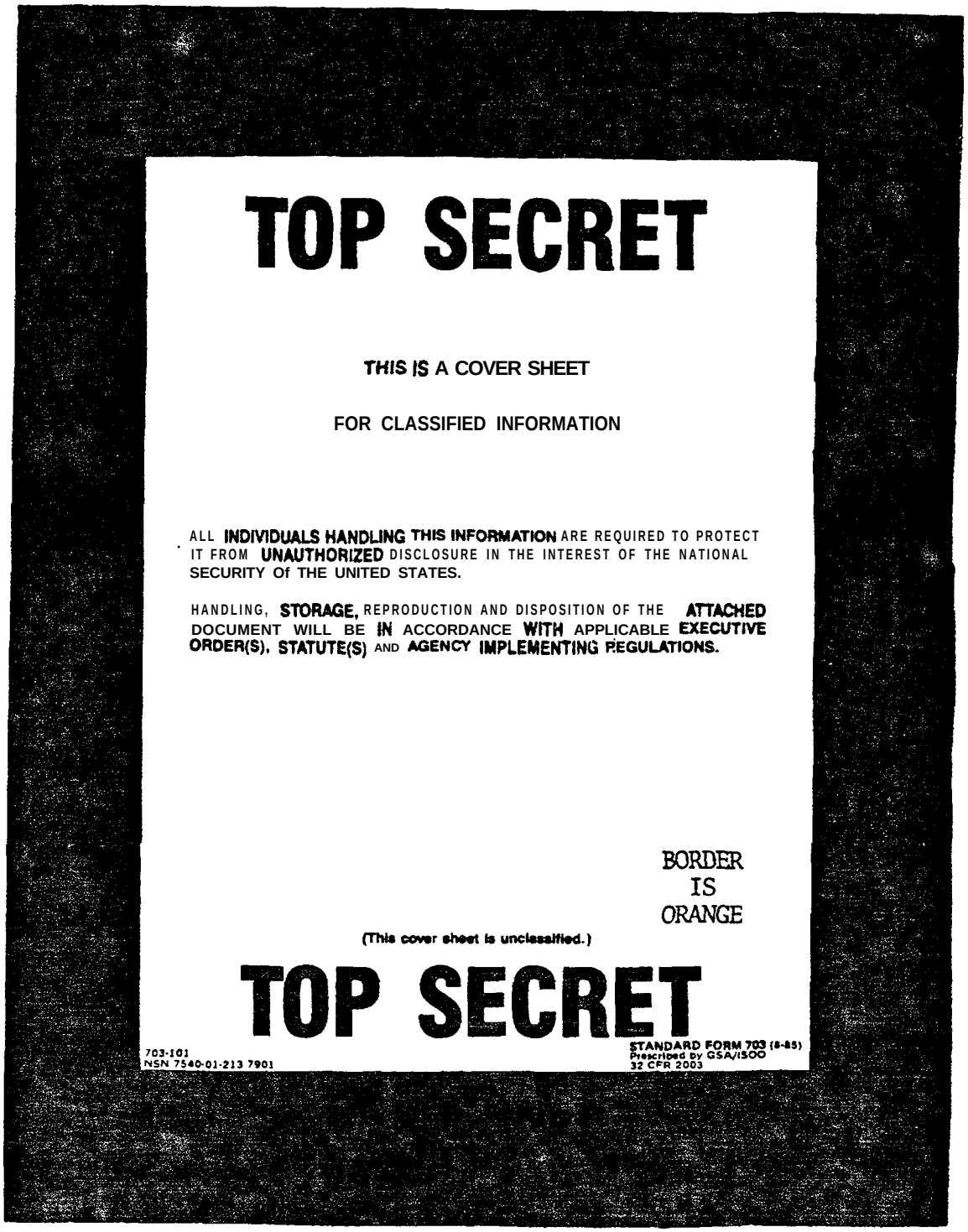
FROM | ROOM NO | BUILDING | CONTAINER NO

CERTIFICATION

I CERTIFY, BY *MY* INITIALS *BELOW, THAT I HAVE* OPENED. *CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.*

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME



TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY Of THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

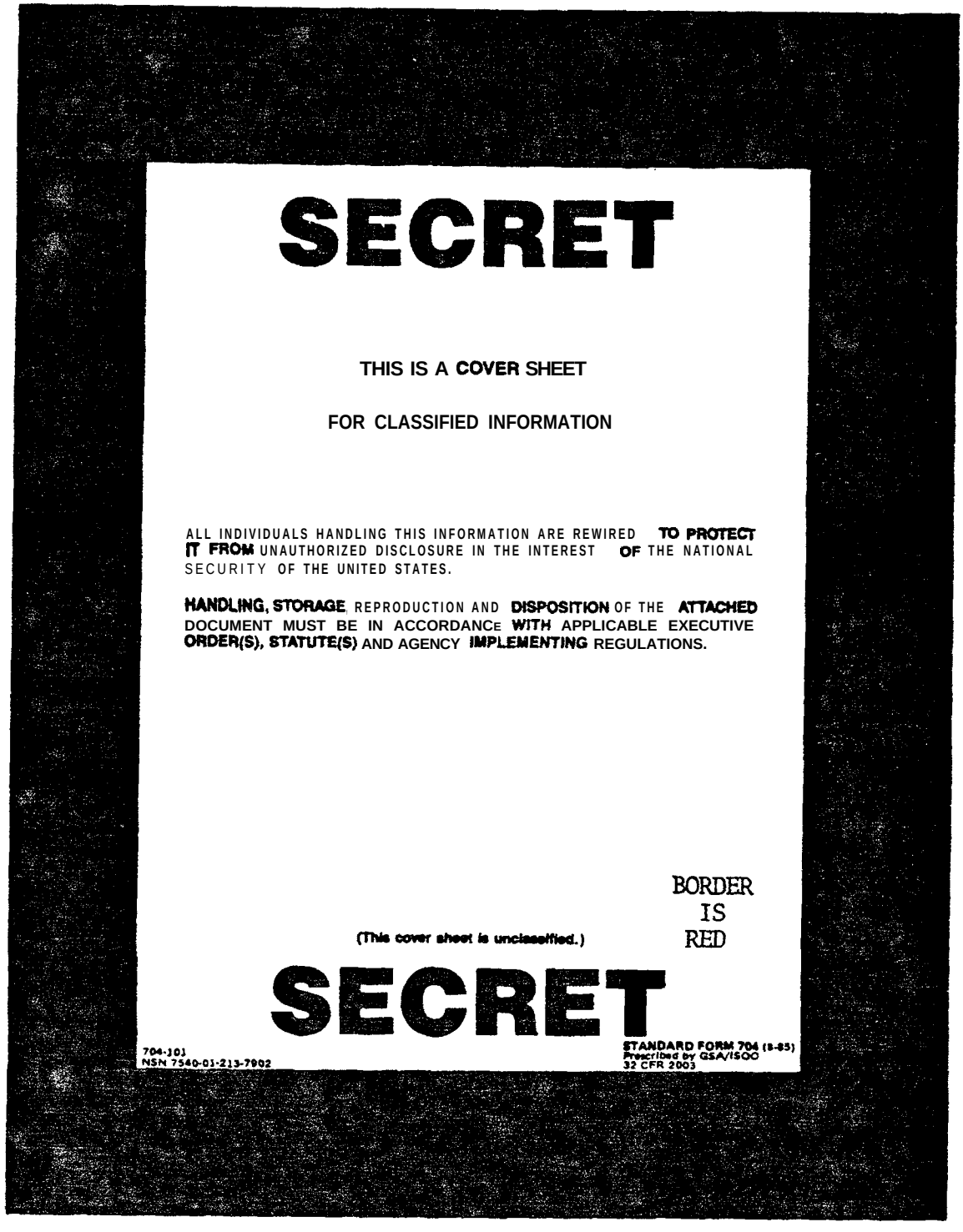
BORDER
IS
ORANGE

(This cover sheet is unclassified.)

TOP SECRET

703-101
NSN 7540-01-213 7901

STANDARD FORM 703 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003



SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REWIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

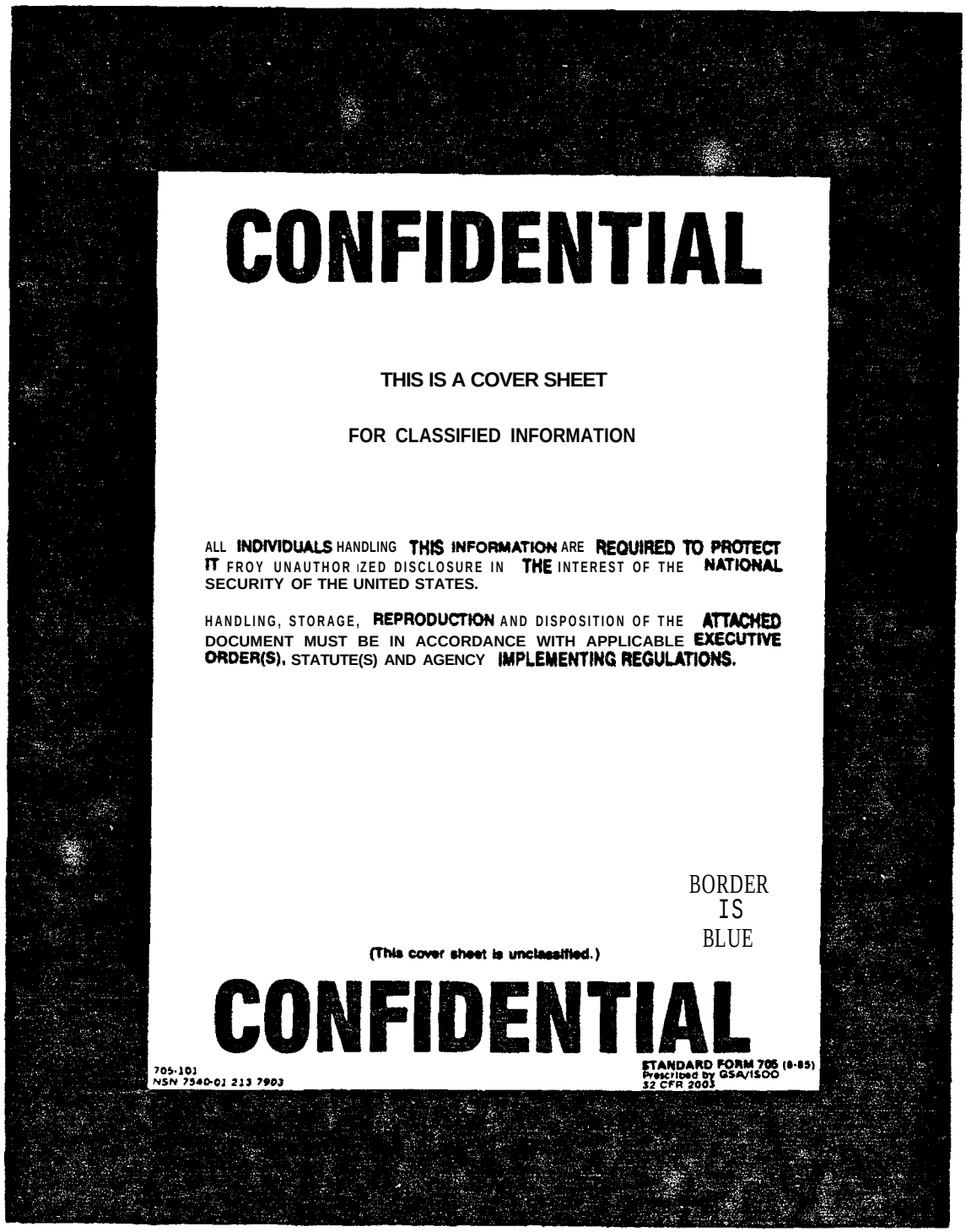
BORDER IS RED

(This cover sheet is unclassified.)

SECRET

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003



CONFIDENTIAL

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROY UNAUTHOR IZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

BORDER
IS
BLUE

(This cover sheet is unclassified.)

CONFIDENTIAL

705-101
NSN 7540-01 213 7903

STANDARD FORM 705 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003