United States International Trade Commission

Handbook
For
National Security Information
Version 1.0

Office of Security and Support Services
500 E Street, SW
Washington, DC 20436

December 5, 2014

A Procedural Handbook for the Proper Safeguarding of Classified National Security Information (NSI)

Table of Contents

Contents

Introduction

In accordance with Executive Order 13526, the Information Security Oversight Office implementing directive, 32 C.F.R. Part 2001, and as an accompaniment to the USITC Directive 1340 on Information Security, this handbook implements policy and establishes procedures for the marking, control, safeguarding, storage, destruction, transmission, and transportation of classified National Security Information (NSI). This handbook is intended to specifically address typical USITC procedural topics, and is not all inclusive of the requirements contained in the above referenced documents.

Access to NSI

Access to classified materials at the Commission shall be limited to authorized persons. The term "authorized person" means a person who has a favorable determination of eligibility for access to classified information (*i.e.*, a security clearance), has signed an approved nondisclosure agreement, and has a need-to-know.

The Investigative Process

- The Personnel Security Officer (PSO) will provide access to the on-line Electronic Questionnaires for Investigations Processing (e-QIP) system to new-hire candidates to begin the security investigation process if required. A candidate will have 14 days to complete the e-QIP security process and schedule an appointment for fingerprinting.
- New employees may be granted interim access to NSI after a favorable review of preliminary checks and a background investigation has been initiated.
- Interim access will only be granted after the following criteria have been met:
  - The Office of Human Resources has provided an OF 8 Position Description with a complete description of the sensitive duties and a Position Designation with a designation level of Tier 2 or higher.
  - The employee has submitted an OF 306, resume, fingerprints, and e-QIP.
  - The preliminary checks have been reviewed and adjudicated favorably.
- Employees who complete the security investigation process prior to their entry on duty date may be eligible for access on their first day of work at USITC.

Entering on Duty

- Office Directors will provide an employment candidate's appropriate and relevant position information to the Office of Human Resources prior to the candidate's arrival, including the enter-on-duty date.
- The Office of Human Resources runs the Office of Personnel Management Automated Designation Tool to determine the appropriate investigation and risk level.
- If access to classified information is a requirement for the candidate's position, the PSO will notify the NSI Program Manager after requisite checks have been reviewed and adjudicated favorably.

- The NSI Program Manager will then contact the candidate to schedule a security briefing which includes review and signing of the Standard Form 312. Electronic signatures on the SF 312 are prohibited.

Need-to-Know

Need-to-know is the determination by a holder of NSI that a prospective recipient requires access to specific classified information in order to perform their job functions. Need-to-know is an ongoing requirement that must be determined by the holder of the classified information each time NSI is disclosed. In addition, the holder must verify the recipient's identification and security clearance through the NSI Program Manager, if not already known. No employee has a right to gain access to NSI solely by virtue of title, position, or level of security clearance. Office directors must ensure that only authorized persons obtain access to NSI; however, final responsibility for determining whether an individual needs to know specific classified information rests with the individual who has possession, knowledge, or control of the information, not with the prospective recipient.

Certification of Security Clearance to another Federal Agency

Any USITC employee or contractors who needs to certify their security clearance for a visit to another agency or facility must request that the PSO certify the security clearance to that agency or facility. Contact information for the Security Office of the agency to be visited must be provided. The request should be submitted as soon as the need for a visit is determined.

Obtaining Access to NSI for Visitors to the USITC

Employees, contractors, or consultants of another federal government agency may obtain NSI access in the USITC to perform official duties only after the verification of an appropriate security clearance through approved security channels. In the case of repeated short-term visits by an individual, clearance certification must be provided at least annually from the federal agency concerned to the PSO.

Administrative Downgrade or Termination of Security Clearance

A security clearance may be downgraded or terminated for administrative reasons unrelated to an adverse security determination. The immediate supervisor, project manager, or contracting officer's representative (COR) is responsible for requesting a security clearance and for advising the PSO whenever an administrative downgrade or termination of security clearance is appropriate based on a change in need to know. When a person no longer needs access to a particular security classification level, the security clearance should be adjusted, or downgraded, to the classification level still required for the performance of the person's duties and obligations. Security Officer shall revoke a security clearance when the clearance or access is no longer consistent with the interests of national security.

NSI Debriefing

Employees and contractors who have access to NSI must be debriefed on their responsibilities related to disclosure of NSI when they leave the Commission or if their clearance is withdrawn or revoked. Upon termination of a security clearance, the holder

must receive a formal security debriefing describing the continuing responsibility to protect the NSI to which the individual had access. The individual will complete the debriefing section of the SF-312, Classified Non-Disclosure Agreement, upon debriefing. In addition, the debriefed employee will be provided with a written copy of the list of sanctions authorized by Title 18, U.S.C. to emphasize that unauthorized disclosure of NSI may result in criminal prosecution. Whenever there is an administrative action, the individual will receive an updated "Clearance Record," indicating the new level of NSI access. This Clearance Record will be filed in the employee's Official Personnel Folder (OPF), and the Office of Personnel Management (OPM) Personnel Investigations Processing System (PIPS) will be updated. This debriefing is provided by appointment with the NSI program manager, and for employees leaving the Commission, should be scheduled prior to the employee's final day of access.

Departing Employees

Classified information (in any form), including copies, is not personal property and may not be removed from the government's control by any departing employee or official. Office NSI Coordinators shall ensure that all separating personnel account for all classified information in their possession, and transfer all classified material to an authorized custodian. The authorized custodian should work closely with the NSI program manager to ensure departing personnel have no classified information in their possession before departing.

Security Education and Awareness Training

Initial NSI In-Briefing

Employees and contractors who are approved and cleared for access to NSI must be briefed on their responsibilities and procedures for handling NSI. Individuals must complete a Classified Information Nondisclosure Agreement, SF-312, before being granted a final security clearance. No employees or contractors will have access to classified information until they have received the NSI Briefing and have signed the SF-312. This briefing is provided by the NSI Program Manager.

Annual NSI Refresher Training

USITC employees with NSI access must attend annual NSI security and awareness refresher training. Refresher training shall reinforce the policies, principles and procedures covered in initial training. Annual refresher training should also address identification and handling of other agency-originated information and foreign government information, as well as the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Annual refresher training should also address issues or concerns identified during agency self-inspections.

Biennial NSI Derivative Classification Training

USITC employees who apply derivative classification markings must receive training in the proper application of derivative classification principles, emphasizing the avoidance of over-classification. At a minimum, the training shall cover the principles of derivative classification, classification levels, duration of classification, identification and markings,

classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. Personnel shall receive this training prior to derivatively classifying information. In addition to preparatory training, derivative classifiers shall receive such training at least once every two years.

Safeguarding Classified Information

Classified Storage

At all times, classified information must be kept under continuous observation by personnel with the appropriate security clearance and need to know, or stored in a locked General Services Administration (GSA) approved security container. An office that receives classified information (in any form) and has no authorized storage equipment available must either return the classified information to the sender, arrange with another office to properly store the information, or destroy it by an approved method. Under no circumstances shall classified information be left unattended, in an unauthorized storage container, or in the custody of a person who does not have the proper security clearance and an established need to know.

Bulky secret and confidential information may be stored in a location designated by the NSI program manager. No other area shall be used for classified open storage without prior accreditation and written approval. Custodians of classified information must ensure that persons assigned to or visiting an office who do not possess an appropriate security clearance and need to know do not take or read classified information, overhear classified conversations, or have visual access to classified information. Classified information must not be placed or displayed where it can be seen through a window or a doorway. Holders of NSI shall close and lock the office door when working on NSI materials.

Incoming Classified Information

All classified materials shall be delivered to the addressee or his designee immediately upon receipt at the Commission. In the event that the addressee or his designee is not available to receive the materials, they shall be delivered to the Secretary and secured, unopened, in a GSA-approved security container in the Secretary's office until the addressee or his designee is available. Under no circumstances shall classified materials that cannot be delivered to the addressee or his designee be stored other than in a GSA-approved security container. Office procedures will be established which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient.

Where practical, the NSI program manager shall be informed of the activities regarding the protection of incoming classified mail, bulk shipments, or items delivered by messenger to the mail room. Procedures must be in place to limit access to classified information to appropriately cleared personnel only. U.S. Postal Service first class, certified, and registered mail should be presumed to possibly contain classified information. At no time shall mailroom personnel be allowed to open any incoming

classified mail or "presumed classified" mail.

NSI on IT Systems
NSI can only be processed on a certified NSI system (e.g., thin client) provided by the CIO Helpdesk. If the team is using laptops, the CIO Helpdesk will also provide approved, removable media to share information with NSI approved members of your project team. This media must be clearly marked at the highest level of classification, and must be safeguarded in the exact same manner as prescribed in this handbook for printed classified information. Flash drives are not permitted for the storing or transporting of NSI.

The Project leader shall complete the NSI Network Access Authorization form and submit it to the PSO. The PSO will check to ensure that all team members are eligible to access NSI and will certify and sign the NSI Network Access Authorization form and forward it to the CIO for final approval.

The certified NSI system/equipment can only be used for NSI processing. You cannot process any information on the system that is not related to the NSI study to which you have been assigned. Emailing NSI, either internally or externally, is strictly prohibited.

IT Storage Media
Storage media that contains classified information shall bear external classification markings and internal notations indicating the classification level, authority, and declassification instructions. Exterior labels shall be used to mark media, other non-paper media, and equipment for which cover sheets are not feasible. Standard Form (SF) labels 706, 707, 708, 709, and 710 will be affixed as appropriate. The labels are available from the CIO.

Safes and the Security Container Check Sheet, SF-702
A Security Container Check Sheet, SF-702, (Appendix A, Figure A-2), shall be placed on the exterior of each classified security container to record each time the container is opened, closed, and checked. The individual conducting such actions shall include his or her initials in the applicable part of the form. The "Checked By" column will be used every day that the office is occupied to conduct work to ensure the container is locked. Currently, the USITC does not provide a guard force check. The originating office shall retain each completed SF-702 for ninety (90) days.

Commingling of Classified Information with Unclassified Information
Commingling of information is the storage of unclassified information with classified information in the same secure container. Where practicable, classified materials and working papers should not be comingled with unrelated materials in the same drawer of the same secure container.

Access to Classified Combinations
Only appropriately cleared and authorized employees shall have access to classified combinations. The number of employees with access shall be kept to a minimum and be clearly identified on the SF-700 "Security Container Information" form, which is a two-

part form. One part of the form is posted inside the safe drawer, and the other part is maintained by the NSI Program Manager. Combinations shall not be provided to anyone who is not identified on the SF-700.

Changing Safe Combinations

Combinations shall only be changed by OSSS personnel and under the following conditions:

- Whenever such equipment is placed into use;
- Whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; or
- Whenever a combination has been subject to possible unauthorized disclosure.

Protecting Classified Combinations

The safe combination used for storage containers housing classified information shall be afforded protection at the highest level of classified information stored in the container. The combinations are classified and shall be recorded only on the SF-700. Completed SF-700's will be maintained by the NSI Program Manager. Combinations are not to be written down or recorded on any electronic device. Recording safe combinations in any format other than on the SF-700 constitutes a security violation.

Relocating Containers Housing Classified Information

Supervisors or program managers responsible for control of a security container must notify the NSI program manager before relocating the security container so that the NSI program manager can note the new location of the container. The NSI program manager must annotate any changes to the relocation of the security container on the SF-700.

End-of-Day Security Check

The responsibility for the end-of-day security check shall be placed on the occupant of a private office, and on the last employee to depart a shared office area. Individuals who work later schedules should familiarize themselves with the locations of all the safes in their area, and typical work schedules of those working in their area to ensure someone has accepted the responsibility for the end of the day check each day. Individuals responsible for conducting the end-of-day security check must thoroughly check the entire work area where classified information is processed, handled, discussed, and stored, and then sign and date the SF-701 "Activity Security Checklist." Each operating unit shall establish a system of security checks at the close of each working day to ensure that the following conditions are met:

- All classified information has been returned to the appropriate GSA-approved security container and is properly secured;
- Classified waste is properly stored or destroyed;
- Wastebaskets and recycle containers do not contain classified material;
- All security containers are double-checked to ensure that the container is properly locked and secured by pulling on the handles of the drawers and spinning the combination dial at least four rotations;
- The Security Container Check Sheet, SF-702, has been filled out properly;

- All doors to the area are locked;
- Cryptographic ignition keys (CIKs) are removed from secure telephone equipment (STEs) and secure telephone units (STU-III) are properly safeguarded.
- Alarms (if in place) are properly activated; and
- The Activity Security Checklist, SF-701 (Appendix A, Figure A-1), has been filled out each day that the office was occupied for duty purposes. The SF-701 shall be displayed at the office exit door only in offices in which NSI is stored and/or processed. The originating office shall retain each completed SF-701 for ninety (90) days.

Custody of NSI During Emergencies

In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, classified information shall be protected by removing it under secure means, by placing it in GSA approved security containers, or by proper destruction. Individuals, who are away from their offices and have classified information in their possession at the time, shall maintain custody until such information can be properly secured. The director of each office shall prepare a plan for the emergency protection or destruction of classified information. The destruction plan for classified information shall be distributed to all cleared personnel working with classified information. The plan shall include the location and identity of the information to be destroyed; and the priority for destruction, persons responsible for destruction, and the recommended place and method of destruction.

Inspection Procedures Compliance Reviews

The NSI program manager has responsibility for conducting an annual agency wide self-inspection and additional random reviews of individual program offices to ensure that NSI is properly safeguarded. The NSI program manager will conduct an annual pre-announced self-inspection in coordination with the individual offices. A list of employees participating in the reviews will be provided to the office director in advance of the inspection. These individuals will be authorized to enter any offices that possess NSI holdings. Inspections may consist of a search of desktops, desk drawers, and cabinets, or other office furniture and equipment. Designated personnel will minimize the impact on business activities while carrying out such inspections.

Inspection procedures and frequency of reviews may vary based on program needs and the magnitude of security activity. Means and methods for conducting inspections may include the following:

- Interviews with key personnel and holders of classified materials;
- A review of internal procedures and processes pertaining to the safeguarding of classified and sensitive information; and
- A sampling of classified materials created and stored by the operating units.

Security Incident Reporting

Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person, and any person who discovers classified information improperly safeguarded or left unattended and unsecured, shall immediately report the circumstances to the NSI Program Manager and to their immediate supervisor. In addition, an employee who discovers or believes that a classified document is missing or compromised must report to the NSI Program Manager as soon as possible, but no later than twenty-four (24) hours following the discovery.

Corrective Actions
Office directors, in consultation with the Director, OSSS, and human resources staff may need to be involved to determine the corrective action that will be applied to any person who violates USITC security requirements. Subsequent to the corrective action, any determinations to reconsider granting access requires the concurrence, in writing, of the Director, OSSS. Anyone who willfully violates, attempts to violate, or conspires to violate any regulations or order involving the USITC security program is subject to corrective action up to and including termination of employment.

When reporting, the user should provide as much information as possible, including:

- Who was involved in the event?
- What exactly occurred?
- What information and equipment were involved?
- Where did the event take place?
- When was the event discovered and by whom?

Some important tips for the user to remember in initial handling of events are:

- If the incident occurs on a computer, do not shut down the system or disconnect it from the network without contacting and receiving instruction to do so from the CIO. Do not continue to work on a computer where a security incident is suspected.
- Do not attempt to investigate whether data was accessed without permission; otherwise, you may destroy valuable evidence.
- Do not talk to the news media. Refer all news media inquiries to the USITC Public Affairs Office in the Office of External Relations.

Security incidents that should be reported to the NSI Program Manager include, but are not limited to, the examples below:

- Improper destruction of NSI;
- Transmission of NSI via non-secure means or use of unauthorized equipment;

- Improper storage of NSI;
- Loss of NSI material;
- NSI mailed via non-registered/certified mail, or mailed in single wrapper/container;
- Markings on outer container divulged classification of contents;
- Classification not marked on inner container;
- No return receipt;
- Inadequate wrapping: not securely wrapped or protected;
- Classified mail received in poor condition: comprise probable;
- Envelope addressed improperly;
- Information classified by unauthorized original classifier;
- Markings incorrect;
- Derivative classification markings incorrect or missing; and
- No markings.

Security incidents that should be reported to the Chief Information Officer include, but are not limited to, the examples below:

- Any person using a USITC employee's individual password and/or account information;
- Failure to protect passwords and/or access codes (i.e., taping codes to equipment to avoid memorizing);
- Leaving a thin client or system signed on/unattended;
- Unauthorized use of external computer connections (i.e. USB flash drives);
- Indication of computer virus;
- Theft of computer equipment or software;
- Inappropriate use of software, such as illegal copying of licensed computer software;
- Inappropriate use of E-mail;
- Misuse or defacing government equipment;
- Destruction or tampering with government equipment;

Reports to the Information Security Oversight Office (ISOO)

The senior agency officials shall notify the Director of ISOO when a violation occurs that:

- Is reported to oversight committees in the Legislative branch;
- May attract significant public attention;
- Involves large amounts of classified information; or
- Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

Disclosure

Meetings

See APPENDIX B "Security Procedures for Conducting Classified Discussions" for additional guidance.

Classified Information Appearing in Public Media

The fact that classified information has been made public does not mean that it has been declassified. Information remains classified unless and until it is formally declassified. An employee who becomes aware of classified, or other sensitive information, appearing in the public media should bring it to the attention of the NSI program manager immediately.

Freedom of Information Act (FOIA) and Privacy Act Requests

Requests for declassification submitted under the provisions of FOIA, as amended, or the Privacy Act of 1974 are processed in accordance with the provisions of those acts. Unless the Secretary to the Commission determines otherwise, requests for documents that contain classified information will be referred to the agency that originally classified the information for processing. The Secretary may, after consultation with the originating agency, inform the requester of the referral unless the originating agency determines that such association is itself classified.

Classification

Original Classification Authority

Original classification is the initial decision that particular information requires protection in the interest of national security and could be expected to cause damage if subjected to unauthorized disclosure. USITC does not have Original Classification Authority (OCA). The USITC derivatively classifies information in accordance with classification guidance from the United States Trade Representative (USTR). No USITC employee may classify information unless authorized through the derivative classification guidance provided by USTR.

Derivative Classification

Derivative classification refers to incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply from the source document.

All classified material generated by USITC staff will be derivatively classified based on guidance received from USTR. USTR provides classification guidance or derivative classification instructions to the Commission in the form of classification guidance letters and a classification guide for the work activities that the Commission performs on its behalf. Any existing, properly marked classified document can also be used as a source document for derivative classification.

The duplication or reproduction of existing classified information is not derivative classification. Training in derivative classification is provided upon request, or at a

minimum of once every two years. A marking guide is also available.

Classification Standards
Information may be classified only if all of the following conditions are met:

- The information is owned by, produced by or for, or is under the control of the U.S. Government;
- The information falls within one or more of the categories of information listed in Section 1.4 of Executive Order 13526; and
- The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the OCA is able to identify or describe the damage.

Classification Levels
Information may be classified by an OCA at one of the three levels identified below. No additional terms, such as sensitive, agency, business, or administrative, shall be used in conjunction with the terms Top Secret, Secret, or Confidential to identify classified NSI.

- **Top Secret** shall be applied to information which reasonably could be expected to cause exceptionally grave damage to the national security if disclosed to unauthorized sources.
- **Secret** shall be applied to information that reasonably could be expected to cause serious damage to the national security if disclosed to unauthorized sources.
- **Confidential** shall be applied to information that reasonably could be expected to cause damage to the national security if disclosed to unauthorized sources.

Confidential Business Information (CBI)
Confidential Business Information (CBI) and the lowest level of National Security Information (NSI) Confidential both include the word "confidential" in their label; however, the terms are not synonymous and refer to two distinctly different types of information that require different levels of protection. A document that contains both NSI and CBI must bear the appropriate markings for both types of information.

Duration of Classification
The USITC shall be guided by the USTR on the duration of classification for all work activities that the USITC performs on its behalf.

Classification Challenges
Authorized holders of classified information are encouraged to challenge classification decisions to promote proper and thoughtful classification actions. A formal classification challenge shall be in writing and coordinated with the Secretary of the Commission, the Office of External Relations, and the NSI program manager. The formal classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries are

encouraged and should be used to reduce the number of formal challenges. Contact the NSI program manager for additional guidance.

Compilations or Aggregation of Unclassified Information
Individually unclassified documents may become classified if the compiled information reveals an additional association or relationship that meets the standards for classification under Executive Order 13526. The relevant Office Director and the NSI Program Manager can review the compilation of unclassified information for proper classification as needed. The information may need to be referred to USTR for a final classification determination.

Declassification

USITC does not have declassification authority. Classified information shall be declassified according to guidance provided by USTR. All declassification decisions rest with USTR.

Automatic Declassification
Automatic declassification is the declassification of information based solely upon the occurrence of a specific date or event as determined by the OCA, or the expiration of a maximum time frame for duration of classification established under Executive Order 13526. All classified records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of Executive Order 13526. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead. Classified records containing information that originated with other agencies, such as USTR, can be referred to those agencies for review when in doubt as to the appropriate declassification of the information.

Systematic Declassification Review
The Secretary retains the official copies of all classified reports. Each operating unit shall confer with the Secretary to ensure that that the Secretary has the official copy of all agency classified documents. The Secretary shall establish and implement procedures for systematic referral of these documents to USTR for declassification. This program shall apply to records or permanent historical value exempted from automatic declassification under section 3.3 of Executive Order 13526.

Downgrading NSI
Information designated at a particular level of classification may be assigned a lower classification level only by the OCA. USITC does not have downgrading authority.

Changes in Classification Markings
Whenever classified information is downgraded or declassified by the originator or the initial classification changes, the information shall be marked to reflect the change as well as the

authority for and date of the action. The following markings shall be applied to records, or copies of records, regardless of media:

- The word, "Declassified;"
- The identity of the declassification authority, by name and position, or by personal identifier, or the title and date of the declassification guide. If the identity of the declassification authority must be protected, a personal identifier may be used or the information may be retained in agency files.
- The date of declassification; and
- The overall classification markings that appear on the cover page or first page shall be lined with an "X" or straight line. An example might appear as: ~~SECRET~~
- Declassified by David Smith, USTR Division Chief, August 17, 2008

Marking NSI (Electronic and Paper)

Physically marking classified information with appropriate classification and control markings serves to warn and inform holders of the degree of protection required. Other notations aid in derivative classification actions and facilitate downgrading or declassification. It is important that all classified information and material be marked clearly to convey the level of classification assigned to the portions that contain or reveal classified information, the period of time protection that is required, and any other notations required for protection of the information or material.

The overall classification markings and portion markings of the source document should supply adequate classification guidance to the derivative classifier. If portion markings or classification guidance are not found in the source document, and no reference is made to an applicable classification guide, guidance should be obtained from the originator of the source document. In the case of the Commission, this would be the USTR.

Please refer to the Information Security Oversight Office Marking Handbook for detailed marking guidance: http://www.archives.gov/isoo/training/marking-booklet.pdf, or contact the NSI Program Manager for assistance.

Classified Document Cover Sheets

Classified document cover sheets must be used at all times when handling classified information. SF-703 (Top Secret), SF-704 (Secret), or SF-705 (Confidential) cover sheets will be used on all classified files, folders, binders, and similar groups of documents on the outside of the folder or document holder. The cover sheet will always be the outermost covering. Transmittal memos should be placed under the document classification cover sheet. The only time a cover sheet does not need to be affixed to an individual document is when the document is placed in a folder or binder with other classified documents and the appropriate cover sheet is affixed to the exterior cover to identify the highest level of the documents contained within the folder or binder.

Other material, such as bulky material, equipment, and facilities, shall be clearly identified in a manner that leaves no doubt about the classification status of the material or space, the level of protection required, and the duration of classification.

Classified Working Papers

Working papers shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, portion marked, and if appropriate, destroyed when no longer needed in accordance with the agency's records disposition schedule. When any of the following conditions apply, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

- Released by the originator outside the originating activity;
- Retained more than 180 days from the date of origin; or
- Filed permanently.

Transmission of NSI

Classified information shall be transmitted and received in a manner that ensures evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method which assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information properly, in accordance with applicable regulations.

Office directors shall establish and implement procedures that ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. Any individual receiving classified information is responsible for preventing unauthorized access, inspecting for tampering, and ensuring timely acknowledgment of receipt.

Transmission of Classified Information over Non-secure Systems

NSI material shall not be transmitted over any non-secure telephone, facsimile machine, or electronic mail system. Emailing NSI, either internally or externally, is strictly prohibited. The Commission's local area network is not certified to process or distribute NSI.

Transmitting Via Telephone or Facsimile

Classified NSI shall not be discussed over non-secure phone lines, and must only be communicated on Secure Telephone Equipment (STE), which is located in OSSS.

Transmittal Outside of the USITC Building

Classified information may be transmitted by authorized means (see "Transporting NSI" and "Mailing Classified Information" below) both inside and outside of the agency; however, classified information may not be removed from the USITC without written approval from the Office Director and the NSI Program Manager. Permission to carry classified material overseas may be granted on a case-by-case basis. Requests for permission to carry classified information aboard a commercial passenger aircraft should be submitted in writing to the NSI Program Manager no less than ten (10) working days before departure.

Transmission of NSI classified reports to USTR is the responsibility of the Office of External Relations. Individual staff, project managers, or Office Directors should work through that office and should not be submitting classified reports to USTR on their own or through the mail room. External Relations will make the arrangements with the mail room courier and will insure that the classified report is delivered to the appropriate staff person at USTR.

Visits to Other Agencies
Any employee, or contractor who has a need to visit another agency or facility involving access to classified information must initiate a Visit Authorization and Clearance Certification Request through OSSS.

Transporting NSI

Wrapping Guidance
All classified information transported outside a USITC facility shall be enclosed in two layers, an opaque inner and outer cover (e.g., sealed envelopes, wrappings, or a locked container), both of which conceal the contents and provide reasonable evidence of any tampering.

The appropriate cover sheet shall be affixed to the top of the classified document: SF-703 (Top Secret), SF-704 (Secret), or SF-705 (Confidential). The inner sealed cover shall be clearly marked on both sides with the highest classification level of the information contained within, any required protective markings, and complete forwarding and return addresses. The outer sealed opaque cover shall be addressed in the same manner (i.e., intended recipients shall be identified by name only as part of an attention line) but shall not bear any classification markings or other indication that classified information is enclosed.

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

Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capacity to store classified information properly in accordance with applicable regulations. Please see the NSI Program Manager for wrapping assistance.

Transporting NSI Inside of the USITC Building
All classified information hand-carried between offices within the USITC facility shall be placed in a folder or envelope to prevent inadvertent disclosure and to conceal the classified cover sheet from casual observance. The document must also have the appropriate cover sheet affixed to the front, and the cover sheet must remain the outermost page of the document. Do not cover the cover sheet with any sort of routing sheet or other paper. Individuals transporting classified documents within USITC

facility shall not carry classified documents into public areas (e.g., galleys, snack room, restrooms) while in route to their destination. Packages containing NSI may not be left unattended in any office. If no authorized individual is available to receive the package, a note should be left announcing the attempted delivery and delivery should be attempted again at a later time.

NSI "Red Folder" Action Jacket (NSI AJ) Distribution

All classified action jackets hand-carried between offices or operating units within the USITC facility shall have the appropriate cover sheet depending on the classification level of the material, i.e., SF-703 Top Secret, SF-704 Secret, or SF-705 Confidential, affixed to the top of the action jacket. The cover sheet shall remain attached until the document is destroyed.

In addition, the following procedures for transmitting classified documents shall be followed:

- First Commissioner listed on the AJ Approval Record receives the NSI AJ from the project leader, verifies described NSI material is attached, and signs the Action Jacket Log form.
- After review, that Commissioner's office distributes the NSI to the next Commissioner's office listed who checks to make sure described NSI material is attached, signs the Action Jacket Log form and provides a photocopy of the log to the project leader as proof of transfer. Each Commissioner's office handles the NSI in the same manner as described above.
- As the last Commissioner's office on the list, the Chairman's office distributes to the NSI AJ to the Secretary's office.
- The Secretary's office receives the NSI AJ from the Chairman's office, verifies described NSI material is attached, signs Action Jacket Log form, and provides a photocopy of the log to the distributor as proof of transfer.
- The Secretary's office contacts the project leader to pick up the NSI AJ.
- The project leader picks up the NSI AJ, verifies described NSI material is attached, signs Action Jacket Log form, and provides a photocopy of the log to the distributor as proof of transfer.
- All offices must return their NSI material to the project leader for destruction.
- The project leader provides the NSI AJ and all control logs to Lead Office Director for record retention.

Transporting NSI Outside of the USITC Building

Employees may hand-carry classified information within the United States and its territories. The employee must be an authorized courier and possess a courier card when in possession of classified information outside of the Commission. To be an authorized courier, the employee must hold an appropriate security clearance and possess a valid USITC NSI Courier Authorization Card. Classified information shall not be opened, read, studied, displayed, used, or discussed in any manner in a public conveyance or location.

Hand-carrying of NSI on trips involving an overnight stop is not permissible without prior arrangements for storage at a cleared facility.

USITC Courier Authorization Card

The USITC Courier Authorization Card authorizes the bearer to transport or hand-carry classified information on a recurring basis. The USITC Courier Authorization Card does not authorize the courier to hand-carry classified information aboard commercial aircraft. Appropriately cleared personnel may obtain a Courier Authorization Card to hand-carry classified information outside USITC-controlled space subject to the following conditions:

- The supervisor of the intended bearer shall request the issuance of a Courier Authorization Card in writing to the NSI program manager;
- The bearer of the USITC Courier Authorization Card must report the loss or damage of the card in writing to the NSI program manager as soon as possible; and
- The bearer must return the USITC Courier Authorization card to the NSI program manager upon termination of his or her security clearance, when the authorization is no longer needed, or when an occurrence dictates the need to withdraw the courier authorization, as determined by the NSI program manager.

Hand-Carrying Classified Information aboard Commercial Passenger Aircraft

Appropriately cleared personnel may be authorized to hand-carry classified information aboard commercial passenger aircraft when there is neither time nor means to properly transmit the information by other authorized means. Before carrying classified information across international borders, the courier must make arrangements to ensure that the information will not be opened or viewed by customs, border, postal, or other inspectors, either U.S. or foreign. The courier must travel aboard a U.S. carrier. Foreign carriers may be used only when no U.S. carrier is available. The courier must ensure that the information remains in his or her custody and control at all times. Classified information must not be checked with baggage or left in private residences, vehicles, hotel rooms and safes, aircraft, train compartments, buses, public lockers, or other locations where the information could be compromised. Classified information must be appropriately stored in a GSA-approved security container at all times when not in use. When possible ensure the information is delivered to intended persons as soon as landing before making another travel stops.

The NSI program manager shall brief the courier concerning security safeguards and the need to possess a Commission photo identification badge. An authorization letter is required for a courier to carry classified information aboard commercial aircraft. The courier shall display the photo badge and written authorization upon request by the appropriate airline personnel. The classified information shall be sealed in double wrappings and carried in a locked briefcase or other carry-on luggage. Screening officials may check the envelope by x-ray machine, flexing, feel, weight, and so on without opening the envelopes. Opening or reading the classified documents is not permitted.

Advance arrangements for appropriate overnight storage shall be made to ensure that the facility has authorized storage capability at the appropriate level. The storage capability should be available and accessible at the designated time of the visit. When traveling, the courier shall make contingent arrangements in the event that unforeseen problems result in late or delayed arrivals.

Mailing Classified Information Within and Between the U.S., Puerto Rico, or a U.S. Possession or Trust Territory

Top Secret

Top Secret information shall be transmitted by direct contact between authorized persons; the Defense Courier Service, an authorized government agency courier service, or a designated courier or escort with Top Secret clearance. Under no circumstances will Top Secret information be transmitted via the U.S. Postal Service or any other cleared or uncleared commercial carrier.

Secret

Secret information shall be transmitted by any of the methods established for Top Secret; U.S. Postal Service Priority Mail Express and U.S. Postal Service Registered Mail, as long as you check the "signature is required" box; and cleared commercial carriers or cleared commercial messenger services. The use of street-side mail collection boxes is strictly prohibited.

Note: Effective July 2013, the USPS changed the name of Express Mail to Priority Mail Express and updated the label to reflect that change. The new Priority Mail Express label requires that you actually check the "signature is required" box, whereas with the prior Express Mail label, the signature was automatically obtained as a part of Express Mail delivery, unless indicated otherwise. Please note that you may see use of either the "Express Mail " or "Priority Mail Express " labels until existing stocks of "Express Mail" labels are depleted. In either case, it is the sender's responsibility to ensure that the recipient's signature is obtained when sending SECRET information through the U.S. Postal Service System via express mail.

Confidential

Confidential information shall be transmitted by any of the methods established for Secret information or U.S. Postal Service Certified Mail. In addition, when the recipient is a U.S. Government facility, the Confidential information may be transmitted via U.S. First Class Mail. However, Confidential information shall not be transmitted to government contractor facilities via first class mail. When first class mail is used, the envelope or outer wrapper shall be marked to indicate that the information is not to be forwarded, but is to be returned to sender. The use of street side mail collection boxes is prohibited.

Mailing to a U.S. Government facility located outside the U.S.

The transmission of classified information to a U.S. Government facility located outside the fifty (50) states, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, shall be by methods specified above for Top Secret information

or by the Department of State Courier Service. U.S. Registered Mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

Destruction of Classified Material

Classified documents shall be destroyed in equipment specifically approved for that purpose in a manner that precludes recognition or reconstruction of the classified information. NSI cannot be placed in a recycle bin or "burn" bins. All approved shredders are specifically labeled for the destruction of NSI material and are located in room 511-C and 600-A.

Records of Destruction

USITC requires records of destruction for Top Secret, Secret and Confidential information. Each Program Office NSI Coordinator is responsible for maintaining these records. The record of destruction shall include an unclassified description of the material, signatures of the destroyer of the material, and the individual who witnessed the destruction. Destruction records shall be retained for at least two years for Secret and Confidential information.

Classified material may also be placed in a striped NSI burn bag. Do not leave burn bags unattended. Burn bags must be stored in a GSA approved NSI storage container until custody is transferred to OSSS. Notify the NSI Program Manager for burn bag pick up, which should occur within one working day. Burn bags need to be sealed with staples, marked with highest classification level contained in the bag, and labeled with owner's name and office phone extension. Classified material receipts are not necessary when the custody of the burn bag is transferred to OSSS.

Annual Inventory and Disposal of Classified Holdings

Offices maintaining classified information must conduct an annual inventory to review their classified holdings to reduce the amount necessary for operational and program purposes. The inventory shall include a review to identify classified holdings that may be eligible for possible downgrade, declassification, or destruction. The Records Manager shall work closely with offices that have documents to be either destroyed or declassified. The NSI Program Manager will schedule annual destruction events as needed.

Storing and Transporting Material for Destruction

Classified material awaiting destruction shall be stored in a GSA-approved storage container. Individuals transporting containers with classified waste material must provide adequate safeguards to prevent unauthorized disclosure of the information during transport. Such containers must not be left unsecured or unattended when being transported to an authorized destruction site.

Reproducing NSI

- Reproduction of NSI must be held to the minimum consistent with operational requirements unless restricted by the originating agency. Confidential and Secret information may be reproduced to the extent required by operational needs. Top Secret information requires special permission. Contact the NSI Program Manager for guidance.
- Do not use office copiers to reproduce NSI material at any time. NSI material may only be reproduced using NSI dedicated copiers which are clearly marked "Authorized for Printing Classified NSI Material."
- Single copies of a study can be printed on approved and properly marked stand-alone printers that are provided by the CIO Helpdesk to the NSI project team. These printers will have a colored label indicating the approved highest level of classification.
- Contact the NSI program manager if you need to reproduce multiple copies.
- All copies will be marked at the same classification level as the original.
- All copies are subject to the same controls and safeguards as the original information.
- All copies that are distributed outside of the project team must be logged. At the end of the study, all copies of NSI materials must be retrieved and returned to the project leader for retention or destruction.

Copier Security Procedures

The following procedures shall be followed when reproducing classified Information:

- Copies may be made only by authorized persons who know the procedures for copying classified information, and those individuals will remain at the copier until classified reproduction is complete;
- Copiers used to reproduce classified information shall not be connected to any network or telephone line;
- Before leaving the copier, individuals must check for any copies or originals that may be left in the copier;
- Classified waste, such as rejected copies or blank copies run after classified material is processed, must be destroyed in accordance with this handbook; and
- If the copier malfunctions and cannot be cleared or the copies cannot be retrieved, the NSI program manager shall be notified to ensure that the copier is removed from service until the malfunction has been properly cleared, at which time the copier may be recertified for classified usage.
- Unless a notation on the document or its cover restricts reproduction, permission is authorized without the approval of the originating department or agency for the reproduction of Secret and Confidential documents. Reproduction of the documents must be limited to that which is essential for efficient operations.

Scheduled Maintenance

Copy machines shall have the memory removed by an authorized person before being serviced by personnel that are not cleared. The NSI Program Manager shall be notified of the scheduled service visit and arrange for an appropriately cleared employee to be present. Any documents, image retaining drums, or memory chips removed from the machine shall be collected by the cleared employee and turned over to the NSI program manager. No unescorted maintenance person shall be allowed access to any equipment used to reproduce classified materials.

Foreign Travel

Before Departure

Individuals with a security clearance must schedule a foreign travel briefing with the NSI Program Manager and fill out a foreign travel acknowledgement form prior to leaving for their trip for both official and personal travel. The briefing will also provide the most current country specific threat information.

Upon Return

Contact the NSI program manager to report foreign contacts and any unusual incidents. You are required to report all contacts with individuals of any nationality, either within or outside the scope of your official activities, in which illegal or unauthorized access is sought to classified or otherwise sensitive information, or you are concerned that you may be the target of an actual or attempted exploitation by a foreign entity.

APPENDIX A - SAMPLE SECURITY FORMS

Figure A-1: Activity Security Checklist (SF 701)

ACTIVITY SECURITY CHECKLIST	DIVISION/BRANCH/OFFICE	ROOM NUMBER	MONTH AND YEAR
Irregularities discovered will be promptly reported to the designated Security Office 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 surfaces and receptacles 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

Form designed using PerForm Pro software.

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

Figure A-2: Security Container Check Sheet (SF 702)

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

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

APPENDIX B – SECURITY PROCEDURES FOR CONDUCTING CLASSIFIED DISCUSSIONS

General: The following guidance is applicable to classified discussions held within USITC conference rooms and private offices where Confidential and Secret National Security Information (NSI) will be discussed. A USITC employee meeting host must be identified for all such discussions. These procedures do not apply to Top Secret or Sensitive Compartmented Information (SCI) discussions which will only be held in a Sensitive Compartmented Information Facility (SCIF).

The meeting host must:

1. Notify the NSI Program Manager as far in advance as possible of any classified discussions, and provide the desired location if other than room 613P.
2. Provide a list of USITC attendees to the ISO as soon as possible. The ISO will verify that all attendees have the appropriate security clearance.
3. Security clearances for non-USITC personnel should be certified from the external agency to the OSSS five working days (if possible) before the meeting. OSSS cannot contact the external agency for the certification. It must come from them to us.
4. Establish need-to-know of all attendees.
5. Close the door and window blinds.
6. Disconnect telephones from the wall jacks.
7. Turn off microphones and speakers.
8. Disconnect video teleconferencing equipment.
9. Remove portable electronic devices (PEDs) are not permitted in the room including, but not limited to, cell phones, personally owned laptops, and readers/tablets. Turning the device off is not sufficient. Devices will be collected by the meeting host prior to starting the discussion and removed from the room. USITC issued unclassified computers may remain on and in the room.
10. Use of classified computers and other classified electronic devices shall be permitted only with prior approval from the OCIO.
11. Monitor entrances to the meeting and check each individual's security clearance level on the approved list as they arrive. In the case of unexpected additions, verify the individual is appropriately cleared with the assistance of OSSS before disclosing classified information.
12. Read the "Classified Discussion Statement Guidance" to the attendees prior to starting the meeting, and each time the meeting reconvenes.
13. Where practicable, ensure the perimeter of the meeting area is monitored and controlled to prevent unauthorized personnel from overhearing classified discussions.
14. Provide escorts for uncleared personnel providing services, or delivering messages to the meeting. Discontinue discussions until the individual has left the room.
15. Advise attendees that they should not take notes unless it is necessary to fulfill the U.S. Government purpose for the meeting. Unclassified laptop computers, personal electronic devices, and other similar devices shall not be used for note taking during classified discussions. If notes are necessary, they must be handled as classified information until they can be reviewed by an authorized classification review authority such as a program manager. External attendees may hand carry their notes only if they have a courier card, and the notes have been properly wrapped or placed in a courier pouch.
16. Ensure that classified information, documents, transcriptions, audio recordings, audiovisual material, information systems, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported in accordance with established USITC procedures.
17. Ensure that all materials used by a cleared court reporter are properly secured in approved USITC space, and that subsequent transcription is performed under proper controls.

18. Advise external attendees that they may hand carry their notes only if they have a courier card, and the notes have been properly wrapped or placed in a courier pouch.

CLASSIFIED DISCUSSION STATEMENT TO BE READ PRIOR TO THE START OF A NATIONAL SECURITY INFORMATION (NSI) MEETING:

Today's meeting includes the discussion of (select one) CONFIDENTIAL OR SECRET information.

- Everyone in this meeting must have a clearance level of (Confidential or Secret) and must have a need to know this information to perform their job function.
- Portable electronic devices such as cell phones, blackberries, personal laptops, and readers/tablets are prohibited. Turning the device off is not sufficient. ITC issued computers may remain on and in the room, but must not be used for note taking.
- Notes should not be taken unless it is absolutely necessary. If notes are necessary, they must be handled as classified information until they can be reviewed by an authorized classification review authority.

STATEMENT TO BE READ AT THE CONCLUSION OF THE MEETING:

You are reminded that the information discussed at this meeting was (select one) CONFIDENTIAL or SECRET information and of the special handling requirements associated with that information.

At the conclusion of the discussion, the meeting host must:

1. Remind attendees of their responsibility to protect the classified information that was discussed during the meeting.
2. Collect any notes taken for classification review, storage, or destruction. Inform attendees that notes will be returned to them once the classification has been determined. If time permits, classification reviews may be done at the conclusion of the meeting, and the notes may be returned to the attendee after the appropriate cover sheet is affixed to the notes if classified information is identified.
3. Visitors may remove classified notes from the building provided the notes are properly wrapped in accordance with established procedures, or secured in a locking courier pouch.
4. Recover all copies of classified information handed out during the meeting.
5. Ensure that no classified information has been left behind prior to leaving the room. (Check tables, chairs, white boards, floors, etc.).

CLASSIFIED DISCUSSIONS THAT IMMEDIATELY FOLLOW AN UNCLASSIFIED DISCUSSION

In the event that a classified discussion immediately follows an unclassified discussion, all in attendance who are not authorized to attend the classified discussion must vacate the room. A list of the attendees authorized to remain for the classified meeting will be maintained by the meeting host. Anyone not appearing on the list must leave the room. It is the responsibility of the meeting host to ensure that only authorized and appropriately cleared persons are in attendance before starting the classified meeting.