



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.9.1

NOVEMBER 6, 2023

EFFECTIVE DATE

(11-06-2023)

PURPOSE

- (1) This transmits revised IRM 10.9.1, Classified National Security Information (CNSI).

MATERIAL CHANGES

- (1) IRM uses the term Classified National Security Information (CNSI) to discuss classified material of any type and avoid it being associated with the Information Technology (IT) sphere. The terms “CNSI,” “classified information,” and “material” are synonymous and used interchangeably throughout.
- (2) Updated the entirety of the IRM was updated to provide clarity on the CNSI and National Industry Security Program (NISP) subsections.
- (3) Subsections were relocated, reformatted, or organized to improve readability and internal controls added in compliance with IRM 1.11.2.
- (4) Expanded the information in the subsections related to the program owner, authority, roles/responsibilities.
- (5) Updated acronyms and security terms/definitions.
- (6) Removed or combined subsections:
 - a. Information contained in the Exhibits was incorporated into appropriate subsections throughout the document.
 - b. Removed subsection 10.9.1.3.3, Record Requirements and Chronological Files.
 - c. Combined subsections 10.9.1.7, Dissemination, and 10.9.1.9, Information Reproduction Controls, into a new subsection 10.9.1.4, Information, Dissemination, and Reproduction Controls.
- (7) Added language/subsections on the following:
 - a. IRM 10.9.1.1.3, Updated responsibilities to accurately reflect CNSI program and NISP administration, to include formally adding the roles of Classified Document Custodian, Security Container Custodian, Top Secret Control Officer, Responsible Party, etc.
 - b. IRM 10.9.1.8.4, Combination Locks and Key Operated Locks and Security Container Movements was updated to include key control.
 - c. IRM 10.9.1.8.6, Security Areas was added as a subsection to cover Open Storage up to Secret, Treasury Secure Data Network (TSDN) Limited Areas (LA), Top Secret Space, and Sensitive Compartmented Information Facilities (SCIF).
 - d. IRM 10.9.1.10, The Transmission subsection was rewritten in more detail, combining information regarding transmission throughout the former IRM into one subsection.
 - e. IRM 10.9.1.10.1, Courier Requirements had additions made to clarify when a courier card or letter is required.
 - f. IRM 10.9.1.11, Detailed information was added on North Atlantic Treaty Organization (NATO) and Foreign Government Information (FGI) as IRS authorized holders access both types of information at other facilities.
 - g. IRM 10.9.1.12.1, Destruction Process was added to account for destruction requirements for Top Secret vs. Secret and Confidential.
 - h. IRM 10.9.1.14, Security Incidents and Associated Inquiries was rewritten for clarity of process.

- (8) Various grammatical and editorial changes throughout, and renumbered and/or renamed subsections where applicable, to improve the flow of information.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.9.1, dated April 13, 2021.

AUDIENCE

This IRM is for all IRS employees and contractors that are authorized holders, as defined in subsection 10.9.1.1.6(3) of this IRM, responsible for handling, processing, storing, transmitting, accounting for, tracking and/or destruction of CNSI, as well as IRS Business Units that intend, or have entered into, contracts that require contract employees to access CNSI in the performance of their duties or hold national security clearances.

Richard L. Rodriguez
Chief
Facilities Management and Security Services

10.9.1

Classified National Security Information

Table of Contents

10.9.1.1 Program Scope and Objectives

10.9.1.1.1 Background

10.9.1.1.2 Authority

10.9.1.1.3 Roles and Responsibilities

10.9.1.1.4 Program Management and Review

10.9.1.1.5 Program Controls

10.9.1.1.6 Terms/Definitions/Acronyms

10.9.1.1.7 Related Resources

10.9.1.2 Classification Levels

10.9.1.3 Original Classification and Original Classification Authority

10.9.1.3.1 Limits to Classification and Reclassification

10.9.1.3.2 Derivative Classification

10.9.1.3.3 Classification Challenges

10.9.1.3.3.1 Challenge Requirement and Handling

10.9.1.4 Information, Dissemination, and Reproduction Controls

10.9.1.4.1 Marking

10.9.1.4.2 Requirements for Paper

10.9.1.4.3 Requirements for Electronic Mail (email)

10.9.1.4.4 Working Papers

10.9.1.5 Document Cover Sheets

10.9.1.5.1 Labels on Equipment and Electronic Media

10.9.1.6 Downgrading and Declassification

10.9.1.6.1 Declassification Reviews

10.9.1.7 Secure Voice/Data Communication

10.9.1.8 Safeguarding CNSI

10.9.1.8.1 Access to CNSI

10.9.1.8.2 General Safeguarding Provisions

10.9.1.8.3 Standards for Securing CNSI

10.9.1.8.3.1 Storing Top Secret

10.9.1.8.3.2 Storing Secret and Confidential Information

10.9.1.8.4 Combination Locks and Key Operated Locks, and Security Container Movements

10.9.1.8.5 Processing CNSI

10.9.1.8.6 Security Areas

10.9.1.9 Contractors and CNSI

10.9.1.10 Transmission

-
- 10.9.1.10.1 Courier Requirements
 - 10.9.1.11 North Atlantic Treaty Organization (NATO) and Foreign Government Information (FGI)
 - 10.9.1.12 Destruction of CNSI
 - 10.9.1.12.1 Destruction Process
 - 10.9.1.13 End of Day Security Checks
 - 10.9.1.14 Types of Security Incidents and Associated Inquiries
 - 10.9.1.15 Self-Assessments

10.9.1.1
(11-06-2023)
Program Scope and Objectives

- (1) This IRM implements baseline standards within the IRS for creation, classification, safeguarding, handling, transmission, and destruction, hereafter termed 'lifecycle,' of Classified National Security Information (CNSI).
- (2) **Purpose:** This document implements policies and procedures for the handling of CNSI throughout its lifecycle, as well as processes if a security incident, either infraction or violation, occurs. This program includes in the CNSI program is the National Industrial Security Program (NISP), which allows IRS contractors to access CNSI or have a national security clearance to perform the scope of duties in their contract. The NISP is underneath the CNSI program with the shared goal of protecting classified information.
- (3) **Audience:** This IRM section provides policy and guidance to be used by authorized holders and managers who are responsible for CNSI at any point in its lifecycle. The provisions in this IRM apply to all offices, business, operating, and functional units, as well as any individuals/organizations these entities have contractual arrangements with, in the IRS who handle CNSI.
- (4) **Policy Owner:** Chief, Facilities Management and Security Services (FMSS) serves as the Senior Agency Official (SAO) for the IRS CNSI Program.
- (5) **Program Owner:** Associate Director (AD), Security, FMSS.
- (6) **Primary Stakeholders:** Criminal Investigations (CI), Cyber Security Incident Response Center (CSIRC), Personnel Security, Continuity of Operations (COOP) in National Headquarters, Chief Counsel, Facilities Management and Security Services (FMSS), Privacy, Governmental Liaison and Disclosure (PGLD), and any IRS personnel that makes use of, or encounters, CNSI throughout its lifecycle.
- (7) **Program Goals:** The objectives of the program are to ensure the CNSI that IRS holds or creates is safeguarded for its lifecycle in accordance with the guiding documents and references contained in IRM 10.9.1.1.2, Authority.

10.9.1.1.1
(11-06-2023)
Background

- (1) This revision addresses policy updates to implement changes that will allow the IRS to provide clarity regarding required safeguards for CNSI and appropriately handle CNSI from its inception to destruction.

10.9.1.1.2
(11-06-2023)
Authority

- (1) Treasury Department Publication (TD P) 15-71, Department of the Treasury Security Manual, dated June 17, 2011.
- (2) Treasury Order (TO) 105-19, Delegation of Original Classification Authority; Requirements for Downgrading and Declassification, dated June 17, 2011.
- (3) Department of Treasury Security Classification Guide dated March 2, 2012.
- (4) Treasury Directive 85-01, Department of the Treasury Information Technology (IT) Security Program, dated February 28, 2022.
- (5) Information Security Oversight Office (ISOO) Directive No. 1, 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, Classified National Security Information (implementing Executive Order 13526), dated June 22, 2010.
- (6) ISOO, Marking Classified National Security Information, Rev. 4, dated January 2018.

- (7) Executive Order (EO) 13526, Classified National Security Information, dated December 29, 2009.
- (8) EO 12968, Access to Classified Information, dated August 2, 1995, as amended.
- (9) EO 12829, National Industrial Security Program, dated January 8, 1993, as amended.
- (10) 32 CFR Part 2004, National Industrial Security Program (NISP), dated May 7, 2018, as amended.
- (11) 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPO), dated February 24, 2021.
- (12) North Atlantic Treaty Organization (NATO) Instruction 1-07, Implementation of NATO Security Requirements, dated April 5, 2007.
- (13) IRM 10.23.1, National Security Positions and Access to Classified Information.
- (14) IRM 10.23.3, Personnel Security/Suitability Program for Employment and Personnel Security Operations.
- (15) Physical Security Design Manual, dated November 4, 2020.

10.9.1.1.3
(11-06-2023)
**Roles and
Responsibilities**

- (1) The IRS Commissioner is responsible for:
 - a. Establishing the IRS CNSI program and NISP in accordance with the authorities and references contained in this IRM.
 - b. Demonstrating personal commitment and committing senior management to the successful implementation of the IRS CNSI program and NISP.
 - c. Appointing a Senior Agency Official (SAO) to direct and administer the CNSI program under which the information is protected throughout its lifecycle.
- (2) The Chief, FMSS is responsible for:
 - a. Overseeing, as SAO, the IRS CNSI program and NISP.
 - b. Approving and issuing IRS security policies and guidance for the conduct of the CNSI program and NISP.
 - c. Establishing and maintaining an ongoing CNSI self-assessment program, which includes periodic review and assessment of the IRS CNSI holdings and classification products in accordance with 32 CFR 2001, TD P 15-71, Chapter 3, Section 31 and this IRM 10.9.1.
 - d. Establishing that risks associated with the CNSI program are identified, analyzed, responded to, reported on, and monitored to ensure the program's health and compliance with National and Treasury guidance.
 - e. Ensuring the timely and accurate response on the ISOO annual request for completion of the Standard Form (SF) 311, Agency Security Classification Management Program Data.
 - f. Delegating the signature authority for courier letters and cards to the Associate Director (AD), Security. This serves as the official delegation.
 - g. Serving as the approval authority for the IRS on Sensitive Compartmented Information Facility (SCIF) Justification Memoranda prior to sending to Treasury for final approval.
 - h. Coordinating with other Agencies as the IRS liaison on classification challenges and requests for declassification or reclassification.

- (3) The Associate Director (AD), Security, FMSS is responsible for:
 - a. Administering and directing the IRS CNSI program and NISP on behalf of the SAO.
 - b. Appointing Program Managers responsible for execution of the CNSI program and NISP.
 - c. Ensuring the coordination and performance of self-assessments for the CNSI program.
 - d. Serving as the IRS approval authority for Security Areas, to include Top Secret Spaces, by signing their certification letters (Open Storage of Secret or Top Secret Spaces) or submitting them to Treasury (Treasury Secure Data Network (TSDN) Limited Areas (LA)), as applicable.
 - e. Serving as review authority for SCIF Justification Memoranda.
 - f. Reviewing and approving, as applicable, administrative and risk-based decision documentation regarding the IRS CNSI program.
- (4) The Senior Executive responsible for an office or a business, functional or operating unit is responsible for:
 - a. Ensuring effective management of CNSI within their organization.
 - b. Ensuring that CNSI within their organization is appropriately protected throughout its lifecycle in accordance with this IRM.
 - c. Ensuring that non-Senior Executive Service employees with a security clearance are rated on their protection of CNSI annually via Form 15283, Classified National Security Information Critical Element for Employees Whose Duties Require a National Security Clearance.
- (5) The Senior Manager(s) in an office or a business, functional, or operating unit is responsible for:
 - a. Ensuring effective management of CNSI within their organization.
 - b. Verifying the clearance of and designating, as needed, a primary and alternate Classified Document Custodian(s) (CDC) in writing.
 - c. Ensuring the CDC is trained and provided the resources to protect CNSI.
 - d. Ensuring the CNSI Program Manager (PM) is made aware of changes to the Classified Document Custodian appointments.
 - e. Justifying the need for and, if approved, appointing a Top Secret Control Officer in writing.
 - f. Ensuring the CDC conducts self-assessments as prescribed by FMSS Security.
 - g. Appointing a Top Secret Control Officer after a Top Secret Space is certified or SCIF is accredited.
 - h. Appointing, in the event of a security incident, an appropriately cleared alternate Inquiry Official if the local CDC is materially involved.
 - i. Ensuring that subordinate managers and staff participate fully in an inquiry into a security incident, and, as applicable, that appropriate remediations for clearance holders found at fault in a security incident are applied.
 - j. Ensuring authorized holders are rated on their protection of CNSI at the end of each rating period.
- (6) The Security Section Chief (SSC) is responsible for:
 - a. Coordinating with security contractor(s), Business Units and CNSI PM on physical security requirements, upgrades, or construction related to CNSI.

- b. Ensuring physical security requirements in national, Treasury and IRS guidance are implemented as appropriate.
- (7) CNSI Program Manager (PM) is responsible for:
- a. Managing the IRS CNSI program and NISP on behalf of the SAO.
 - b. Authoring and updating CNSI and NISP policy in accordance with Authorities in this IRM.
 - c. Completing the annual ISOO SF 311 and sending to the AD, Security.
 - d. Serving as the liaison for classification challenges, reclassification requests, declassification confirmation, courier cards/letters, and security incidents between IRS and Department of Treasury and/or other Agencies as required.
 - e. Ensuring a system exists to process, track and record formal classification challenges, reclassification requests, declassification requests, courier cards/letters, and security incidents.
 - f. Hosting, granting and removing access to the Security Container Tracker based upon input from the field.
 - g. Coordinating with those involved in procurements requiring NISP compliance to ensure the appropriate security features appear in contractual documents.
 - h. Ensuring all CNSI and NISP related security, education, and awareness training is implemented in accordance with authorities in this IRM.
 - i. Serving as a single point of contact at the headquarters level on all security matters related to Security Areas that protect CNSI to include the approvals, certification letters, and provisions of security policy.
- (8) The Top Secret Control Officer is responsible for:
- a. Maintaining a Top Secret security clearance, at minimum, and receiving training from Treasury Office of Intelligence and Analysis if the information held is at the Top Secret/Sensitive Compartmented Information (TS/SCI) level.
 - b. Ensuring Top Secret information is protected throughout its lifecycle per the requirements in this IRM.
 - c. Maintaining current accountability records of Top Secret information received within their office and attendant supply of Top Secret document forms.
 - d. Following prohibitions against reproduction of Top Secret information.
 - e. Ensuring Business Unit authorized holders know to immediately notify their Top Secret Control Officer whenever they receive any Top Secret material.
 - f. Maintaining Treasury Department Form (TD F) 15-05.4, Document Control Register, for all Top Secret information held by the Business Unit.
 - g. Conducting an annual physical inventory of Top Secret information within the Business Unit under their purview using TD F 15-05.4, with the designated alternate Top Secret Control Officer (if appointed) or another authorized holder to serve as witness.
 - h. Downgrading, declassifying, or destroying Top Secret documents, as appropriate, per this IRM.
 - i. Maintaining accountability records, receipts of the transmission, and receipts of destruction of Top Secret information.
 - j. Verifying authorized holders that receive Top Secret information have the appropriate security clearance, need-to-know, and storage capability that has been approved by AD, Security prior to the information being released.

Note: A Top Secret Control Officer is appointed by the Business Unit who owns the accredited Top Secret Space or SCIF. A Top Secret Control Officer can serve concurrently as Classified Document Custodian and/or Security Container Custodian.

- (9) The Classified Document Custodians, both a primary and alternate, are responsible for:
- a. Serving as the principal advisor to the appointing official and supervisor in matters pertaining to security of CNSI.
 - b. Providing full name(s) of replacements to CNSI PMs prior to departure from the role.
 - c. Serving as Cognizant Security Official by providing guidance to authorized holders regarding protection of CNSI and discussing issues/solutions with the CNSI PMs.
 - d. Conducting self-assessments as laid out in subsection IRM 10.9.1.15.
 - e. Conducting incident inquiries in accordance with subsection IRM 10.9.1.14 and provide timely updates to management and CNSI PM.
 - f. Coordinating with Treasury Inspector General for Tax Administration (TIGTA), CSIRC, and CNSI PM on security incidents.
 - g. Ensuring that access to CNSI is limited to authorized holders with a need-to-know as defined in subsection IRM 10.9.1.8.1.
 - h. Annually verifying the Security Container Tracker for all containers used to store CNSI under their purview.
 - i. Clearing security containers prior to being decommissioned in accordance with this subsection IRM 10.9.1.8.4(9).
 - j. Maintaining combinations of security containers under their control in accordance with the manufacturer's operating instructions and this IRM.
 - k. Creating and maintaining a list of the CNSI to be taken on travel and, upon return, verifying that all CNSI has been returned by the authorized holders who traveled.
 - l. Establishing written administrative procedures for the control of CNSI under their control in line with this IRM. At a minimum, procedures must cover:
 - i. Information, dissemination, and reproduction control measures that fit the local environment.
 - ii. Personnel security clearances and need-to-know verification.
 - iii. End-of-day and after-hours security checks.
 - iv. Whether security container combination storage will be centralized in one container or decentralized among many.
 - v. Additional protections for CNSI telephone conversations in spaces certified by Business Units to host them.
 - vi. Emergency procedures for protecting CNSI in the event of an emergency.

Note: Classified Document Custodians must be appointed at every facility that houses CNSI under a given senior manager (e.g., if two Business Units have CNSI at a given facility, each Business Unit must appoint a primary/alternate for their CNSI; if necessary, the alternate CDC may be located at another facility). If the facility is a large, multi-building campus or similar with a multitude of security containers, then senior management should decide how many Classified Document Custodians should work in concert to ensure the safety of the CNSI. Senior Management must verify that the

appointed Classified Document Custodian has a clearance commensurate with the highest level of the CNSI present at the facility(ies) for which they are responsible prior to their appointment. The Classified Document Custodian's responsibilities must be removed in the event of the clearance's lapse. Classified Document Custodians may serve concurrently as Top Secret Control Officer and/or Security Container Custodian.

(10) The Security Container Custodian is responsible for:

- a. Implementing the administrative procedures laid out by this IRM and the local Classified Document Custodian for the security container(s) under the Custodian's purview.
- b. Ensuring authorized holders requesting access to the security container be verified by Personnel Security (*hco.ps.national.security.programs@irs.gov*) to have the clearance of the highest level of information stored in the security container and the requisite need-to-know, as defined in Terms/Definitions/Acronyms.
- c. Listing their information on the SF 700, Security Container Information on all security containers assigned security containers.
- d. Ensuring the container combination is turned over to the local Classified Document Custodian and the next Security Container Custodian prior to their departure from their position.
- e. Ensuring the individuals with access to the container properly use the SF 701, Activity Security Checklist, as required and SF 702, Security Container Check Sheet, by discussing the requirements and reviewing the forms every 90 calendar days for compliance.
- f. Ensuring a list of those with access to a container is maintained for the purposes of combination maintenance.
- g. Maintaining and changing the combination to security containers in accordance with the manufacturers operating instructions and this IRM.
- h. Ensuring authorized holders with access to the security container perform an annual review of material in the container to ensure that the classified material is:
 - i. appropriately marked,
 - ii. required for job performance/records, purposes and
 - iii. destroyed, as applicable, in a National Security Agency/Central Security Service (NSA/CSS) Evaluated Products List (EPL) approved shredder.
- i. Ensuring the Classified Document Custodian is aware of security container movements or decommissioning.
- j. Clearing the security container prior to being decommissioned in accordance with subsection IRM 10.9.1.8.4(9).

Note: This subsection applies to any individual who is responsible for a security container, regardless of Business Unit. A Security Container Custodian must be appointed for every security container owned by the Business Unit and may serve concurrently as Top Secret Control Officers and/or CDCs.

(11) The Security Area Responsible Party is responsible for:

- a. Serving as the primary Point of Contact (POC) of the Business Unit who is responsible for the Security Area and appointing an alternate POC from Authorized Personnel when unavailable to perform duties listed in b) - q) below.
- b. Being designated as one of the individual(s) listed on the SF 700 the secure side of the Security Area's entry door.
- c. Serving as liaison on the Security requirements for the Security Area, including but not limited to:
 - i. Coordinating with CNSI PMs to procure required security items (shredder, security container, etc.).
 - ii. Physical Security requirements.
 - iii. Behavioral compliance in protecting CNSI.
 - iv. Self-assessments in conjunction with the Classified Document Custodian.
- d. Responding to a Security Area when called in the event of an alarm, disturbance, or facility emergency. In the event of a safety concern, the monitoring entity must be informed prior to Responsible Party entering.
- e. Ensuring year-round coverage for after-hours response.
- f. Verifying the clearance and need-to-know of all Authorized Personnel prior to granting them access.
- g. Verifying the clearance and need-to-know of visitors, ensuring those who are unauthorized are escorted.
- h. Ensuring the lock and combination for the access door is maintained and changed as prescribed in subsection IRM 10.9.1.8.4(6), Federal Specification FF-L-2740, Locks Combination, and the manufacturer's operating manual.
- i. Ensuring that utilization of IRS Form 5421 Limited Area Register and on-site storage of the register for one year.
- j. Participating in and accommodating any security assessments or security incident inquiries.
- k. Issuing, or ensuring the issuance of, local written procedures for the Security Area that includes life safety requirements and Occupant Emergency Plans in accordance with TD P 15-71, Chapter 5, Section 1,9.
 - i. Arranging for a security container in another room in which to store CNSI typically held in a Security Area in the event of emergency in consultation with the local Classified Document Custodian.
- l. Reviewing access lists to Security Areas biannually, to include validating clearances, and coordinate with the SSC to remove those who no longer meet the requirements of access or who no longer require access.
- m. Ensuring the removal of Authorized Personnel who no longer require access from the access control system promptly.
- n. Updating the monitoring entity promptly when changes occur to the after-hours response list.
- o. Monitoring and securing any keys for the Security Area doors per subsection IRM 10.9.1.8.4(5).
- p. Preventing unauthorized access to the Security Area by ensuring that a Responsible Party or Authorized Personnel for the space physically controls the entry/exit door should either need to be opened for any length of time (due to an emergency or other).

- q. Serving as the Key Custodian for keys to Security Areas, as specified in this IRM.

Note: This subsection applies to any individual named Responsible Party for an Open Storage Security Area or Treasury Secure Data Network (TSDN) Limited Area (LA) by the Business Unit who owns the space. This person can serve concurrently as a Top Secret Control Officer, Security Container Custodian, and/or Classified Document Custodian.

- (12) The Authorized Personnel is responsible for:

- a. Serving as alternate Responsible Party if appointed.
- b. Protecting CNSI and Security Areas by following this IRM.
- c. Escorting unauthorized individuals inside Security Areas.
- d. Responding, if designated by the Responsible Party, in the event of an alarm or disturbance or facility emergency. In the event of a safety concern, the monitoring entity must be informed prior to Authorized Personnel entering the Security Area.
- e. Opening and closing the Security Area to accommodate business hours in a secure manner, as directed by the Responsible Party.

Note: This subsection applies to any individual, regardless of Business Unit who owns the Security Area, granted Authorized Personnel privileges for an Open Storage Security Area or TSDN LA.

- (13) The Inquiry Official is responsible for:

- a. Serving as a neutral party to the security incident (e.g., not involved in the events leading up to or directly causing the security incident).
- b. Holding a security clearance commensurate with the level of CNSI the security incident involves if the Inquiry requires review of classified information.
- c. Familiarizing themselves with this subsection IRM 10.9.1.14, regarding the conduct of the inquiry and meeting the deadlines associated.
- d. Preventing further unauthorized disclosure of CNSI, as prescribed throughout this document.

Note: This subsection applies to any individual, regardless of Business Unit, who is appointed to be the Inquiry Official. This role is typically filled by the local Classified Document Custodian but may need to be appointed by the CNSI PMs if there is a conflict of interest.

- (14) The authorized holder of CNSI is responsible for:

- a. Ensuring consistent protection of CNSI from unauthorized disclosure by meeting safeguarding requirements prescribed throughout this document.
- b. Contacting the local Classified Document Custodian promptly in an unclassified manner in the event of a security incident, either infraction or violation.
- c. Ensuring that CNSI is not communicated over unsecured voice or data systems, (e.g., IRS network, phone line, cell phones, etc.) in public conveyances or places, or in any other manner that permits interception by unauthorized personnel.
- d. Completing the required annual training -Integrated Talent Management Item, "Annual Security and Derivative Classification Brief."

Note: This subsection applies to any individual, regardless of Business Unit, who possesses a security clearance for the performance of their duties at the IRS.

- (15) The authorized holders working at another agency or organization are responsible for:
 - a. Following the CNSI policies and procedures of both the IRS and the agency they are working at.
 - b. Completing the annual training - Integrated Talent Management “Annual Security and Derivative Classification Brief.”
 - c. Ensuring the request of an IRS issued courier device, as needed, to courier CNSI from IRS to other authorized holders in accordance with subsection IRM 10.9.1.10.1.
- (16) The authorized holders detailed to another agency or organization are responsible for:
 - a. Following the CNSI policies and procedures of the agency they are detailed to.
 - b. Completed the annual training - Integrated Talent Management Item, “Annual Security and Derivative Classification Brief.”
 - c. Returning any IRS issued courier device prior to going on detail and obtaining one, as required, from the agency they are detailed to.
 - d. Notifying the CI Security Specialist and/or CNSI PMs of their involvement in a security incident, either infraction or violation.

10.9.1.1.4
(11-06-2023)
**Program Management
and Review**

- (1) **Program Reports:** The CNSI program will be assessed via self-assessment at an interval set by AD, Security. The CNSI PM will direct the self-assessment program. The designated Classified Document Custodian is responsible for conducting the self-assessment in local field offices where CNSI is held. Annual reporting on the health of the CNSI program, based on the self-assessments takes place via the SF 311 per TD P 15-71. The SF 311 reporting will occur to ISOO by the end of fiscal year.

10.9.1.1.5
(11-06-2023)
Program Controls

- (1) The CNSI Program requests Business Units that handle CNSI through its life cycle conduct an annual self-assessment indicating the status of their organization’s protection of classified material and compliance with relevant policies. The CNSI program managers compile the data into a report for FMSS AD, Security, Chief, Protection Management, and signature of the Chief, FMSS. This report is sent by the CNSI Program to the Department of Treasury CNSI Program using the SF-311.

10.9.1.1.6
(11-06-2023)
**Terms/Definitions/
Acronyms**

- (1) **Access** - The ability and opportunity to obtain knowledge or possession of CNSI information and material or access to Security Areas processing CNSI.
- (2) **Agency** - Any “Executive Agency,” as defined in 5 United States Code (USC) 105, and any other entity within the executive branch that comes into the possession of CNSI.
- (3) **Authorized Holder** - A Federal employee who has a favorable determination of eligibility (e.g., security clearance) for access to CNSI, signed an approved nondisclosure agreement, and has a need-to-know the CNSI in the performance of official duties, and has fulfilled the requirement to take the annual

Integrated Talent Management Item, “Annual Security and Derivative Classification Brief.” This includes contractor personnel on a NISP compliant contractor personnel on a NISP compliant contract who meet the same qualifications. Employees who are holders of, or have access to, CNSI or serve as Classified Document Custodians, CNSI PMs, or Responsible Party(ies) must be authorized holders.

- (4) **Authorized Personnel** - An IRS authorized holder, vetted by the Responsible Party(ies) and Personnel Security, with a valid work requirement who is allowed unrestricted access to the Security Area and given the combination to both the door and the Intrusion Detection System (IDS).
- (5) **Automated Information System (AIS)** - An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.
- (6) **Automatic Declassification** - The declassification of information based solely on the occurrence of a specific date or event as determined by an Original Classification Authority (OCA) or the expiration of a maximum timeframe for the duration of classification established under EO 13526.
- (7) **Classification** - The process by which information is determined to be CNSI either by original or derivative means as discussed in subsection IRM 10.9.1.3 and IRM 10.9.1.3.2.
- (8) **Classification Guide** - A documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. OSP’s classification guidance will be used, as IRS does not have its own Classification Guide.
- (9) **Classification Management** - Classification management seeks to ensure that official information is classified only when required in the interest of national security and is properly identified and retains the classification assigned if necessary.
- (10) **Classified National Security Information (CNSI)** - Information that has been determined pursuant to EO 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status regardless of its form (document, technology, equipment, etc.). Termed “CNSI” in this IRM.
- (11) **Closer** - A Responsible Party or Authorized Personnel who is entrusted with the task of closing the Security Area in a secure manner at the end of the business day.
- (12) **Cognizant Security Official** - An employee of the Federal government (e.g., Classified Document Custodian, Regional Security Officer, Special Security Officer (SSO)) charged with responsibility for physical, technical, personnel, and information security affecting that organization.
- (13) **Communications Security (COMSEC)** - Measures and controls taken to deny unauthorized personnel information derived from telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptographic security, transmission security, emission security, and physical security of COMSEC material.

- (14) **Compromise** - The unauthorized disclosure of CNSI to an individual without the appropriate clearance or need-to-know.
- (15) **Confidential** - The classification level applied only to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.
- (16) **Control** - The authority of an agency that originates CNSI, or its successor in function, to regulate access to the information.
- (17) **Declassification** - The authorized change in the status of information from CNSI to unclassified and the subsequent revision of associated markings.
- (18) **Declassification Authority** - Officials delegated declassification authority in writing by the Secretary of Treasury or Treasury's Senior Agency Official (SAO) responsible for Treasury's CNSI program.
- (19) **Declassification Guide** - The written instructions issued by a declassification authority that detail what specific elements of information may be declassified and the elements that must remain classified.
- (20) **Derivative Classification** - The 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 to the source information. Derivative classification includes the classification of information based on a classification guide. The duplication or reproduction, such as copying or printing, of existing CNSI is not derivative classification.
- (21) **Disclosure** - The communication or physical transfer of CNSI to an unauthorized recipient by showing or revealing CNSI, whether orally, in writing or any other medium (e.g., video, graphic, etc.).
- (22) **Downgrading** - A determination by a downgrading/declassification authority that information classified and safeguarded at a specified level must be classified and safeguarded at a lower level.
- (23) **Foreign Government Information (FGI)** - Information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence. -OR- Information produced by the U.S. Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence. -OR- Information received and treated as "Foreign Government Information" pursuant to the terms of a predecessor order to EO 13526.
- (24) **Industrial Security** - The segment of security concerned with protecting CNSI released to and in the possession of contractors. This term describes the program under which the United States Government (USG) engages in a contract that has security policies and responsibilities for safeguarding the CNSI, CNSI systems, assets or facilities, which are imposed on the contractor, and in which the USG provides guidance to and conducts oversight of contractor implementation of those policies.

- (25) **Information Security** - The program established by EO for the classification, declassification, downgrading, and safeguarding of CNSI. This includes protection of Sensitive but Unclassified (SBU), non-national security information.
- (26) **Lines of Inquiry (LOI)** - Discreet, measurable items reviewed during an assessment to ascertain the operational ability of a program.
- (27) **Limited Area** - An Area to which access is limited to Authorized Personnel only and requires a two-factor authentication mechanism to gain access.
- (28) **Mandatory Declassification Review** - The review for declassification of CNSI in response to a request for declassification that meets the requirements for EO 13526.
- (29) **Material** - In the context of a security incident, an individual is considered material to the inquiry if they were a part of the issue that lead to the incident or if they have knowledge regarding the incident that will influence, or is crucial to, the inquiry.
- (30) **Monitoring Entity** - The entity responsible for the monitoring of alarms linked to Security Areas.
- (31) **National Security** - The national defense or foreign relations of the U.S. and includes, with a Treasury context, U.S. economic vitality, global competitiveness, market sensitivity, and tracking terrorist assets/financial crimes.
- (32) **National Security Clearance** - Certification issued by a designated personnel security official or designee that a person may access up to Secret or Top Secret CNSI on a need-to-know basis granted after a valid, in scope Tier 3 or Tier 5 investigation, respectively.
- (33) **Need-to-know** - A determination by the employee's direct management and HCO that an employee requires access to CNSI to perform or assist in a lawful and authorized governmental function.
- (34) **Non-Disclosure Agreement (NDA)** - An officially authorized contract between an individual and the USG signed by an individual as a condition of access to CNSI and specifying the security requirements for the access and details the penalties for noncompliance carried out via the SF 312, Classified Information Nondisclosure Agreement.
- (35) **North Atlantic Treaty Organization (NATO)** - NATO is an alliance of countries from Europe and North America enabling cooperation in the field of defense, security and crisis-management. As a participant in NATO, the U.S., and therefore IRS, must protect NATO CNSI in accordance with, NATO Instruction 1-07, Implementation of NATO Security Requirements. The information in this Manual applies only to NATO CNSI.
- (36) **Open Storage** - The storage of CNSI openly (i.e., not requiring storage inside a security container) when Authorized Personnel do not occupy the facility. In all instances, "open storage" must be specifically approved in writing by OSP to store CNSI at the Secret level. This term is used in concert with TSDN LA.
- (37) **Opener** - A Responsible Party or Authorized Personnel who is entrusted with the task of opening the Security Area in a secure manner at the beginning of the business day.

- (38) **Original Classification** - The initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.
- (39) **Original Classification Authority(ies) (OCA)** - An individual authorized in writing, either by the President or by agency heads, or other officials designated by the President, to classify information in the first instance. Within Treasury, OCA are designated by the Secretary (at the Top Secret, Secret, or Confidential levels) or by the Department's SAO (at the Secret or Confidential levels). IRS does not have an OCA.
- (40) **Paragraph or Portion Markings** - Required markings on classified documents to indicate the specific level of classification applicable to each paragraph or portion of a document shown as follows: (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified.
- (41) **Personnel Security** - The segment of security that concerns the trustworthiness and integrity of Federal employees and others associated with the USG. It is also the process in the USG for complying with national security interest requirements under EO 10450 or with other similar authority.
- (42) **Physical Security** - The segment of security concerning protective requirements and means for safeguarding IRS employees, property, facilities, and information.
- (43) **Public Trust** - Investigations (Tier 1, Low Risk; Tier 2, Moderate Risk; Tier 4, High Risk) performed to ascertain whether an individual is suitable or eligible to work in sensitive or public trust positions.
- (44) **Responder** - A designated, cleared Responsible Party or Authorized Personnel who will respond when called, regardless of day or time, to the Security Area to perform a walkthrough in the event of an alarm.
- (45) **Response Force** - The portion of the monitoring entity that responds to the Security Area in an alarm event and remains until a responder arrives to perform a walkthrough.
- (46) **Responsible Party** - An IRS authorized holder who is accountable for ensuring the Security Area remains secure, that those with access are vetted and trained, and that the responder list is maintained.
- (47) **Safeguarding or Safeguards** - Physical, procedural, or electronic measures and controls prescribed to ensure CNSI and SBU is not accessed inadvertently or improperly.
- (48) **Secret** - The classification level applied only to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.
- (49) **Secure Telephone Equipment (STE)** - The USG current encrypted telephone communications system for wired or "landline" communications, for example the Sectera vIPer.
- (50) **Security Area** - Consists of either controlled or limited areas, which require individual access authentication to gain entry. It is noted that in the Treasury Directive Policy (TD P) 15-71, Treasury Security Manual, the overarching term

for areas requiring security to protect assets is termed “Controlled Area” but the term “Controlled Area” is used in IRS as a specific type of area requiring physical security.

- (51) **Security Classification Guide (SCG)** - A documentary form of guidance, issued by an OCA, providing the user with instructions on what types of information may be classified and the level/duration thereof.
- (52) **Security Container** - A General Services Administration (GSA) approved security container equipped with built-in (mounted), dial-type, changeable combination lock, specifically designed for the CNSI. A security container may be used for protecting money and other highly negotiable materials or assets; however, this IRM only applies to any container housing CNSI.
- (53) **Security Container Tracker** - A system created and hosted by the CNSI PM for the Classified Document Custodians and Security Container Custodians to maintain the status of the security containers used to protect CNSI.
- (54) **Security Clearance** - An administrative authorization for access to CNSI, up to a stated classification level (Top Secret, Secret, or Confidential), and referred to as a clearance.
- (55) **Security Countermeasures** - Actions, devices, procedures, and/or techniques to reduce security risks.
- (56) **Security Incident** - An act that constitutes a threat to a security program or is a deviation from existing security regulations. Security incidents will be categorized as security infractions or violations.
- (57) **Security-in-Depth** - A determination by the agency head, or designee, that a facility’s security program consists of layered and complementary security controls enough to deter and detect unauthorized entry and movement within a facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an intrusion detection system, random guard controls, etc.
- (58) **Security Infraction** - Any knowing, willful, or negligent action contrary to the requirements of EO 13526 or its implementing directives that does not result in an unauthorized disclosure CNSI.
- (59) **Security Violation** - Any knowing, willful, or negligent action that could reasonably be expected 1) to result in an unauthorized disclosure of CNSI, 2) to classify or continue the classification of information contrary to the requirements of EO 13526 or its implementing directives, or 3) to create or continue a special access program contrary to EO 13526.
- (60) **Senior Agency Official (SAO)** - The official designated by the agency head under EO 13526 to direct and administer the agency’s security program, under which information is classified, safeguarded, handled, or declassified.
- (61) **Sensitive but Unclassified (SBU)** - Treasury, bureaus, or another authority has determined to require protection from unauthorized or unwarranted public disclosure.

- (62) **Sensitive Compartmented Information (SCI)** - Information concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established by the Director National Intelligence (DNI).
- (63) **SCI Facility(ies) (SCIF)** - An area or installation certified and accredited as meeting DNI security standards for the processing, storage and/or discussion of SCI. SCIF must be coordinated by the Business Unit via the CNSI PMs with Treasury's SSO in advance of construction.
- (64) **Sensitive Position** - Any position the occupant of which could bring about, by virtue of the nature of the position and access to CNSI, a materially adverse effect on the national security, the mission of the Department, or the IRS. All sensitive positions are designated as either non-critical sensitive, critical sensitive, or special sensitive.
- (65) **Source Document** - An existing document containing CNSI that can be incorporated, paraphrased, restated, or generated into a new document.
- (66) **Systemic Declassification Review** - The review for declassification of CNSI contained in records the Archivist of the U.S. has determined to have a permanent historical value in accordance with 44 U.S.C. 2107.
- (67) **Threat** - The intention and capability of an adversary to undertake actions that would be detrimental to the interests of the U.S.
- (68) **Top Secret (TS)** - The classification level applied only to information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe. Approval from the AD, Security is needed prior to storing TS.
- (69) **Treasury Secure Data Network (TSDN) Limited Area (LA)** - A room that offers the protection necessary to store CNSI systems and material up to the Secret level through a combination of Protective Service Officers (PSO), responders, detectors/alarms, and/or locking devices.
- (70) **Unauthorized Personnel** - An individual lacking appropriate level of security clearance, need-to-know, SF 312, or annual CNSI Refresher Briefing.
- (71) **Unauthorized Disclosure** - Communication or physical transfer of classified information to unauthorized personnel (e.g., those who lack the appropriate security clearance or need-to-know).
- (72) **Visitor** - Any person who is not a Responsible Party or Authorized Personnel for the Security Area, regardless of the visitor's level of clearance and need-to-know.

Acronyms

Acronym	Definition
A/S	Assistant Secretary
AO	Accrediting Official
CA	Controlled Area

Acronym	Definition
CFR	Code of Federal Regulations
CI	Criminal Investigation
CNSI	Classified National Security Information
CNSI PM	Classified National Security Information Program Manager
CO	Contracting Officer
COMSEC	Communications Security
COR	Contracting Officer's Representative
DCSA	Defense Counterintelligence Security Agency
DD F	Department of Defense Form
DNI	Defense National Intelligence
DO	Treasury's Departmental Offices
EO	Executive Order
EPL	Evaluated Product List
ERC	Employee Resource Center
FCL	Facility Security Clearance
FF-L	Federal Specification
FGI	Foreign Government Information
FOIA	Freedom of Information Act
FSL	Facility Security Level
FY	Fiscal Year
GSA	General Services Administration
HCO	Human Capital Office
ICD	Intelligence Community Directives
IDS	Intrusion Detection System
IPS	Information Processing System
ISCAP	Interagency Security Classification Appeals Panel
ISOO	Information Security Oversight Office
LA	Limited Area
NATO	North Atlantic Treaty Organization

Acronym	Definition
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
NSA	National Security Agency, aka NSA/Central Security Service (CSS)
OCA	Original Classification Authority
OCIO	Office of the Chief Information Officer
OSP	Treasury's Office of Security Programs
PD	Position Description
POC	Point of Contact
SAO	Senior Agency Official
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	SCI Facility
SCG	Security Classification Guide
SF	Standard Form
SSM	Site Security Manager
SSO	Special Security Office (part of Treasury)
STE	Secure Telephone Equipment
TCS	Treasury Communications System
TD	Treasury Directive
TD F	Treasury Department Form
TD P	Treasury Directive Publication
TFIN	Treasury Foreign Intelligence Network
TO	Treasury Order
TSA	Transportation Security Agency
TSDN	Treasury Secure Data Network
TSDN LA	Treasury Secure Data Network Limited Area

Acronym	Definition
USC	United States Code
USG	United States (U.S.) Government
USSAN	United States Security Authority for NATO

10.9.1.1.7
(11-06-2023)

Related Resources

- (1) *IRS CNSI and NISP Website*, updated as new versions of the forms are issued
- (2) *ISOO Marking Guide*
- (3) *Department of Treasury Security Classification Guide* (document is FOUO)
- (4) *NSA/CSS EPL for Shredders*
- (5) *NSA/CSS EPL for Degaussers*
- (6) *IRM 10.2.14, Methods of Providing Protection*
- (7) *IRM 10.2.18, Physical Access Control (PAC)*
- (8) *IRM 10.23.1, National Security Positions and Access to Classified Information*
- (9) *IRM 10.23.3, Personnel Security/Suitability for Employment and Personnel Security Operations*
- (10) *Physical Security Design Manual*

10.9.1.2
(11-06-2023)

Classification Levels

- (1) CNSI will be identified by one of the following three levels:
 - a. "Top Secret" will be applied to information that could be expected to cause exceptionally grave damage to the National Security; the OCA must be able to identify or describe the damage to the national security that may occur.
 - b. "Secret" will be applied to information that could be expected to cause serious damage to the national security; the OCA must be able to identify or describe that serious damage to the national security may occur.
 - c. "Confidential" will be applied to information that could be expected to cause damage to the national security; the OCA must be able to identify or describe the damage to the national security that may occur.
- (2) No terms other than Confidential, Secret, or Top Secret will be used to identify CNSI, except as otherwise provided by statute.

10.9.1.3
(11-06-2023)

Original Classification and Original Classification Authority

- (1) CNSI is information that has been determined pursuant to EO 13526 Section 1.4, any predecessor order, and its implementing directive Information Security Oversight Office (ISOO) Directive No. 1, 32 CFR Parts 2001 and 2003, to require protection against unauthorized disclosure and is marked to indicate its classified status. Information may be originally classified only if its unauthorized disclosure could reasonably be expected to result in damage to the national security.

- a. Original Classification Authority(ies) (OCA) are those authorized to originally classify information. OCA are designated by the President and are typically heads of agencies or other officials.
 - b. Delegations of OCA by agency heads to subordinates are limited and the agency head must ensure that the subordinates have demonstrable and continuing need to maintain the delegation.
- (2) No information may remain classified indefinitely; declassification instructions are created by the OCA at the time of original classification based on EO 13526. Upon reaching the date or event specified on the CNSI, the information will be automatically declassified.
- (3) OCA must be delegated in writing to IRS officials by the Secretary of Treasury and Treasury's SAO.
- a. As there is no OCA in IRS (currently or historically), the requirements for declassification reviews noted in EO 13526 do not apply.
 - b. As there is no OCA in IRS, redactions of CNSI in Freedom of Information Act (FOIA) reviews are not performed by IRS.
- (4) Should a need for OCA authority develop within IRS, the official requesting it will coordinate with the CNSI PM in advance of OCA decisions being made. Until, and if OCA is granted to IRS, Treasury OCAs will be requested to handle original classification decisions.

10.9.1.3.1
(04-13-2021)

**Limits to Classification
and Reclassification**

- (1) In no case will CNSI remain classified or be reclassified to:
- a. Conceal violations of law, inefficiency, or administrative error.
 - b. Prevent embarrassment to a person, organization, or agency.
 - c. Restrain competition.
 - d. Prevent or delay the release of information that does not require protection in the interest of the national security.
- (2) Information may not be reclassified after declassification and subsequent release to the public under proper authority unless:
- a. The reclassification action is approved in writing by the Secretary of Treasury based on the determination that reclassification is required to prevent significant, demonstrable damage to national security and the information may be reasonably recovered without bringing undue attention.
 - b. The reclassification request is reported promptly through the CNSI PM to the Director, OSP.

10.9.1.3.2
(04-13-2021)

Derivative Classification

- (1) Derivative classification is the restatement of existing CNSI by unauthorized holders who reproduce, extract, summarize, or apply classification markings derived from source material or as directed by a classification guide. Derivative can also mean incorporating, paraphrasing, restating, or generating in new form or information that is already classified and marking the newly developed material consistent with the classification markings that apply to the source information.
- (2) The basis for derivative classification actions involves use of one or more of the following types of information:
- a. Existing classified source document.

- b. Approved classification guide.
 - c. Classified communication (e.g., information provided orally via STE or obtained/discussed during a classified meeting).
- (3) Derivative classification may be exercised by any authorized holder, including consultants or contractors under the National Industrial Security Program (NISP), who have received initial derivative training prior to creating derivative decisions and/or are current on the required biannual derivative training. Derivative classifiers will keep accessible up-to-date, official materials that aid in their ability to perform accurate derivative classification (i.e., TD P 15-71, Chapter III, Section 6; ISOO Marking Guide; ISOO Derivative Classification training video).

10.9.1.3.3
(11-06-2023)
**Classification
Challenges**

- (1) Information classified under EO 13526 and prior EO is subject to challenge by any authorized holder of the information. Authorized holders are defined as:
- a. Cleared USG authorized holder who is a recipient of the CNSI in the course of conducting official business.
 - b. Agency security official who is responsible for properly safeguarding classified information.
 - c. Contractor or consultant on a contract with classified scope per the NISP.
- (2) Challenges of classification decisions are intended to bring about corrective action that ensures only information legitimately requiring protection based upon criteria in EO 13526 is appropriately classified. The decision to challenge is based on one of the following assumptions:
- a. Information should/should not be classified.
 - b. Information should be classified at a lower/higher level (under/over-classification).
 - c. Information is improperly classified (including an overly restrictive period or without proper authority).
 - d. Information is improperly marked.
- (3) Those who exercise a classification challenge will not be subjected to adverse action, reprisal, retribution, retaliation based on their election to engage the challenge provision.

10.9.1.3.3.1
(11-06-2023)
**Challenge Requirement
and Handling**

- (1) Classification challenges must be kept unclassified, whenever possible, and sufficiently describe the information being challenged to enable the classifier (or designee) to locate it with a reasonable amount of effort. Regardless of the originating agency, the CNSI PM must be directly sent the initial challenge. The authorized holder challenging the classification:
- a. Identifies their rationale behind the challenge. Rationale for informal challenges can be as simple as questioning why information is or is not classified at a certain level. Formal challenges should include why the challenger believes the information is improperly or unnecessarily classified.
 - b. Ensures that the material in question is suitably protected to prevent unauthorized access commensurate with the level of classification initially assigned to the information, if the information was classified at the time of the challenge. This includes marking, packaging, transmittal, accountability, couriering, reproduction, etc., until such time as a decision is reached.

- c. Ensures the information, in the case of any material that the holder believes should be CNSI but has not been classified and marked at the time of the challenge, is protected at the Secret level pending the final decision.
 - d. Collaborates with the CNSI PM to report to appropriate classifiers any conditions that lead an authorized holder to feel the classification is improper, needless or restrictive.
 - e. Notifies, in an unclassified manner, all authorized holders accessing or holding the information undergoing the challenge that the CNSI is undergoing a challenge.
- (2) Informal challenges involving Treasury information:
- a. Informal challenges are used when the information is originated in Treasury only. The CNSI PM engages with the Chief, FMSS to coordinate with Treasury's SAO on ensuring completion of the challenge review and reporting the results of the review in writing to the requester.
 - b. The requester makes a written request with justification of the reason for changes to the classification or markings.
 - c. The Original Classifier determines whether the classification and markings meet guidance. If there is an error, the correction is made, new material is sent to the requester and old material is destroyed.
 - d. If the Original Classifier does not believe an error has occurred, the requester is informed. If the requester decides not to appeal, the process ends.
 - e. If the requester appeals, then the OCA of the information decides the issue and the requester is informed. If the requester decides not to appeal, the process ends. If the requester does appeal, then a formal challenge is launched.
 - f. The requester should expect to receive an initial response within 60 calendar days of Treasury receiving the challenge.
- (3) Formal challenges involving Treasury or another Agency's information:
- a. Formal challenges involve the business unit disputing the classification, IRS FMSS, Treasury's SAO, all authorized holders of the information, and the OCA. The CNSI PM will engage with Chief, FMSS to coordinate with Treasury's SAO to submit the formal challenge to the appropriate OCA.
 - b. The requester submits a written request with justification of reasons for change(s) to classification to the OCA. The OCA decides the issue and responds or provides a date for response within 60 calendar days of receiving the request. If the requester decides not to appeal, the process ends.
 - c. If the requester appeals, the originating Agency considers the issue and provides a response to the requester within 60 calendar days of receiving the request or provide a date of final response. If the requester decides not to appeal, the process ends.
 - d. If the requester appeals via the CNSI PMs, the issue goes to the Inter-agency Security Classification Appeals Panel (ISCAP) to adjudicate the appeal. If the originating Agency does not appeal, the process ends and the requester is informed of the decision. ISCAP can also be brought the challenge if:

- i. The challenger received no external agency response within 120 calendar days.
 - ii. The challenger received no internal appeal response within 90 calendar days.
 - iii. The challenge was denied.
- e. If the agency that originated the CNSI appeals ISCAP's decision, the President makes the final decision on the issue.
- (4) If the information being challenged has been the subject of a challenge in the past two years, or is the subject of pending litigation, the agency is not obligated to process the challenge beyond informing the challenger of this fact and providing appeal rights.
- (5) Classification challenges are considered separately from FOIA or other requests and should not be processed simultaneously with pending FOIA or other access requests.

10.9.1.4
(11-06-2023)
**Information,
Dissemination, and
Reproduction Controls**

- (1) The Classified Document Custodian must ensure a system of information control measures, to include access to CNSI being limited to authorized holders. Control measures will be appropriate to the environment in which the access to CNSI occurs, as well as the type (e.g., electronic, paper) and volume of information. All other roles in the protection of CNSI (e.g., Security Container Custodian, local Classified Document Custodian, Top Secret Control Officer, holders, etc.) should collaborate with the Classified Document Custodian on the control measures to promote local efficiency and must comply with those established.
- (2) Control measures include administrative, physical, personnel, technical, and technological control measures.
 - a. Administrative measures may include regular verification of the accuracy internal distribution rosters (e.g., assuming the existence of a clearance or need-to-know), access, limited generation to suit mission purposes, and participation in mandatory, for Top Secret, or voluntary inventories. Administrative measures are required when technical, physical and personnel measures are insufficient to deter and detect access of unauthorized individuals.
 - b. Physical measures must include segregation of the equipment used for reproducing CNSI from unclassified equipment, ensuring the equipment used in CNSI reproduction is marked appropriately, thorough sanitization of the removable memory pieces of equipment used in classified processing, escorting all individuals that have not been granted access to Security Areas, sound baffling, etc.
 - c. Personnel measures may include ensuring authorized holders are knowledgeable of the procedures for CNSI reproduction (e.g., conspicuously identifying the copied material as CNSI, etc.), aware of the appropriate machine to reproduce on, understand the limitations originators place on documents, etc.
 - d. Technical measures include specialized paper, copy numbering and distribution restrictions.
 - e. Technological measures include equipment that is used to prevent, discourage, or detect unauthorized reproduction (e.g., pin testing, port security).

- (3) Authorized holders of CNSI must ensure dissemination control measures are exercised. These include:
 - a. Documents created prior to June 25, 2010, may not be disseminated outside the agency to which they have been made available without the consent of the originating agency.
 - b. For the procedures regarding provision of CNSI to the Legislative and Judicial branches, see TD P 15-71, Chapter 3, Section 13.
 - c. Protecting passwords, PIN codes, or combinations in the same manner as the highest level of CNSI that the container, computer, or system (including IDS) is accredited to store or protect. Passwords and combinations must never be written down. Passwords and PIN codes are never shared; combinations can be shared in a secure manner with individuals only after verification of their status as an authorized holder.
- (4) Reproduction of CNSI must be held to the minimum standards required to meet operational needs. The following additional control measures must be taken:
 - a. Reproduction is accomplished by authorized holders knowledgeable of the procedures for CNSI reproduction and best methods to ensure the protection of CNSI (e.g., observing copies being made, checking copier for original and reproductions before leaving, destroying unusable copies immediately, 'copying' several blank pages of paper if the copier stores images, etc.).
 - b. Restriction on Reproduction: Per TD P 15-71, the reproduction of Top Secret is prohibited unless approved of by the originator, including documents originating outside of Treasury, in writing with a limit on the number of copies produced. Secret and Confidential information has no such restriction unless it is restricted by the originating agency. All copies are subject to the same protections and accountability as the original.
 - c. Reproduction will only be accomplished on authorized equipment, provided by a Treasury managed contract, bearing the appropriate SF 706, 707, or 708.
 - d. Networked copiers or printers on any unclassified network or outside the Security Area cannot be used to reproduce CNSI.
 - e. Copiers equipped with remotely accessible memory, diagnostic, or maintenance capability cannot be used to reproduce CNSI.
 - f. Once the reproductions are no longer needed, they are promptly destroyed in a National Security Agency/Central Security Service (NSA/CSS) Evaluated Products List (EPL) approved shredder. Equipment approved on a previous EPL may be used for up to six years after its removal from the EPL.

Note: Thumb drives are not permitted to store CNSI.

- (5) Disposition or destruction of all at-risk CNSI is required when control measures are insufficient to deter and detect access by unauthorized personnel.

10.9.1.4.1
(11-06-2023)

Marking

- (1) Marking must be accomplished per the requirements stated in TD P 15-71, Chapter 3, Section 6 and this IRM.
- (2) If CNSI in the IRS's possession is not marked in accordance with Treasury guidelines, the authorized holder who is protecting the CNSI must request clarification from the originator. Clarification comes from the individual on the

“classified by” line or the originating agency and should be marked in an unclassified manner in writing; if issues arise in contacting the originator, the CNSI PM should be contacted for assistance. Records should be kept regarding the request for clarification about the erroneous marking.

- (3) If unclassified is comingled with CNSI, the designation of “(U)” must be used in portion marking; pages that are entirely unclassified should be included as an addendum or in an unclassified version of the document. It is encouraged that unclassified be kept separate from CNSI whenever possible.
- (4) If SBU is comingled with CNSI, the designation of “(SBU)” must be used in portion marking. Like unclassified information, pages that are entirely SBU should be included as an addendum or as an SBU version of the document.
- (5) For bulky material or classification by compilation, consult 32 CFR 2001.24. Classification by compilation may occur if items that are individually unclassified are placed into the same document and meet, through their aggregation, the standards in section 1.2 of EO 13526. In this event, any unclassified portions will be portion marked “(U)” while the banner markings will reflect the overall classification of the compilation.
- (6) Dissemination control and handling markings identify any limitations to the distribution of the information, these markings appear after the classification level on the top and bottom of each page. The markings used must be those approved by ISOO or the Office of the DNI.

10.9.1.4.2 (11-06-2023)

Requirements for Paper

- (1) Markings for derivatively classified documents: For information derivatively classified based on a single source or multiple sources, the derivative classifier carries forward the date or event for declassification that corresponds to the longest period of classification among the sources; the level of classification reflects the highest level of classification of the portions of the source document used.
 - a. Overall/Banner Classification Marking: This is determined by the highest level of classification of any one portion of the document and must be placed at the top and bottom of the page. If there is more than one page, the overall marking must be on the front cover, title page, first page, each interior page, and outside of the back cover/page. The markings at top and bottom of each page must be marked with either the highest level of classification on that page, including “Unclassified” when applicable, or with the overall classification of the document.
 - b. Portion Markings: Must be marked at the highest level of information contained at the start of the subject/title, each paragraph, graph, table, picture, etc. Note that if a source document is not portion marked, then it cannot be used in a derivatively classified document.
 - c. Classification Authority Block consisting of:
 - i. “Classified By” identifying the derivative classifier by given name and title or personal identifier and agency of origin. If a personal identifier is needed, contact the CNSI PMs.
 - ii. “Derived From” identify the source document(s), including agency and office of origin when available. When there are multiple sources, the derived from line will state “multiple sources” and a follow-on page listing the citations is attached if the sources are too numerous to fit in the block.

iii. "Declassify On" line contains the furthest date or event on the classification block(s) of the source document(s).

- d. Documents lacking any of the markings above, except for the declassification instruction, cannot be used as sources for derivative classification.
 - e. Documents that lack a declassification instruction must have a date calculated 25 years from the creation of the source document or, if that date is missing, then a date calculated 25 years from the date of the creation of the derivative document.
 - f. If the document has declassification instructions, like X1-X8, Originating Agency's Determination Required (OADR), or Manual Review (MR), consult 32 CFR 2001.22(e).
- (2) A CNSI addendum is used whenever CNSI constitutes a small portion of an otherwise unclassified document to allow for dissemination at the lowest classification level possible or in unclassified form. The unclassified portion of the document can then be distributed freely; the CNSI portion must be distributed to authorized holders in accordance with this IRM.
 - (3) Dissemination control and handling markings based on the source documents must carry over to the derivative document.
 - (4) Date of origin of the document must be indicated in a manner that is apparent at the top of the first page.
 - (5) Transmittal documents, or 'cover letters,' that transmit CNSI documents shall indicate on the face the highest classification level of any CNSI attached or enclosed. It must also have one of the following, as appropriate:
 - a. "Unclassified when classified enclosure removed" or
 - b. "Upon removal of attachments, this document is (Classification Level)."

10.9.1.4.3
(11-06-2023)
**Requirements for
Electronic Mail (email)**

- (1) Emails containing CNSI must be sent only on approved systems for the level of CNSI (e.g., TSDN for up to Secret) being sent by an authorized holder.
- (2) Ensuring all the requirements for marking paper documents from IRM 10.9.1.4.2 are met, along with the following specifics:
 - a. The subject line of the email must be portion marked, but not reflective of the classification markings of the email content or attachments and should be kept unclassified.
 - b. If attachments exist, the titles of the attachments must be portion marked and should be kept unclassified. The title of the attachment and associated portion mark does not reflect the classification of the attachment.
 - c. The overall/banner classification of the email must be marked at the top and bottom (after the derivative classification block) of each individual email.
 - d. When forwarding or replying to an email, authorized holders must ensure that, in addition to the markings required for the content of the reply or forward email itself, the markings must reflect the overall classification and declassification instructions for the entire string of emails and attachments. This will include any newly drafted material, material received from previous senders, and any attachments.
 - e. Portion marking unclassified emails that reside on an CNSI system is required.

- f. Marking in the electronic environment, to include web pages, URLs, dynamic documents, relational databases, classified wikis, instant messages or chats shall be in accordance with 32 CFR 2001.23.
- g. Classification Authority Block must occur after the signature line but before the bottom banner marking.

10.9.1.4.4
(11-06-2023)
Working Papers

- (1) Working papers are documents (e.g., notes, drafts, prototypes), materials (e.g., presentation boards or models), or other electronic media created during development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated. Working papers and materials containing CNSI must be:
 - a. Dated when created.
 - b. Marked with the highest classification of any information contained therein.
 - c. Safeguarded as required for the assigned classification.
 - d. Conspicuously marked "Working Paper" on the cover and/or first page of the document or material or comparable location for electronic media/items (e.g., on the CD itself or on the most visible part of an item) in larger typeface than existing text.
 - e. Destroyed when no longer needed.
- (2) Working papers or other working materials must be destroyed in the same manner as CNSI.
- (3) Working papers must be marked and controlled as finished products of the appropriate classification when retained more than 180 calendar days from date of origin (regardless of if they are complete), filed permanently, or released outside the IRS.
- (4) Working papers must only be shared between authorized holders internal to the IRS or between agencies of the same working group, either physically or electronically, without controlling them as permanent documents only when the working materials are shared information (e.g., collaborative documents or coordinating drafts) in the development process.

10.9.1.5
(04-13-2021)
Document Cover Sheets

- (1) SF 703, 704, and 705 are used to alert authorized holders that a document, file, or folder to which it is affixed contains CNSI and must be protected. Document cover sheets shield CNSI while being used and provide protection from unauthorized visual contact. Cover sheets are required whenever a document is taken out of the security container, but they are suggested to remain on the document even in the container. The cover sheets are color-coded to provide a visual cue of what is being protected:
 - a. SF 703: Orange for Top Secret information
 - b. SF 704: Red for Secret information
 - c. SF 705: Blue for Confidential information
- (2) Individuals preparing, processing, packaging, or hand carrying CNSI are responsible for affixing the appropriate document cover sheet. If CNSI is delivered or received without the required cover sheet, the recipient is responsible for attaching the proper cover sheet.
- (3) Additional maintenance guidance for cover sheets:

- a. Cover sheets should be removed from CNSI prior to destruction.
- b. Cover sheets are meant to be continually recycled until worn out.
- c. Cover sheets will not be photocopied in black/white.
- d. To accommodate emergency use, cover sheets may be reproduced on a color copier.

10.9.1.5.1
(04-13-2021)
**Labels on Equipment
and Electronic Media**

- (1) SF 706, 707, and 708 are labels required to identify equipment approved for processing CNSI. Labels are color-coded in the same manner as document cover sheets:
 - a. SF 706: Orange for Top Secret
 - b. SF 707: Red for Secret
 - c. SF 708: Blue for Confidential
- (2) Additional SF labels exist for equipment and are also required:
 - a. Purple for “classified but level determination pending,” protection must be at the Top Secret level (SF 709).
 - b. Green for “unclassified” (SF 710). In environments in which CNSI and unclassified is stored, the “unclassified” label must be used to positively identify equipment/electronic media authorized for unclassified use only.
- (3) Once applied, the label must not be removed.
 - a. A label to identify a higher classification level may be applied on top of a lower classification level, if the classification content changes.
 - b. A lower classification label must never be applied to equipment already containing or processing a higher level of CNSI.
- (4) Authorized holders working with or processing CNSI are responsible for properly labeling and controlling equipment in their custody.
- (5) All removable electronic and magnetic media used to process CNSI will be physically labeled with the highest level of CNSI contained therein.
 - a. Removable electronic media must be physically detached from the processing equipment at the close of business each business day and secured in a security container.
 - b. An exception to the requirement to physically remove and store such electronic media items is authorized when the equipment and processing occurs in a TSDN LA or SCIF that has been equipped with minimum security standards prescribed in this IRM or Intelligence Community Directives (ICD), then approved by Treasury.
 - c. Removable electronic media will always be safeguarded when not in use or under the supervision of an authorized holder.
- (6) Failure to apply the appropriate labels is a security infraction. If the failure results in improper storage, loss, unauthorized access, or compromise of CNSI, it is a security violation.

10.9.1.6
(11-06-2023)
**Downgrading and
Declassification**

- (1) Downgrading and declassification are the jurisdiction of the OCA and Agency that originated the information. Requesting information to be downgraded or declassified prior to the date on the declassification block is a formal process.

- (2) Per Treasury Order (TO) 105-19, CNSI originates outside the jurisdiction of the IRS, as IRS has never had an OCA. Given this, the Commissioner cannot make any declassification decisions.
- (3) IRS must consult the OCA of the originating agency on the downgrading or declassification questions or clarifications if that individual is still serving in the same position and remains a delegated OCA. If the originator has left the position, then the originator's current successor in function will be contacted in lieu of if that person has an OCA. If the delegation goes further, the Agency's security organization must be consulted.
- (4) If CNSI that originates from another agency has a downgrading or declassification date that has passed, it is incumbent on the IRS holder of the CNSI to ensure that the original classification markings on the document are stricken and replaced with the downgraded or unclassified markings, as appropriate. A downgrade or declassification block consisting of name/title and downgrade/ declassification date must be noted on the page with the classification or derivative classification block.

10.9.1.6.1
(04-13-2021)

Declassification Reviews

- (1) Automatic Declassification Review: All CNSI contained in records that are more than 25 years old and that have been determined to have permanent historical value under Title 44 U.S.C. is automatically declassified, unless it meets the requirements of EO 13526 Section 3.3 paragraphs (b)-(d) and (g)-(j). The 25-year automatic declassification process is a sliding scale as records age and applies annually to CNSI on December 31.
 - a. Information exempted from automatic declassification remains subject to the mandatory and systematic declassification reviews.
 - b. CNSI cannot be automatically declassified because of an unauthorized disclosure of identical or similar information.
 - c. Prior to public release, all declassified records must be appropriately marked to reflect the declassified status of the information.
- (2) Systematic Declassification Review: This function is carried out by the agency with the OCA responsible for the classification of a given piece of CNSI. Detailed information can be found in EO 13526, Section 3.4.
- (3) Mandatory Declassification Review: This function is carried out by the OCA responsible for the classification of a given piece of CNSI. Detailed information can be found in EO 13526, Section 3.5.

10.9.1.7
(11-06-2023)

**Secure Voice/Data
Communication**

- (1) Authorized holders must use Secure Telephone Equipment (STE) for voice or other secure communications for conducting CNSI discussions. When these communications are owned by IRS, they must be under provisions established by Treasury systems security officials in TD P 85-01 Volume 1, Part 2.
- (2) IRS Criminal Investigation (CI) has the responsibility to implement and certify areas for the sole purposes of classified conversations via STE. Documentation of certification must be kept and available for provision.
- (3) Fax machines that have historically hooked up using the STEs are no longer linked, so faxes within IRS facilities can no longer be used to process classified information. The SF 707 stickers must be replaced with SF 710s and the equipment excessed if no longer needed. There are no latency concerns with faxes.

10.9.1.8
(11-06-2023)
Safeguarding CNSI

- (1) CNSI, regardless of its form, must be afforded the level of protection against loss or unauthorized disclosure commensurate with its level of classification. It is the responsibility of all authorized holders to ensure its protection and proper handling.

10.9.1.8.1
(11-06-2023)
Access to CNSI

- (1) In order to access CNSI, the individual must be an “authorized holder” that meets requirements listed in (1) a) - d) as follows:
 - a. A favorable determination of eligibility for access. An individual is eligible for access to CNSI only after a positive showing of trustworthiness as determined by the proper IRS authority based upon an investigation and favorable adjudication in accordance with national personnel security standards and accompanying Treasury guidance.
 - b. A signed SF 312.
 - c. A need-to-know the CNSI, defined as a determination in accordance with directives issued pursuant to EO 13526 that a prospective recipient requires access to specific CNSI to perform or assist in a lawful and authorized USG function.
 - d. Participate in mandatory Integrated Talent Management Item, “Annual Security and Derivative Classification Brief,” instituted by the CNSI PM on the proper safeguarding of CNSI and on the criminal, civil, and administrative sanctions that may be imposed if the CNSI is not protected from unauthorized access.
- (2) No employee must be deemed to be eligible for access to CNSI merely by reason of:
 - a. Federal service or contracting, licensee, or certificate holder
 - b. Grantee status
 - c. As a matter of right or privilege, or because of any title, rank, position, or affiliation
 - d. Solely having a clearance
- (3) IRM 10.23.3, Personnel Security, Personnel Security/Suitability for Employment and Personnel Security Operations, must be followed in matters of personnel security, which include but not limited to: requesting security clearances, transfer of clearances to attend meetings, etc.
- (4) Prior to allowing access to CNSI, verify security clearances at least seven business days in advance:
 - a. IRS or contractor employees via *hco.ps.national.security.programs@irs.gov*.
 - b. Visitors reference requirements in IRM 10.23.1.18, National Security Positions and Access to Classified Information.

10.9.1.8.2
(11-06-2023)
General Safeguarding Provisions

- (1) Each authorized person is responsible for safeguarding CNSI from possible loss, compromise, or unauthorized disclosure. The knowledge and physical custody includes ensuring:
 - a. That CNSI is protected over the course of its lifecycle, regardless of what action is being taken with it.
 - b. That it is not communicated over unclassified voice, email, or any other system (e.g., TSDN for up to Secret or Treasury Foreign Intelligence Network (TFIN) for up to TS/SCI), nor in public conveyances or places

(to include hallways or unsecured conference rooms, even in a government facility), or in any other manner that potentially permits interception by unauthorized personnel.

- c. Failure to protect CNSI is recognized as a security incident. Any potential or actual security incidents must be reported to the local Classified Document Custodian immediately after ensuring that CNSI is protected.
- (2) Authorized holders transmitting CNSI are responsible for ensuring that intended recipients are authorized persons with the capability to store CNSI at the level being sent, regardless of the method of transmission (e.g., electronic, hand-carry).
- (3) STEs located in an area owned by CI are certified by CI to prevent access to both the equipment and unauthorized disclosure of the conversation or a certified Security Area will be used for conducting classified discussions.
- (4) CNSI approved for destruction must be destroyed in accordance with this IRM.
- (5) CNSI may not be removed from IRS premises without a courier letter or card and authorization, as appropriate (e.g., removal for purposes of disclosure to a foreign entity, etc.).
- (6) An IRS authorized holder leaving IRS may not remove CNSI from IRS control or direct that information be declassified to remove it from IRS control.
- (7) To maintain the ability to access CNSI there must be a requirement for the employee to maintain the clearance. The justification of continued need must be documented in the Position Description.
- (8) Access to CNSI must be terminated when an employee no longer has a need for CNSI to accomplish their duties; the employee's management must ensure the transition to a Public Trust Position Description (PD). Access must also be terminated as required in the IRM 10.23 series, Personnel Security.
- (9) In the event of immediate threats (i.e., fire, earthquake, bomb threat, etc.) or anticipated threats (i.e., hurricane, flood), if time permits, immediately secure all CNSI on site in an approved security container. If adequate storage is not available in the Security Area, the Security Container Custodian (if a security container) or Responsible Party (if Security Area) must have pre-arranged a security container in another space for the items.

10.9.1.8.3
(11-06-2023)
**Standards for Securing
CNSI**

- (1) Security containers used for storage of CNSI material must conform to standards specified by the General Services Administration (GSA).
 - a. For documents, the requirement is a Class 5 or 6 container with a lock meeting FF-L-2740 standard.
 - b. GSA approved security container meeting Federal Standard (FED STD) AA-C-2786 to store Information Processing Systems (IPS).
 - c. GSA-approved field security containers are intended for storage of CNSI in situations where normal storage is not possible such as on ships, in vehicles, or in military field operations; they may not be used in an IRS facility.

- (2) Whenever a new security container is procured, it must be compliant with the requirements and purchased through GSA Global Supply, and the Classified Document Custodian responsible must input the container into the Security Container Tracker.
 - a. Contact the CNSI PMs via **FMSS Classified Information Security Team* for information and instructions on the purchase of a new container.
- (3) CNSI must be stored under conditions designed to deter and detect unauthorized access.
- (4) Storage at overseas locations must be at USG facilities, unless it is otherwise stipulated by the U.S. government security authority for that area (e.g., State Department Chief of Mission or Regional Security Officer).
- (5) The SF 702 must:
 - a. Have the information section (e.g., room number, building, container number, month/year) filled out appropriately.
 - b. Be completed each time the security container or Security Area is accessed and/or checked every business day, regardless of whether it was opened.
 - c. The SF 702 must be kept for 90 calendar days.
- (6) Firearms, monetary assets or evidentiary matter cannot be commingled with CNSI in the same drawer; unclassified or SBU information may be commingled only if the unclassified or SBU is part of the classified document.

Note: The tops and sides of the security containers must be kept barren except for the required SF, the GSA certification label, and the optional “open/close” sign.

10.9.1.8.3.1
(11-06-2023)
Storing Top Secret

- (1) Top Secret information will be stored in one of the following ways:
 - a. In a GSA-approved Class 5 or 6 security container with one of the following supplemental controls:
 - i. Secret-level cleared personnel must inspect the security container once every 2 hours.
 - ii. An Intrusion Detection System (IDS) with responders arriving within 15 minutes of alarm annunciation.
 - iii. Security-in-depth coverage in the area in which the GSA approved security container is located, provided the container is equipped with an FF-L-2740 lock.
 - b. In an open storage area built to 32 CFR 2001.53 standards with the supplemental controls as follows:
 - i. For areas covered by security-in-depth, an IDS with personnel responding within 15 minutes of the alarm annunciation.
 - ii. For areas not covered by security-in-depth, and IDS with personnel responding to the alarm within 5 minutes of the alarm annunciation.
 - c. In a vault built to Federal Standard 832 with one of the above supplemental controls.

- (2) All IDS must be in accordance with standards approved by the ISOO. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the agency head.

10.9.1.8.3.2
(11-06-2023)

Storing Secret and Confidential Information

- (1) Secret information must be stored according to one of the following methods:
 - a. In the same manner prescribed for Top Secret information.
 - b. In a GSA-approved Class 5 or 6 security container or a vault built to FED STD 832 without supplemental controls.
 - c. In an open storage (e.g., approved Open Storage Security Area) area with one of the following supplemental controls:
 - i. Secret-level cleared personnel must inspect the security container or open storage area once every 4 hours.
 - ii. An IDS with responders arriving within 30 minutes of alarm annunciation.
- (2) Confidential must be stored in the same manner as Top Secret or Secret, except that supplemental controls are not required.

10.9.1.8.4
(11-06-2023)

Combination Locks and Key Operated Locks, and Security Container Movements

- (1) Before being given access to a security container or Security Area, the individual's status as an authorized holder must be established.
- (2) Dial-type electromechanical locks must meet the FF-L-2740 standard and combinations are considered classified at the highest level of CNSI that is protected by the lock. This applies to the locks installed on a container or door of a Security Area.
- (3) Key-operated high security padlocks are not authorized to secure CNSI.
- (4) Pedestrian doors to Security Areas must have an FF-L-2740 lock and meet all life-safety requirements. Additionally, pedestrian door lock extensions must meet FF-L-2890, Lock Extensions (Pedestrian Door Lock Assembly Preassembled, Panic and Auxiliary Deadbolt) standards.
- (5) Keys for pedestrian door lock extension that are required to meet local life-safety requirements on Security Area pedestrian door protecting CNSI must be afforded the same level of protection as the information being protected. Additional administrative procedures for key control and accountability will include the following:
 - a. Great Grand Master key systems are not authorized for Security Area.
 - b. Keys may not be duplicated.
 - c. The Security Section Chief must issue keys to the Responsible Party for the Security Area as Key Custodian, this will be documented via Form 1930-D, Key Custody Receipt (KCR). The Key Custodian may only issue keys to other Security Area Responsible Parties or Authorized Personnel when life-safety or emergent reasons arise. Keys may not be taken out of the building.
 - d. Keys will have a unique identifier either attached to the key or engraved on the key head. Unique serial numbers for keys may be used as the identifier. The key must also be engraved with the words "U.S. Government - DO NOT DUPLICATE."
 - e. Lost or stolen keys:

- i. Contact the Classified Document Custodian, Security Area Responsible Party, and CNSI PM at **FMSS Classified Information Security Team* of a possible security incident in an unclassified manner promptly after the discovery of the potential loss.
 - ii. Contact all Authorized Personnel with access to the key to ascertain if it is in their possession; follow up with the Classified Document Custodian, Security Area Responsible Party, and CNSI PM.
 - iii. Perform immediate inventory of all CNSI documents.
 - iv. GSA approved technicians must be contacted promptly to replace core.
 - v. If applicable, after the core is replaced all the remaining original keys must be destroyed so they cannot be confused with replacements.
 - f. Key Inventory Log. A locally developed log to record the inventory of Security Area keys. The Key Custodian will conduct a physical inventory at least quarterly. Key Inventory Logs must be retained for six months for Interagency Security Committee (ISC) Facility Security Level (FSL) I-III; ISC FSL V facilities for three years. The Key Inventory Log will document the following:
 - i. Date and Time of inventory.
 - ii. Full name and signature of Key Custodian conducting the inventory.
 - g. Key Control Register. A locally developed register to record the issuance of Security Area keys to Authorized Personnel. The Key Control Register will be inspected at least quarterly to ensure compliance with this IRM. Key Control Registers must be retained for six months for Interagency Security Council (ISC) FSL I-III; ISC FSL V facilities for three years. The Key Control Register will document the following:
 - i. Unique key identifier.
 - ii. Date and time key issued.
 - iii. Issued by Full name and signature of Key Custodian issuing the key out.
 - iv. Issued to Full name and signature of other Responsible Party or Authorized Personnel signing the key out.
 - v. Date and time key was signed out and in.
 - vi. Received by Full name and signature of Key Custodian receiving the key.
- (6) Combinations will be changed only by personnel with a security clearance, verified prior to the change occurring by emailing *hco.ps.national.security.programs@irs.gov*, commensurate with the level of CNSI in the container and who have knowledge as to how to appropriately change the combination. The combinations will not be sequential numbers, or the standard combination, 50-25-50; additionally, combinations must be either high-low-high or low-high-low (e.g., 75-38-61 or 23-55-31).
- a. Contractors must not be used to change combinations, unless they are GSA certified technicians, or it is in the scope of work of the contract and the contract meets NISP requirements. Contact the CNSI PM with the contract documents. If no contract was established, and the service is bought via credit card, it is the Business Units responsibility to ensure the technician is GSA certified and has the appropriate clearance prior to the combination being changed.

- b. Combinations must be changed when:
 - i. The container is first placed into service with the end-user.
 - ii. An authorized holder knowing the combination no longer requires access to it unless existing controls prevent unauthorized access to the security equipment (e.g., container is in a SCIF or other Security Area with prescribed access control restrictions preventing the authorized holder access).
 - iii. A combination has been subjected to possible compromise, actual compromise, or unauthorized disclosure.
 - iv. The equipment is taken out-of-service.
 - v. At least every 3 years, unless conditions dictate sooner, such as the need to store a particular type of CNSI or material. The minimum time frame is to ensure combinations have an official termination point and to avoid an infrequently opened security container's combination being lost.
- (7) An individual that has authorization to access the security container must be present to specify the desired combination and verify the change.
- (8) Combinations to security containers storing CNSI must be recorded on a new SF 700, sealed, then stored in a different GSA approved security container with the same or higher level of classification.
 - a. Part 1, the tear-away, carbon-copy portion that lists the name and contact information of individuals with access to the security container must be placed on the inside of the drawer with the lock on it in a conspicuous place or on the secure side of the Security Area entry door.
 - b. Part 2A, the tear-away, perforated portion for the combination, must be placed in the envelope portion, Part 2, of the SF 700. This is the portion of the form that must be stored in another security container.
- (9) Excessing, Recycling, or Scrapping: Containers should be processed if no longer needed by the Business Unit for any reason (e.g., not currently used/no planned future use, inoperable, etc.). Prior to an Employee Resource Center (ERC) ticket being submitted for the security container, the following steps must be followed in order:
 - a. The lock for the container may need to be removed for demilitarization if the container is inoperable or potentially going to be excessed, so the CNSI PMs must be contacted with the make/model of the lock prior to proceeding with the steps below.
 - b. The Classified Document Custodian or Security Custodian Customer will ensure that all the CNSI in the container has been destroyed or moved to another GSA approved container.
 - c. The Classified Document Custodian or Security Container Custodian will open all drawers to the container one at a time and, using a flashlight, inspect:
 - i. That it is empty of all documentation,
 - ii. That a light is shined in the spaces surrounding the pulled-out drawer to ensure that there is no material in the crevices,
 - iii. If material appears to be present, that the drawer is removed, and the material is retrieved.
 - d. The Classified Document Custodian or Security Container Custodian will ensure the combination for the container is changed to the standard

- default of 50-25-50. Contact **FMSS Classified Information Security Team* if there are issues with setting the combination.
- e. If the container is inoperable, remove the GSA label by using a razor blade or flathead screwdriver.
 - f. The ERC ticket must state the following in the Purpose Box: "Please remove the security container as it **(no longer meets the requirements to secure CNSI material/no longer needed by the office)**. The security container is **(operable/not operable)**. The security container is open. **(The lock is not operable and has been removed and returned to FMSS for demilitarization with the Department of Defense Lock Program or re-use within IRS. The combination is affixed to the lock and the lock has been set to default.)** The container has been verified as clear of CNSI by **(Insert name of POC, contact phone #, email)**. Thank you."
 - g. Once the container has been picked up for dispositioning, the Classified Document Custodian must update the Security Container Tracker.
 - h. The IRS Property Officer will determine what to do with the security container based on its condition and the needs of the USG.
- (10) If repairs to the Class 5 or 6 security container or FF-L-2740 lock are required, the technician hired to address them must be GSA certified. The Business Unit must remove CNSI from the defunct container and place it in another Class 5 or 6 container. If the technician is not GSA certified, then the security container must be decommissioned (i.e., not used to store CNSI) until a GSA certified technician can recertify it. The two organizations mentioned in a) and b) maintain lists of certified technicians worldwide, as well as provide GSA certified training:
- a. Lockmasters Security Institute
1014 South Main Street
Nicholasville, KY 40356
Phone: 866-574-8724 (USA Toll Free)
Phone: 859-887-9633
 - b. MBA USA, Inc.
200 Orchard Drive
Nicholasville, KY 40356
Phone: 888-622-5495 (USA Toll Free)
Phone: 859-887-0496
- (11) Movements of a security container between rooms or facilities, to include decommissioning to a warehouse or excessing, must be tracked by the Classified Document Custodian with responsibility for the container via the Security Container Tracker. The tracker should note which other security container is used for holding the SF 700.

10.9.1.8.5
(11-06-2023)
Processing CNSI

- (1) CNSI may only be processed on approved equipment (e.g., TSDN, TFIN, or accredited systems housed in other agencies).
- (2) Information systems approved for CNSI processing cannot be connected to any system not approved for classified operation. Systems approved for CNSI processing will not share peripherals with unclassified processing equipment except through NSA/CSS approved switching devices. Approval for the use of switching devices must be included in the security authorization documentation.

- a. Prior to using the switch, the individual must be taught appropriate protocols by the IRS or DO IT department. The switch must be labeled on both the unclassified and CNSI side with the appropriate stickers: SF 710 for unclassified and SF 706, 707, or 708 for CNSI at the respective level.
- (3) Refer to TD P 85-01 Volume II and TD 15-03 and/or contact the Treasury Office of the Chief Information Officer (OCIO) for information on uniform procedures to ensure automated information systems, including networks and telecommunications systems, that:
 - a. Collect, create, communicate, compute, disseminate, process, or store CNSI.
 - b. Prevent unauthorized access, ensure information integrity.
 - c. Use common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information to authorized holders who meet the standards set by EO 13526 for access to CNSI.

10.9.1.8.6
(11-06-2023)
Security Areas

- (1) Rooms being used to process CNSI on electronic systems, or discuss CNSI, must be built to specific standards and follow detailed operational requirements. There are four types of rooms that IRS Authorized Personnel may use to process CNSI; three Collateral Security Areas (Open Storage of Secret, TSDN LAs, Top Secret Space) and SCIFs.
 - a. Open Storage of CNSI up to the Secret level is used only in circumstances where there is:
 - i. Up to Secret level equipment that is required to be stored,
 - ii. Insufficient space in GSA approved security containers,
 - iii. Not a need to process via secure system.
 - b. TSDN LAs can process up to Secret CNSI and can be compared to Treasury's Secure Work Areas. Treasury does not permit TSDN LAs to openly store CNSI documentation.
 - c. Top Secret Spaces can store Top Secret paper and host Top Secret conversations, they cannot host TFIN.
 - d. SCIFs are utilized when storing and processing TS/SCI information, such as TFIN.

Note: Prior to any of these areas being constructed the AD, Security, must approve the upgrade using a form provided to the requesting Business Unit by the CNSI PMs.
- (2) Security Area Daily Maintenance: This subsection applies to Open Storage of up to Secret, TSDN LA and Top Secret Spaces. SCIFs have additional protocols that are detailed during the certification process. During the workday, care must be taken to ensure that CNSI always remains protected.

Accessing:

- Note:** Responsible Party(ies) and Authorized Personnel should be IRS Federal employees; if IRS contractors must be used, they must be on a NISP compliant contract.

- a. Only a Responsible Party or Authorized Personnel, who will be termed “Opener”, can know the combination required to open the Security Area; as such, discretion must be used as to the number of individuals given the responsibility.
- b. All persons must have a current and ongoing need-to-work in the Security Area at minimum of one time per month prior to seeking access. IRM 10.2.18.10.4 must be followed to document access requests. This request must contain the individual’s given name, verification that individual has appropriate clearance level, verification the individual has a need-to-know and requires consistent access to the Security area, and whether the individual is a Responsible Party or Authorized Personnel.
 - i. Personnel Security must be given a minimum of seven business days to verify the individual’s clearance.
 - ii. The Responsible Party must ensure that all Authorized Personnel are trained on the appropriate procedures for opening, closing, workday maintenance, alarm response, etc. prior to being given their own IDS code and the combination to the FF-L-2740 compliant lock.
- c. At the beginning of business hours, the opener will enter the combination into the FF-L-2740 compliant lock, read their SmartID on the access control device (ACD), and enter their PIN.
 - i. All electronic devices (smartwatch, cellular phone, tablet, computer, Bluetooth, or wireless headphones, etc.) must all be placed in the cell phone locker prior to entry. The introduction of prohibited items into the Security Area is a security incident.
- d. Should an Authorized Personnel need to have a wireless/Bluetooth device for health reasons, such as a pacemaker, notification to the Responsible Party and the CNSI PM must be made.
- e. The SF 702, kept on the outside of the entry door, must be filled out.
- f. The magnetic sign on the door must be flipped to ‘open,’ if the signage is available.
- g. Once inside the Security Area, the opener must disarm the IDS and push the life safety switch on the back of the FF-L-2740 lock to prevent lock in.

Workday Maintenance:

- a. Visitors must be sponsored into the Security Area by that area’s Responsible Party or Authorized Personnel, henceforth termed “sponsoring individual”.
- b. The sponsoring individual must coordinate with the visitor and IRS Personnel Security to ensure that the visitor’s clearance and need-to-know are verified prior to the visit taking place. *Personnel Security* must be given a minimum of seven business days to verify the individual’s clearance.
 - i. Visits must be planned to allow for vetting to occur prior to the individual gaining access.
 - ii. Cleaning and maintenance personnel must have been deemed suitable in accordance with 5 CFR 731 and given an ID via normal facility processes prior to entry into the Security Area. Cleaning and maintenance personnel must always be escorted.

- c. The Security Area must be sanitized, and the occupants be made aware prior to the visit, to preclude unauthorized access to CNSI.
- d. Visitors must sign in and out of the Security Area on IRS Form 5421. A one-year history of the Form 5421 must be maintained on-site.
- e. Visitors must adhere to IRS and Treasury orders to ensure the safeguarding of classified information.
- f. One Responsible Party or Authorized Personnel must always remain in the Security Area during the business day, otherwise the space will need to be closed, as discussed in the "Closing" subsection below.
 - i. The SF 701 does not need to be filled out until the last Authorized Personnel leaves for the day. The Security Area does, however, need to be checked by the Responsible Party or Authorized Personnel to ensure no CNSI is left unsecured.

Closing:

- a. Any Responsible Party or Authorized Personnel can close the Security Area and is known in this subsection as the closer. The following must be initiated any time the space is left unoccupied, whether it be for a workday meeting or at the close of the business day.
 - i. The closer must walk the Security Area to ensure that they are the last person in the space, all CNSI has been secured, the security containers are closed appropriately, and all TSDNs, as applicable, have been logged off.
 - ii. The SF 702 must be filled out in the checked by column verifying that it was appropriately closed, regardless of whether the security container was opened on a given day.
 - iii. The SF 701 must be filled out verifying that the Security Area was checked.
 - iv. The closer must then arm the IDS system. Once the system begins the countdown, the closer knows it is time to leave the Security Area.
 - v. Pull the life safety switch on the back of the FF-L-2740.
 - vi. Upon leaving, the closer must verify the door is shut and spin the combination lock one full rotation in each direction, at minimum, and verify that the bolt is engaged by attempting to open the door.
 - vii. Complete the SF 702 with the time exited and the magnetic sign must show 'closed,' if signage is available.
 - viii. If no Responsible Party or Authorized Personnel enter the Security Area on a given duty day, it must be checked to verify that the FF-L-2740 lock is engaged on the door and noted on the SF 702 for the door under the checked by column.

After Business-Hours Access:

- a. If access to the Security Area is required after business hours, on weekends, or holidays, normal business day open and close procedures will be followed.

Alarm or Disturbances and Response:

- a. The names of the Responsible Party(ies) or Authorized Personnel designated to perform response duties, along with their business and personal

contact information, must be provided to the monitoring entity to ensure response to alarm or disturbances. These individuals are known as responders. Coordination in advance of holidays or other periods where multiple responders may be unavailable must occur.

i. Only a Responsible Party or a designated Authorized Personnel can respond to alarms or disturbances.

b. During Business Hours:

i. Once notified of the alarm or disturbance, the responder has up to 15 minutes for Top Secret Spaces and 30 minutes for Open Storage of Secret or TSDN LAs to arrive.

ii. After arriving at the Security Area, the responder, if not in fear for their safety, must enter and perform a thorough check to ensure that there has been no potential compromise or loss of CNSI in any of its forms.

iii. If the responder has safety concerns, the monitoring entity must be notified immediately.

iv. The responder must disable the IDS upon entry into the Security Area.

v. Once the Security Area is clear, the monitoring entity must be notified so that they can clear the alarm.

c. After Hours:

i. The monitoring entity must take appropriate action on all alarms and notify the responders for the Security Area; responders have up to 15 minutes for Top Secret Spaces and 30 minutes for Open Storage of Secret or TSDN LAs to arrive.

ii. After arriving, the responder, if not in fear of their safety, must enter and perform a thorough check to ensure that there has been no potential compromise or loss of the CNSI in any of its forms.

iii. If the responder has safety concerns, the monitoring entity must be notified immediately to facilitate an armed response.

iv. The responder must disable the IDS upon entry into the Security Area.

v. Once the Security Area is clear, the monitoring entity must be notified so that they can clear the alarm.

d. Facilities Emergencies:

i. The monitoring entity must be notified in the event of an emergency (i.e., water leak, heating, and cooling issue, etc.) that is affecting the Security Area and requires entry to address, but the space is unoccupied.

ii. The monitoring entity will notify the responders to open the Security Area.

iii. Responders must respond within 15 minutes for Top Secret Spaces and 30 minutes for Open Storage of Secret or TSDN LAs to arrive.

(3) Open Storage of CNSI up to the Secret level:

a. Background: 32 CFR 2001.43 and .53 detail the requirements needing to be met prior to a Security Area being allowed to openly store CNSI equipment up to the Secret level. This type is not certified for classified conversations.

b. Requesting an Open Storage Area:

- i. Business Units requiring Open Storage must consider the amount of equipment being stored, length of time it will be stored, whether it can be disposed of, if there will be a recurring need to store CNSI equipment and whether there are multiple GSA approved containers in which to store the equipment.
 - ii. If a Security Area is still required based on the considerations above, the AD, Security must approve prior to upgrade or construction starting.
- c. Certification:
 - i. The initial survey of the room will be conducted by the CNSI PMs against 32 CFR 2001 requirements.
 - ii. The CNSI PMs will coordinate with the local SSC and requesting Business Unit to ensure gaps between the status of the room and CFR requirements are addressed. Additionally:
 - 1. No wireless devices of any kind are permitted into the Security Area unless authorized by Treasury.
 - 2. Each Responsible Party and Authorized Personnel must have their own, unique code to the IDS.
 - iii. After-hours response must be coordinated with the SSC, monitoring entity and Business Unit.
 - iv. Once the Security Area has been built, the CNSI PMs will perform a certification inspection. If the space meets requirements, the AD, Security will issue a certification letter.
 - v. The Responsible Party of the Security Area must ensure that security protocols discussed above in subsection IRM 10.9.1.8.5(1) are established and maintained for the space, to include immediate provision of a response roster to the monitoring entity.
 - 1. A copy of the Security Area's certification letter, Form 5421, and the SF 701 must be placed by the primary entry door on the secure side of the door.
 - 2. The SF 702 must be kept on the non-secure side of the Open Storage primary entry door and on other security containers, as applicable.
 - 3. Security Area Entry Door Warning Sign and current access roster on the non-secure side of all entry doors, found on the CNSI Website.
 - 4. Training of Authorized Personnel on appropriate access, closure, and alarm response procedures.
- (4) TSDN LAs: Background: 32 CFR 2001 and the TD P 15-71, and the TD P 85-01 out the requirements for the protection of CNSI material and systems. The below is in addition to the LA guidance found in IRM 10.2.14, IRM 10.2.18, and the physical security requirements for TSDN LAs in the Physical Security Design Manual.

Requesting a TSDN and Milestones:

- a. Business Units requiring a TSDN LA must review the Certification Process, subsection found directly below, prior to selecting a room for conversion into a Security Area. Additional considerations:
 - i. Traffic flow by the room, whether the facility is leased, or what other entities (governmental or not) would be neighbors.

- ii. Consultations with local SSC and FMSS staff on most advisable room to convert given physical security requirements.
- b. The following information must be sent to the CNSI PM:
 - i. Justification stating the need.
 - ii. The location (building address and office number).
 - iii. Assurance that the Business Unit can provide adequate 24/7 coverage to respond to alarms, disturbances, or events in the Security Area. Those chosen for coverage must:
 - 1. Possess a valid Secret clearance.
 - 2. Be an IRS authorized holder.
 - 3. Understand requirements of secure operation.
- c. After the information has been provided, the CNSI PM will work with the AD, Security, to ensure that all requirements are met. AD, Security must provide a response within 30 calendar days of the receipt of all information for the process to begin.
- d. Business Units must discuss with and have the agreement of Treasury OCIO regarding the installation of TSDN in the prospective Security Area prior to coordinating with CNSI PM and SSC to start the process of construction/upgrade.
- e. Treasury OCIO procures all portions of the TSDN system once the Business Unit's requirements are finalized.

Certification Process:

- a. Approval to build the TSDN LA is submitted to the AD, Security by the requesting Business Unit. See "Requesting a TSDN LA and Milestones" subsection above.
- b. The initial survey of the room will be conducted by the CNSI PMs ensuring that the OSP physical security requirements for TSDN LAs are met.
- c. The CNSI PMs will coordinate with the local SSC and requesting Business Unit to ensure gaps between the current status of the room and OSP requirements are addressed:
 - i. The Security Area must be equipped with NSA/CSS EPL shredder, GSA approved class 5 or 6 security container with FF-L-2740 lock, door signage that appropriately warns against unauthorized entry.
 - ii. All trash and recycling bins removed.
 - iii. A Technical Surveillance Countermeasures Survey may be required if unclassified equipment is to remain in place once the room becomes certified or if new unclassified equipment is added after certification. This survey typically occurs after certification but prior to installation of TSDN.
 - iv. No wireless devices of any kind are permitted inside.
 - v. Each Responsible Party and Authorized Personnel must have their own, unique code to the IDS.
 - vi. If windows are present, then the screens for the TSDN system must face away from the windows or be equipped with a privacy screen.
 - vii. Treasury OCIO will advise on proximity between TSDN and unclassified systems, lines, and equipment as required per national guidelines. The proximity must always be maintained.

- viii. TSDN systems must stay in the Security Area that was certified to hold them. The systems cannot be moved by IRS or others from where they are initially placed by Treasury OCIO without prior permission from DO OCIO.
 - d. After-hours response must be coordinated with the SSC, monitoring entity and Business Unit.
 - e. Once built, the CNSI PMs will perform a certification inspection.
 - f. If it meets requirements, the CNSI PMs will forward the inspection documentation to OSP for their assessment and, if the risk is acceptable, provision of the certification letter to the IRS.
 - g. After certification, the Business Unit must coordinate with Treasury OCIO for the installation of TSDN.
 - h. If the Security Area is certified for classified discussions by OSP, STE can be procured by the Business Unit from the IRS COMSEC POC.
 - i. The Responsible Party of the Security Area must ensure that security protocols discussed above in IRM 10.9.1.8.6(2) are established and maintained for the space, to include immediate provision of a response roster to the monitoring entity.
 - i. A copy of the certification letter, IRS Form 5421, and the SF 701 must be placed by the primary entry door on the secure side of the TSDN LA.
 - ii. The SF 702 must be kept on the non-secure side of the primary entry door to the TSDN LA and on other security containers as required.
 - iii. Security Area Entry Door Warning Sign and current access roster on the non-secure side of all entry doors, found on the CNSI Website.
 - iv. The SF 707 and 710 stickers must be placed on equipment as applicable.
- (5) Top Secret Space: Background: 32 CFR 2001 outlines the requirements for the protection of CNSI material and systems. The below is in addition to the guidance found in 32 CFR 2001, IRM 10.2.14 and IRM 10.2.18. These spaces cannot host SCI in any form, but can host Top Secret conversations.

Requesting a Top Secret Space and Milestones:

- a. Business Units requiring a Top Secret Space must review the Certification Process, subsection found directly below, prior to selecting a room for conversion into a Security Area. Additional considerations:
 - i. Traffic flow by the room, whether the facility is leased, or what other entities (governmental or not) would be neighbors.
 - ii. Consultations with local SSC and FMSS staff on most advisable room to convert given physical security requirements.
- b. The following information must be sent to the CNSI PM:
 - i. Justification stating the need for the Security Area and the storage of Top Secret.
 - ii. The location (building address and office number).
 - iii. The given name of a Top Secret Control Officer who will be responsible during upgrade/construction and upon certification, in line with subsection IRM 10.9.1.8.6(7) of this IRM.

- c. Assurance that the Business Unit can provide adequate 24/7 coverage to respond to alarms, disturbances, or events in the Security Area. Those chosen for coverage must:
 - i. Possess a valid Top Secret clearance.
 - ii. Be an IRS authorized holder.
 - iii. Understand security requirements of secure operations.
- d. After the information has been provided, the CNSI PM will work with the AD, Security to ensure that all requirements are met. AD, Security must provide a response within 30 calendar days of the receipt of all information for the process to begin.

Certification Process:

- a. Approval to build the Top Secret Space is submitted to the AD, Security by the requesting Business Unit. See "Requesting a Top Secret Space and Milestones" subsection above.
- b. The initial survey of the room will be conducted by the CNSI PMs ensuring that the 32 CFR 2001 physical security requirements for Top Secret Spaces are met.
- c. The CNSI PMs will coordinate with the local SSC and requesting Business Unit to ensure gaps between the current status of the room and 32 CFR 2001 requirements are addressed.
 - i. The Security Area must be equipped with NSA/CSS EPL shredder, GSA approved class 5 or 6 security container with FF-L-2740 lock, door signage that appropriately warns against unauthorized entry.
 - ii. All trash and recycling bins removed.
 - iii. No wireless devices of any kind are permitted.
 - iv. Each Responsible Party and Authorized Personnel must have their own, unique code to the IDS.
 - v. If windows are present, then they must be equipped with blinds, full coverage shades or similar to preclude visual observation.
- d. After-hours response must be coordinated with the SSC, monitoring entity and Business Unit.
- e. Once built, the CNSI PMs will perform a certification inspection. If the space meets requirements, the AD, Security will issue a certification letter.
- f. If certified for classified discussions by AD, Security, STE can be procured by the Business Unit from the IRS COMSEC POC.
- g. The Responsible Party of the Security Area must ensure that security protocols discussed above in IRM 10.9.1.8.6(2) are established and maintained for the space, to include immediate provision of a response roster to the monitoring entity.
 - i. A copy of the certification letter, IRS Form 5421, and the SF 701 must be placed by the primary entry door on the secure side of the Top Secret Space.
 - ii. The SF 702 must be kept on the non-secure side of the primary entry door to the Top Secret Space and on other security containers as required.
 - iii. Security Area Entry Door Warning Sign and current access roster on the non-secure side of all entry doors, found on the CNSI Website.

- iv. The SF 707 and 710 stickers must be placed on equipment as applicable.
- (6) Sensitive Compartmented Information Facilities (SCIF) request for Approval. Note that this process is only for the approval phase.
 - a. Prior to any designs or construction being created, the approval to build a SCIF must be obtained from the Assistant Secretary (A/S) of Treasury's Office of Intelligence and Analysis (OIA).
 - b. The requesting Business Unit must complete the request form provided by the CNSI PMs and include the following information, at minimum, on a Justification Memorandum on IRS letterhead:
 - i. Definition of need and why other SCIFs in the surrounding area cannot be used in lieu of new construction,
 - ii. Funding source for construction, protection, and maintenance,
 - iii. Stated willingness to cover additional expenses for the guard contract to adequately protect the SCIF (e.g., 24/7 response within 15 minutes maximum),
 - iv. Acknowledge necessity to appoint a trained primary and alternate Site Security Manager (SSM) during the construction phase, the CNSI PMs can provide the acceptable training. The SSM can serve as the SSO.
 - v. Acknowledge necessity to have a dedicated, trained (trainings may require travel, contact CNSI PMs for list of acceptable courses) authorized holder within the Business Unit to serve as SSO once the SCIF has been accredited. Roles and responsibilities of SSO will be outlined by Treasury and in accordance with the ICDs upon accreditation.
 - vi. Appointment of Top Secret Control Officer, who could also serve as the SSO upon the SCIF's accreditation.
 - vii. SCIF Facility Type: Secure Work Area, Temporary Secure Working Area, Continuous Operation, Temporary SCIF, Open Storage, or Closed Storage,
 - viii. Whether the building, if leased, has been reviewed per Interagency Security Committee requirements,
 - ix. If the facility is multi-tenant, list the tenant company names,
 - x. Number of TFIN drops required.
 - c. The Justification Memorandum must be signed by the requesting Business Unit's senior executive and sent to the AD, Security.
 - d. The Justification Memorandum is sent to the Chief, FMSS via the CNSI PMs through the AD, Security.
 - e. Chief, FMSS reviews and provides decision on SCIF packet. If approved the Chief, FMSS will forward the packet to the A/S of OIA via the Deputy Assistant Secretary for Intelligence and Analysis. If not approved, or if more information is needed, the packet goes back the CNSI PMs and over to the Business Unit.
 - f. Chief, FMSS briefs IRS Senior Leadership as required.
 - g. OIA will consider the request and provide an approval or disapproval to Chief, FMSS. The Chief, FMSS will return the packet back to the CNSI PMs.
 - h. CNSI PMs provide requesting Business Unit the final decision.
 - i. If approved, Treasury will provide information regarding the design, planning, and construction process in terms of whom the Cognizant Security Authority, Accrediting Official (AO), and SSO will be for the

- design, construction, and accreditation. The AO will be the primary POC for all security requirements to the CNSI PMs and Business Unit.
- j. If the SCIF is disapproved, there is no appeal process- the requesting Business Unit must find an alternate SCIF in the area to use.

(7) Appointment of Top Secret Control Officer and Responsibilities:

- a. The portions in parenthesis of the Top Secret Control Officer appointment language, below, must be replaced with the appropriate information before being sent to the appointee:
- i. In accordance with IRM 10.9.1, Classified National Security Information, **(given name of person)** is appointed to the position of Top Secret Control Officer for **(name of Business Unit)** at the (facility, campus, etc.). **(Name)** has been verified to have an active, in-scope (Top Secret clearance for Top Secret Space or TS/SCI clearance for a SCIF). **(Name)** is aware that it is (his/her) duty to understand and perform all the requirements noted in IRM 10.9.1 for the position of Top Secret Control Officer.
- b. If a Top Secret Control Officer can no longer perform their duties, a replacement must be appointed promptly. It is requested that a replacement be appointed in advance, if possible.
- c. Responsibilities, these are in addition to the Responsibilities noted in subsection IRM 10.9.1.1.3(8).
- i. Review "TSCO Duties and Responsibilities" material on the *CNSI Website* and discuss with CNSI PMs, as applicable, to understand duties; if the position is Top Secret Control Officer of a SCIF, Treasury OIA training's must also be received.
- ii. The Top Secret Control Officer must ensure that Top Secret is properly stored, shared, transmitted (to include use of required forms, double-wrapping, systems used, etc.) and that such information under their personal custody is destroyed under two-person control and the destruction is documented.
- iii. The Top Secret Control Officer must initially receive an open all Top Secret information in their organization, to include that delivered to the agency by outside courier and/or brought back to the agency by an authorized holder. All incoming Top Secret must be brought to (and logged in by) the Top Secret Control Officer by the next business day.
- iv. Maintaining the TD F 15-05.4, Document Control Register, for all Top Secret information held by the Business Unit. In maintaining the TD F 15-05.4, the Top Secret Control Officer must assign a Top Secret Control Number to all incoming and newly created documents in a calendar-year sequence (e.g., for CY2020: 20-001 and 20-002, where "20" is the calendar year when the document is initially recorded and the "01", "002" are the first and second documents, with numbers continuing sequentially). The control number must be noted on the front page of the document in a conspicuous place. Accountability records must be kept unclassified and can be stored in the security container housing the information so long as the Top Secret Control Officer maintains a backup.
- v. The results of the self-assessment will be provided in an unclassified, written report maintained by the Top Secret Control Officer for review during self-assessments. If there are documents that are unaccounted for, it is treated as a security violation, and the report includes a plan of action

with identifiable milestones and dates for resolving whatever circumstances caused the material to be lost or missing.

vi. Affix a TD F 15-05.10, Top Secret Document Record, as well as the TD F 15- 05.8, to all copies of Top Secret information leaving the immediate office/IRS prior to delivery to other offices for record/response.

1. TD F 15-05.10 must be printed on green card stock and attached to all Top Secret documents. TD F 15-05.10 is in addition to TD F 15-05.4.

2. The TD F 15-05.10 must be maintained for two years from the last, at which point it can be destroyed.

3. In process TD F 15-05.8, Receipt of Classified Information, must be used to start tracer actions after 30 days if they have not been returned. Completed TD F 15-05.8 must be maintained for three years if no outstanding tracer actions exist.

vii. Maintaining accountability records, receipts of the transmission and destruction of Top Secret information for three years from the last date noted.

10.9.1.9
(11-06-2023)
Contractors and CNSI

- (1) Before contractors can have access to CNSI, their contracts must meet the requirements of the NISP per EO 12829, as amended, and 32 CFR 117, the NISP Operating Manual (NISPOM), which include:
 - a. Department of Defense Form 254 (DD 254), Contract Security Classification Specification. This document must be created by the CNSI PM, reviewed/concurred by the Contracting Officers Representative (COR) and program office requesting the procurement, and signed by the Contracting Officer (CO) (or designee, with written designation). DD 254 must be incorporated during the following phases of contracting:
 - i. Solicitation: Prior to the procurement documents being released for solicitation, the CNSI PM must review any whose scope requires the contractors to have access to CNSI to perform their duties. The CNSI PM will create the initial DD 254 based on the solicitation documentation and route it as described above; a minimum of three weeks prior to the issuance of the solicitation is required. This is the only DD 254 that does not require a signature in block 17.h.
 - ii. Pre-Award: Prior to the award being issued, the CNSI PM must be made aware of the intended awardee to ensure that the company has the appropriate Facility Security Clearance (FCL) to handle the CNSI required in the scope of the contract. An award DD 254 is also prepared by the CNSI PM incorporating the awardee's information and routed; a minimum of three weeks prior to the intended award date is required.
 1. If the company does not have the required FCL, the CO will have to apply for the company to obtain the appropriate FCL per the NISP. The company cannot proceed with working on the contract until the FCL is obtained.
 - iii. Modification: If a modification occurs to the contract that affects the security requirements (e.g., higher level of clearance required, additional responsibilities in terms of protecting a Security Area, clearances no longer needed), then the documentation of the change must be routed to the CNSI PM so that the DD 254 can be modified to reflect the change; a

minimum of three weeks prior to the signing of the modification is required.

- b. Federal Acquisition Regulation (FAR) 52.204-2 must be included as a clause for contracts with classified scope; it must also be included in the solicitation documentation.
 - c. Security language specific to the scope of the contract must also be included into the solicitation by the COR, program office requesting the procurement, and CO. The CNSI PM, in the initial review of the solicitation documentation, can suggest appropriate security language.
- (2) Contractors cannot perform security duties (e.g., responsibility for opening/closing a Security Area), if these duties are not covered in the scope-specific security language or DD 254.
- (3) Contractors cannot access CNSI if:
- a. The contractor's company does not provide Personnel Security Office the required documentation to validate their Tier 3 or 5 (for Secret and Top Secret, respectively) investigations.
 - b. The contractor does not maintain their favorably adjudicated clearance.
 - c. The contractor's company does not have (or loses) the required FCL to perform the work or otherwise become non-compliant with the NISP.
- Note:** If any of these conditions exist, then access to CNSI must cease immediately.
- (4) If the awardee does not have an FCL of the appropriate level prior to award, the contractor cannot perform any CNSI work until an FCL has been applied for and obtained. If the FCL process fails on the part of the contractor, then the IRS will terminate the contract for cause.
- (5) If a Foreign Ownership Control or Influence issues are, or become, present in the contractor's company, then contractors must stop work until the issue is resolved. The CO, COR, CNSI PM, and the Defense Counterintelligence Security Agency (DCSA) will coordinate to resolve the issue.
- (6) NATO classified information must not be given to contractors without USSAN 1-07, Section 6 being met; FGI must not be given to contractors without proper contract language. Contact the CNSI PMs at **FMSS Classified Security Information Team* if access to NATO or FGI is required for the contractors to complete their scope of work.
- (7) The COR or Program Manager of the procuring Office reviewing CNSI products of the contractor must, at a minimum, have a security clearance commensurate to the level of the contract they are managing.
- (8) Personal Services contractors, to include experts and consultants, that require access to CNSI or a security clearance will be processed for that clearance by IRS Personnel Security. The contract must include security protocols to protect CNSI, which the CNSI PMs will help the requesting Business Unit accomplish prior to the contract being awarded.

- a. The preferred method of transmission of CNSI is via secure system approved to handle the applicable level of CNSI.
- b. Flash/thumb drives are not approved for storing or transporting CNSI within, or out of, the IRS under any circumstances.
- c. Be an IRS authorized holder with a courier card or letter (if leaving the IRS Facility), appropriate approvals from management as applicable, and a documented travel plan as applicable. Contractors will require approvals from their company's management, as applicable.
- d. Ensure the recipient is cleared, has need-to-know, and has the appropriate storage facility for the level of information being transmitted to them.
- e. CNSI will never be left unattended, it must be given to an authorized recipient.
- f. Permission and information on how to transmit COMSEC, NATO, FGI, and SCI must be obtained from Treasury points of contact in advance.
- g. Prior to disclosing CNSI to foreign nationals or entities, Treasury's Counterintelligence must be consulted and provide written disclosure authorization unless the material is marked as releasable to the recipient.

(2) Transmission within an IRS Facility:

- a. Method:
 - i. It is required that the document have an appropriate cover sheet or the equipment have the appropriate SF sticker and be in an opaque cover.
 - ii. No specific approvals required in advance and no courier card or letter is required.
 - iii. If the CNSI is too large for a folder or envelope, then place the material in a box.
- b. Process:
 - i. The document(s) are placed into an opaque folder or envelope.
 - ii. The authorized holder hand-carries the documents or material to their recipient and ensures the TD F 15-05.8 is signed in Section C.

(3) Transmission out of IRS Building but within local commuting area.

- a. Method:
 - i. The document must have the appropriate cover sheet or SF and be double-wrapped. as follows in 1-3:
 - 1. The inner, opaque envelope must contain the entirety of both addressee's information (given name, address), have overall/banner classification markings on both sides of the envelope and have tamper-evident tape placed around seals. The inner envelope must also have the special types of handling instructions, as applicable. All seams should be sealed with reinforced gummed tape to prevent tampering.
 - 2. This envelope must then be put into another opaque envelope that is sealed and addressed the entirety of both addressee's information (given name, address). All seams should be sealed with reinforced gummed tape to prevent tampering. A locked briefcase or pouch may serve as the outer envelope – see subsection IRM 10.9.1.10(8).
 - 3. If the material is too large for envelopes or similar, the material must be enclosed in two sealed opaque boxes, the marking of which will mimic

the envelopes.

ii. Approval and cognizance of the authorized holder's management for the trip should be given.

b. Process:

i. The local Classified Document Custodian will create an inventory of the CNSI being transmitted, keeping one copy and providing the other to the courier.

ii. The courier must have a valid courier card or letter.

iii. The document or materials are appropriately wrapped and addressed.

iv. The trip should be planned out in advance to ensure that it is point-to-point, if possible, and that the recipient(s) are waiting for the information.

v. While traveling, couriers shall promptly report to Cognizant Security Officials any suspicious contacts and refrain any act that might jeopardize the CNSI (e.g., discussing in public, deviating from authorized schedule, leaving CNSI unattended, opening materials).

vi. Upon reaching the destination, the authorized holder must verify the identity of the recipient(s) via a government issued identification against the printed name on the TD F 15-05.8.

vii. Prior to signature, it must be noted on the TD F 15-05.8 which documents were kept by the recipient. The recipient(s) will sign TD F 15-05.8 in Section C.

viii. The courier will return to IRS and ensure the Classified Document Custodian conducts the inventory of any returned documents. The Classified Document Custodian is given the TD F 15-05.8 for maintenance in accordance with this IRM.

ix. Documents that are not accounted for must be handled as a security violation.

(4) Mailing:

a. Method:

i. Ensure the document has the appropriate cover sheet, includes the TD F 15-05.8 for receipting purposes, and is double wrapped as discussed in (3) above.

ii. Within the U.S. and Puerto Rico, the United States Postal Service (USPS) Priority Mail Express or Registered mail may be used, but the waiver of signature and indemnity blocks must not be completed. The package must be signed for.

iii. Cleared, U.S. owned commercial carriers may be used for bulky material within the continental U.S. only. A list of GSA approved domestic express services can be found here: *GSA Transportation Logistics Services*.

iv. The use of street side collection boxes is prohibited.

v. Only Confidential and Secret may be mailed, Top Secret cannot be mailed.

vi. Selected types of CNSI must be handled separately from the processes discussed above, information on how to transmit these items must be obtained from Treasury points of contact, namely COMSEC, NATO, FGI, and SCI.

b. Process:

- i. The authorized holder mailing the documents must make an inventory of what is in the package for their records and duplicate the information on the TD F 15-05.8, which will be sent with the package.
- ii. The documents will then be double-wrapped.
- iii. The authorized holder will mail the documents and keep the receipt as part of tracking.
- iv. The TD F 15-05.8 must be returned with the recipient's signature within 30 calendar days of the package being mailed. If it is not, the authorized holder must contact the recipient to determine whether the package was received and if there was a delay with the return of the TD F 15-05.8.
- v. If the recipient did not receive the package, a tracer action must be started.
- vi. The authorized holder must maintain the TD F 15-05.8 in accordance with this IRM.

(5) Continental United States: Flying in the 48 contiguous states

a. Method:

- i. Ensure the document has the appropriate cover sheet, includes the TD F 15-05.8 for receipting purposes, and is double wrapped as discussed in (3) above.
- ii. The couriating authorized holder is responsible for ensuring all travel documents and identification are current and valid.
- iii. The airline, if used, must be U.S. owned or part of the U.S. military.
- iv. Prior coordination with a U.S. government or cleared contractor facility during the night is required. The storage provided must meet the 32 CFR 2001 requirements for the CNSI needing storage.
- v. It is recommended that Treasury Counterintelligence be contacted in advance to receive a threat update for the trip.

b. Process:

- i. The Classified Document Custodian will create an inventory of the CNSI being transmitted, keeping one copy, and providing the other to the courier.
- ii. The courier must ensure they have a valid courier card or letter.
- iii. The CNSI document or materials are appropriately wrapped and addressed.
- iv. The trip should be planned out in advance to ensure the trip includes the fewest stops and overnight layovers as possible and that the recipient(s) are waiting for the information on the day of arrival at the terminus.
- v. When traveling on commercial air, upon arrival at the screening checkpoint the authorized holder will ask to speak to the Transportation Security Administration Security Officer and present the required identification and authorization documents to ensure that the CNSI package is not inspected.
- vi. While traveling, couriers shall promptly report to their management, the CNSI PMs, and the Treasury SSO any suspicious contacts and refrain any act that might jeopardize the CNSI (e.g., discussing in public, deviating from authorized schedule, leaving CNSI unattended, opening materials).

- vii. The use of hotel safes to store CNSI is prohibited.
 - viii. Upon reaching the destination, the authorized holder must verify the identity of the recipient(s) via a government issued identification.
 - ix. The recipient(s) will sign TD F 15-05.8, Receipt for Classified Information, is signed in Section C. It must be noted on the TD F 15-05.8 which documents were kept by the recipient.
 - x. The courier will return to IRS and ensure the Classified Document Custodian conducts the inventory of returned documents. The Classified Document Custodian is given the TD F 15-05.8 for maintenance in accordance with this IRM.
 - xi. Documents that are missing, but not receipted for, must be handled as a security violation.
- (6) Outside the Continental United States: Flying to any location outside of the 48 contiguous states: Hawaii, Alaska, U.S. territories, or foreign location
- a. Method:
 - i. Ensure the document has the appropriate cover sheet, includes the TD F 15-05.8 for receipting purposes, and is double wrapped as discussed in (3) above.
 - ii. The couriating authorized holder is responsible for ensuring all travel documents and identification are current and valid.
 - iii. The airline, if used, must be U.S. owned or part of the U.S. military.
 - iv. Prior coordination with a U.S. government or cleared contractor facility during the night is required. The storage provided must be meet the 32 CFR 2001 requirements for the CNSI needing storage.
 - v. Treasury Counterintelligence must be contacted in advance to receive a threat update prior to the trip.
 - vi. It is recommended that the *Department of State's International Travel website* is reviewed for country information and enrollment in the U.S. Bureau of Consular Affairs to receive travel and security updates.
 - vii. It is recommended to contact customs, Transportation Security Administration, and/or immigration officials to facilitate clearance through the airline screening process.
 - viii. It is recommended that the courier coordinate with IRS-CI or Treasury Attaché responsible for the area to obtain and maintain a copy of U.S. Embassy and/or Consulate points of contact for the countries where a layover is required to help with storage or in case of an incident.
 - b. Process:
 - i. The local Classified Document Custodian will create an inventory of the CNSI being transmitted, keeping one copy, and providing the other to the courier.
 - ii. The courier must ensure he/she has a valid courier card or letter.
 - iii. The document or materials are appropriately wrapped and addressed.
 - iv. The trip should be planned out in advance to ensure the trip includes the fewest stops and overnight layovers as possible and the recipients(s) are waiting for the information on the day of arrival at the terminus.
 - v. When traveling on commercial air, upon arrival at the screening checkpoint the authorized holder will ask to speak to the Transportation Security Administration Supervisory Transportation Security Officer and present the required identification and authorization documents to ensure that the CNSI package is not inspected.

- vi. At border crossings, there is no assurance of immunity from search. Presentation of courier card/letter to the senior customs official will usually allow the material to pass through unopened. If the senior official demands to see the package contents, the package may be opened in their presence (outside public view) and should be limited to only proving the package does not contain another item. The senior official should sign the TD F 15-05.8 or the courier certificate stating the document was opened. Note the senior official's name. The package should be re-wrapped as well as possible to conceal the CNSI.
- c. The Cognizant Security Official and the recipient will need to be informed in writing that the package was opened.
 - i. While en route, couriers shall promptly report to Cognizant Security Officials any suspicious contacts and refrain any act that might jeopardize the CNSI (e.g., discussing in public, deviating from authorized schedule, leaving CNSI unattended, opening materials).
 - ii. If an incident occurred (e.g., loss, suspicious contact, etc.), the Cognizant Security Officials, IRS-CI or Treasury Attaché responsible for the area, and Embassy or Consulate in the country where the incident occurred must be made aware.
 - iii. The use of hotel safes to store CNSI is prohibited.
 - iv. Upon reaching the destination, the authorized holder must verify the identity of the recipient(s) via a government issued identification.
 - v. The recipient(s) will sign TD F 15-05.8, Receipt for Classified Information, in Section C. It must be noted on the TD F 15-05.8 which documents were kept by the recipient.
 - vi. The courier will return to IRS and ensure the Classified Document Custodian conducts the inventory of any returned documents. The Classified Document Custodian is given the TD F 15-05.8 for maintenance in accordance with this IRM.
 - vii. Documents that are missing, but not receipted for, must be handled as a security violation.
- (7) Special Considerations:
 - a. Top Secret:
 - i. The TD F 15-05.8 must be used as discussed below in 10.9.1.10(7)c.
 - ii. Transmission of Top Secret information outside of an IRS facility is only accomplished by:
 - 1. Person-to-person contact between authorized holders.
 - 2. State Department diplomatic pouch, which requires prior coordination with Large Business and International or CI.
 - 3. The Defense Courier Service or an authorized government agency courier service.
 - a. This is an expensive option and should only be used as a last resort; contact the CNSI PM with questions.
 - b. The Defense Courier Service is intended to securely transport Top Secret information; SCI, Secret, or Confidential may be included, if the CNSI destination is the same.
 - 4. A designated courier with Top Secret clearance.

iii. Consultation with the Top Secret Control Officer or CNSI PMs must take place prior to transmission regarding the methods for the transmission, whether the material will be briefed, to whom it will be given, etc.

b. Secret or Confidential:

i. The TD F 15-05.8 must be used for Secret information.
ii. Transmission of Secret or Confidential within the U.S., District of Columbia, and the commonwealth of Puerto Rico must be carried out by any of the following methods:

1. One of the means authorized for Top Secret information (subject to the Defense Courier Service restriction in IRM 10.9.1.10(7)a).
2. The USPS Priority Express or Registered mail, the waiver of signature and indemnity block on the label must not be completed.
3. Cleared commercial carriers or cleared messenger services.

c. TD F 15-05.8 is used to document the transmittal and receipt of Secret or Top Secret hand-carried or mailed to another authorized holder.

i. The document must be included with the package for the recipient to sign and return to the sender/courier.
ii. The document must be fully filled out and should be kept unclassified.
iii. If, within 30 calendar days, the receipt hasn't been returned, the authorized holder must start tracer actions to attempt to recover the package. If the package cannot be accounted for or was found to be lost, it must be reported as a security incident.

1. Tracer actions are steps taken to track down a missing package and include:

- a. Calling the recipient to determine if they received the package; if they did, request the TD F 15-05.8 be returned.
- b. If the recipient did not receive the package, use the receipt from the Priority Express or Registered mail to determine its last known location.
- c. Call or, if feasible, go in person to the Post Office that was the last known location and search the facility for the missing package.
- d. Report the incident to the Classified Document Custodian responsible for the courier and management per IRM 10.9.1.14.

iv. The form must be maintained for 3 years prior to being destroyed. It can be destroyed if there are no outstanding tracer actions open. The destruction does not need to be documented.

(8) Briefcases or Zippered Pouch:

- a. Clearly and recognizably display the name and street address of the organization sending the classified material, and the name and telephone number of a point of contact within the sending activity, on the outside of the briefcase or pouch.
- b. Each pouch or briefcase must have a unique serial number that is clearly displayed on the exterior surface.
- c. Lock the briefcase or pouch and place its key in a separate sealed envelope.

- d. Store the briefcase or pouch, when containing classified material, according to the highest classification level and any special controls applicable to its contents.
- e. Ensure the activity authorizing use of the briefcase or pouch maintains an internal system to account for and track the location of the pouch and its key.
- f. Use a briefcase or pouch shall in no way remove personal responsibility to ensure that the classified material is delivered to a person who has an appropriate security clearance and access for the information involved.

10.9.1.10.1
(11-06-2023)

Courier Requirements

- (1) If CNSI must be couriered outside the building in which it is located for any reason, the employee performing that task must have either a courier letter or card.
- (2) IRS employees performing courier duties must:
 - a. Have a final, favorable security clearance at the level they need to courier,
 - b. Proof of courier training completed within the last 30 days and
 - c. Not be currently detailed to another agency to request a courier card or letter from IRS.
- (3) Authorized holders with a need to hand-carry CNSI must request a courier card via a TD F 15-05.12, Request and Receipt for Courier Card available on the *CNSI website*. Either a courier card or letter must be requested and submitted a minimum of 14 business days in advance.
 - a. If the authorized holder has a frequent and recurring need, (e.g., a minimum of 12 times per year) then a courier card will be applied for. Anything less frequent in terms of times per year, a courier letter will be applied for.
 - b. Treasury has delegated the issuance of courier cards for CI employees to CI. The CI Security Specialist must receive and process TD F 15-05.12 for CI employees.
 - c. For all other IRS employees, except CI, TD F 15-05.12 must be sent to the CNSI PM.
 - d. The AD, Security must sign all courier cards and letters.
- (4) Authorized holders requesting a courier card must provide, with the TD F 15-05.12, Request and Receipt for Courier Card, a digitized color photograph on a plain background.
 - a. CI Security Specialist or CNSI PM must use TD F 15-05.7, Courier Card Badge, to create the courier card.
 - b. Upon receipt of the courier card, the authorized holder/courier must sign the TD F 15-05.12 and return it to the CI Security Specialist or CNSI PM.
 - c. CI Security Specialist and CNSI PM must maintain records of the TD F 15-05.12 until the card has expired.
- (5) Authorized holders who must carry CNSI once or routinely on a non-recurring basis must request a courier letter via TD F 15-05.12, with specific attention paid to noting the dates of couriating on the "Frequency of Courier Responsibilities".

- a. CI Security Specialist and CNSI PM must use Attachment 2 in the TD P 15-71, entitled "Sample Courier Letter Format," to create the courier letter.
- (6) If the card or letter grants the authorized holder the ability to carry SCI, Treasury's Special Security Office (SSO) must be the approving official. SCI cannot be stored in other than a SCIF.
- (7) If the card or letter is expired or no longer needed (e.g., employee is terminating employment with the Business Unit, etc.), the card or letter must be returned to the CI or CNSI PM who issued it.

10.9.1.11
(11-06-2023)
**North Atlantic Treaty
Organization (NATO) and
Foreign Government
Information (FGI)**

- (1) NATO classified information shall be controlled and safeguarded according to United States Security Authority for NATO (USSAN) Instruction 1-07. This section applies only to NATO CNSI. A summary of the requirements are listed as follows:
 - a. NATO users will take overall direction and guidance directly from NATO security documents.
 - b. Prior to access, users must receive a briefing regarding the protection of NATO CNSI and complete a statement acknowledging receipt of the briefing, the SF 312 is not applicable. The briefing is obtained by contacting Treasury via *SSO@Treasury.gov*, with a mandatory cc to **FMSS Classified Information Security Team*, and request the briefing. Users must also have the requisite U.S. security clearance and need-to-know to obtain access.
 - c. Security Education and awareness training on the proper handling and safeguarding of NATO must occur and will be presented by Treasury.
 - d. *Authorized holders **cannot** store NATO in IRS facilities or on IRS systems. Treasury's TSDN and TFIN are **not accredited** to store NATO without justification and permission.* If NATO does get loaded or emailed to a Treasury TSDN account, permission to keep the information must be obtained from Treasury's SSO.
 - e. Combinations to containers storing NATO must be changed when someone possessing the combination no longer needs or can have access, when a compromise has occurred or is suspected, or annually.
 - f. Documents containing NATO classified must be marked as listed below, additional information is specified in 5.3 of USSAN 1-07:
 - i. When classifying NATO information, the derivative classifier must express the date when the information can be downgraded or declassified.
 - ii. The top and bottom of each page shall be marked with the overall classification. If individual enclosures or attachments may be marked with a classification level lower than the document.
 - iii. Each portion of a document, including paragraphs, shall be assigned classification markings.
 - iv. Dissemination Limitation Marking may be applied to restrict the distribution of NATO information. NATO markings must be removed from all information approved for release to the public.
 - v. U.S. documents containing extracted NATO information must be marked and handled as follows:

1. U.S. classification marking that reflects the highest level of NATO or U.S. classified information therein. The statement "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" must appear on

the front of the document.

2. Each page of a U.S. document containing NATO information shall be marked with a U.S. classification level that reflects that the highest level of U.S. or NATO classified information found on the page.

3. Each portion, including paragraphs, of a U.S. document containing NATO classified information shall be marked according to the highest level of information contained within.

4. The derivative classifier must be the longest declassification or downgrade instruction on the document (e.g., if the three dates for declassification are 20380422, 20400422, 20450422, then the declassification instruction is 20450422).

5. Declassification and downgrading instructions shall indicate that the NATO information is exempt from declassification or downgrading without the prior consent of NATO, in the absence of other originator instructions, citing the reason "Foreign Government Information".

6. A U.S. document containing accountable NATO information shall be logged, accounted for and handled in the same manner required for NATO accountable information.

- g. Prior to the release of documents containing COSMIC Top Secret (CTS) and NATO Secret (NS), Treasury must be contacted to coordinate with the Department of Defense's Central U.S. Registry. CTS shall not be reproduced without authorization, accountability, marking, and control provisions listed in AC/35-D/2002, Directive on the Security of Information.
- h. NS and NATO Confidential (NC) may be reproduced as required, but NS must be marked with the copy number and total copies made (e.g., "Copy 1 of 4").
- i. Transmission of CTS, NS and NC have specific requirements and require a NATO courier certificate rather than a Treasury one if the documents are being couriered.
 - i. Receipts are required for CTS, NS and any special category information.
- j. CTS must be returned to the appropriate registry for destruction; NS and NC must be destroyed in the same manner as U.S. CNSI.
- k. Security incidents involving NATO information must be reported in accordance with this IRM.
- l. If NATO is stored on a secure system (e.g., Department of Defense, Secure Internet Protocol Router (SIPR), or Joint Worldwide Intelligence Communications System (JWICS)) it is not permitted on Treasury based systems.
 - i. Records of access for systems storing NATO must be kept; CTS for 10 years, NS for 5 years.
 - ii. Systems storing NATO, control units, storage units, periphery equipment, etc. have physical requirements for the rooms they are stored in.
 - iii. Systems storing NATO exclusively must be marked in addition to the required SF stickers.
 - iv. Emails that include NATO must be marked in accordance with USSAN 1-07 and only be sent from and to networks accredited to process NATO.

(2) Foreign Government Information (FGI)

- a. To avoid inadvertent compromise, classified FGI shall be stored in a manner that will avoid commingling with other material to include NATO. For small volumes of material, separate files in the same vault, container, or drawer as other CNSI will suffice.
- b. FGI shall be re-marked if needed to ensure the protective requirements are clear. FGI may retain its original classification if it is in English. However, when the foreign government marking is not in English, or when the foreign government marking requires a different degree of protection than the same U.S. classification designation, a U.S. marking resulting in a degree of protection equivalent to that required by the foreign government shall be applied.
- c. Country codes can be found in TD P 15-71, Chapter III, Section 8.
- d. U.S. documents containing FGI shall be marked as required below in subsection 10.9.1.11(2)e. The foreign government document or authority on which derivative classification is based must be identified on the "Derived from:" line, in addition to the identification of any U.S. classification authority. A continuation sheet should be used for multiple sources, if necessary. A U.S. document containing FGI cannot be declassified or downgraded below the highest level of FGI contained in the document without the written permission of the foreign government or international organization that originated the information.

i. The syntax for marking documents consisting solely of FGI and for jointly produced documents is different than for U.S. CNSI. Both begin with a "/" without a preceding classification. The syntax is:

1. Classified non-U.S. documents: "[country code] [non-U.S. classification]"

2. Classified joint documents: "[//JOINT [classification] [country codes]"

Note: U.S. classification markings, non-U.S. classification markings, and JOINT classification markings are mutually exclusive – they may not be used at the same time in a banner line or a portion mark.

- e. FGI Markings used in U.S. documents:
 - i. FGI markings are used in U.S. products to denote the presence of foreign-controlled information.
 - ii. As damage to the national security is the criteria for classification, FGI requiring protection from disclosure must automatically be classified at a level no less than Confidential, unless otherwise noted in security agreements between the U.S. and foreign governments.
 - iii. FGI documents should state "This Document Contains (country of origin) Information" if disclosure of the country is allowed, if not then the marking will be "This Document Contains FGI Information". If the fact that the document contains FGI should not be disclosed, then use strictly U.S. markings.
 - iv. Use "FGI" with the trigraphic country codes and international organization tetragraphs in the banner line; portion markings for included FGI shall be as stated:
 - 1. Country codes are not included in portion markings when all portions match the banner country codes.

- a. If the country can be named, then the portion mark would be: "(country code)-(classification level)"
 - b. If the country can't be named, then the portion mark would be: "FGI-(classification level)"
2. If a JOINT portion is extracted into a U.S.-produced non-JOINT document, then the country codes must be listed, in alphabetical order, in the portion markings: "//JOINT [classification] [country codes]"
 3. When JOINT information is extracted and used in a derivative U.S. document, the JOINT portions must be separate from U.S. classified information. The banner line of the derivative U.S. document shall show the highest classification level of all portions, expressed as a U.S. classification marking. The JOINT markings are used in applicable portions. FGI markings will be added to the banner line and will include all non-U.S. country codes identified in the JOINT portion(s).
 4. The classification authority block is used only when the U.S. is one of the co-owners.
- f. FGI Markings used in non-U.S. documents:
 - i. This subsection provides guidance on marking documents consisting entirely of FGI.
 - ii. All classification markings on FGI (banner and portion) begin with a double forward slash "//". The required format is "//[country code] [equivalent classification]"
 - iii. Equivalent classifications are: Top Secret, Secret, Confidential, Restricted, and Unclassified.
 - iv. Equivalent foreign government classification markings should be used in conjunction with the classifications above to determine the appropriate marking. If in doubt, consult the CNSI PMs in an unclassified manner via **FMSS Classified Information Security Team*.
 - v. FGI classifications shall not be annotated in the banner line with U.S. classification markings or JOINT classification markings. These three marking categories are mutually exclusive in the banner lines and portion marks.
 - vi. No classification authority block shall be used as all non-U.S. information is excluded from the marking requirements.
 - g. Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.
 - h. The transmission of FGI within the United States among U.S. Government agencies and U.S. contractors with a need-to-know must be in accordance with TD P 15-71.
 - i. The international transfer of foreign government classified information must be by government officials through government-to-government channels, or channels agreed upon in writing by the originating and receiving governments (collectively "government-to-government transfer").
 - j. The receiver shall protect FGI equivalent to the protection required by the provider of the information. FGI shall be controlled and safeguarded in the same manner as prescribed for U.S. classified information, except as described below in i.- iv.
 - i. Control of Foreign Government Top Secret Information. Maintain records for 5 years of the receipt, internal distribution, destruction, annual inventory,

access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction must be witnessed.

ii. Control of Foreign Government Secret Information. Maintain records for 3 years of the receipt, distribution, external dispatch, reproduction, and destruction of material containing Foreign Government Secret Information.

Other records may be necessary if the originator requires. Secret FGI may be reproduced in quantities limited to meet the requirements of the mission.

iii. Control of Foreign Government Confidential Information. Maintain records for 2 years for the receipt and external dispatch of Confidential FGI. Do not maintain other records for foreign government Confidential information unless required by the originating government. Confidential FGI may be reproduced to meet mission requirements.

iv. Foreign Government Restricted Information and Information Provided in Confidence. To ensure the protection of Restricted FGI or foreign government unclassified information provided in confidence, such information shall be classified on the basis that unauthorized disclosure of FGI is presumed to cause damage to the national security. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the information shall be marked "CONFIDENTIAL-Modified Handling" and the following requirements must also be met:

1. Mark foreign government documents that have a classification designation which equates to RESTRICTED, as well as unclassified foreign government documents provided on the condition that they shall be treated "in confidence", with the originating government and "Restricted" (e.g., a French document would be marked "//FRA Restricted"). Additionally mark "CONFIDENTIAL - Modified Handling" above the bottom banner marking.
2. The information shall be provided only to those individuals who have an established need to know, and where access is required by official duties.
3. Individuals given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.
4. Documents shall be stored to prevent unauthorized access (e.g., a locked desk or cabinet or a locked room to which access is controlled).

k. FGI shall not be disclosed to nationals of third countries, including foreign nationals who are protected individuals or permanent resident aliens, or to any other third party, or used for other than the purpose for which the foreign government provided it without the originating government's written consent. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required.

l. Security incidents involving FGI must be reported in accordance with IRM 10.9.1.14.

10.9.1.12
(11-06-2023)
Destruction of CNSI

- (1) Destruction must obstruct retrieval and prevent recognition and reconstruction. Paper documents must be destroyed using an NSA/CSS EPL approved cross-cut shredder, which cuts to 1mm x 5mm.
- (2) Destruction can also be accomplished by burning, wet pulping, melting, mutilation, chemical decomposition or pulverizing, if available.

- (3) CNSI electronic media must be destroyed using an NSA/CSS EPL approved degausser in accordance with NSA 9 -12, NSA/CSS Storage Device Sanitization Manual and a) - d) below:
 - a. Upon degaussing, the SF sticker denoting CNSI must be removed from the equipment,
 - b. hard drives must have their platters destroyed,
 - c. the equipment can be recycled or disposed of,
 - d. store electronic media and processing equipment in a GSA approved security container until it can be destroyed.

Note: Further technical guidance on destruction (methods, equipment, and standards for disposing) of CNSI electronic media and processing equipment may be obtained through the CNSI PM.

10.9.1.12.1
(11-06-2023)

Destruction Process

- (1) Destruction of Top Secret information. Top Secret information, to include duplicates, working papers, etc. will be destroyed in the presence of two authorized persons; one authorized holder performs the destruction and the other person serves as a witness. Both individuals must sign the TD F 15-05.5, Classified Document Certificate of Destruction. The completed TD F 15-05.5 must be maintained on file for three years, after which it may be destroyed. No record of the destruction certificate itself is required. Questions regarding this process should be directed to the Top Secret Control Officer or CNSI PMs. Top Secret cannot be placed in a burn-bag.
- (2) Destruction of Secret or Confidential Information. Secret or Confidential information, to include duplicates, working papers, etc., does not require a certificate of destruction.
- (3) Burn-bags for Temporary Storage. Secret and Confidential only, may be placed in sealed opaque containers commonly designed as "burn-bags." Burn-bags feature multiple alternating groupings of red and white diagonal stripes, which can be purchased on GSA Advantage.
 - a. Burn-bags awaiting destruction must be protected while in the end-user's custody. Burn-bags will only be collected, and contents immediately destroyed, by authorized holders.
 - b. When not in active use, burn-bags containing CNSI are protected commensurate with the level of CNSI within.
 - c. Use of burn-bags should be limited as CNSI requiring destruction should be shredded as soon as possible instead of stored awaiting for bulk destruction.
- (4) The Security Container Custodian must ensure that a review of the information in the security container takes place annually by all those with access to ensure the removal and destruction of CNSI that is no longer needed. The review does not require documentation.

10.9.1.13
(11-06-2023)

End of Day Security Checks

- (1) End-of-day security checks will be conducted in areas that handle, process, or store CNSI. The SF 701, is used to document the check. The SF 701 is a systematic means to thoroughly inspect a Security Area and any areas that CI has certified for use of STE equipment (optional for other places storing hard-copy CNSI in security containers) and to allow for accountability if any irregularities are discovered.

- (2) The history of the SF 701 must be kept for 90 calendar days and each SF 701 include, per the TD P 15-71, the following items:
 - a. "Authorized persons have locked or checked Security containers."
 - b. "Desks, wastebaskets, and other surfaces and receptacles are free of CNSI."
 - c. "Windows/doors are locked."
 - d. "Electronic media (such as disks, tapes, removable hard drives, etc.) for processing CNSI have been properly stored."
 - e. "Security alarms and protective equipment are activated."
 - f. Note that individual groups may include additional information on the SF 701 to suit any unique circumstances (e.g., "ensure all emergency exits are engaged in the closed position," "ensure the SF 702 notes that the security container has been checked," etc.).
- (3) When securing or checking a security container, check each drawer to ensure that it does not open, and note the completed check on the SF 702 "check by" column. The history of the SF 702 for any security container must be 90 calendar days.

Note: Instructions for usage of the SF 701 and SF 702 can be found on the *CNSI Website*.

10.9.1.14
(11-06-2023)
**Types of Security
Incidents and
Associated Inquiries**

- (1) Discovery and Initial Reporting. The employee discovering the security incident is responsible to ensure prioritization of the protection of the classified material and to promptly provide the initial report in an unclassified manner to the Security Container Custodian (as applicable), local Classified Document Custodian, Business Unit management, and CNSI PM. CI may have additional reporting requirements.
 - a. The discovering employee must ensure classified information is protected by an employee with a National Security Clearance or in a General Services Administration (GSA) approved Class 5 or 6 security container. If the classified material was sent via email inappropriately, "spillage," all recipients must be instructed to not access or manipulate (e.g., forward, download attachments, delete, etc.) the email.
 - b. The initial report must be unclassified and cover the subject or type of incident (e.g., spillage on an unclassified system, container found open or unsecured, etc.), date the incident occurred, location of incident, the level of CNSI involved, actions taken to prevent further unauthorized access, and individual reporting the incident; additional information can be included for context as needed.
 - c. The CNSI PM will notify the Senior Agency Official and Treasury OSP; depending on the incident, the CNSI PM may make additional notifications to others such as the IRS/Treasury COMSEC manager or SSO.
 - d. If the incident was caused by an authorized holder from another agency, but involved IRS authorized holders, notification to the Classified Document Custodian and CNSI PM is still required, but no further inquiry actions are required. IRS authorized holders must cooperate with the at fault agency's inquiry.
 - e. If an IRS authorized holder is detailed to work at an Embassy is at fault or another agency is at fault for a security incident, notification to the authorized holder's Classified Document Custodian, Business Unit manager, and the CNSI PM is required, promptly. IRS will not carry out

the inquiry, but the authorized holder must provide their Classified Document Custodian, Business Unit manager, and CNSI PM the finalized report and all attachments.

- f. All evidence related to the incident should be preserved as is for future inquiry or investigation.
- (2) Initial/Preliminary Inquiry. The Initial or Preliminary Inquiry is conducted to uncover the facts of the unauthorized disclosure of CNSI and is administrative in nature. The primary purpose is to provide the who, what, where, when, why, and how as well as any corrective actions taken to date, if any, and recommendations, if any, to IRS management to immediately mitigate the risk of the security incident happening again. The inquiry provides the facts to determine if a security infraction or violation occurred and if further investigation is required.
- a. The CDC will act as the Inquiry Official and complete the Inquiry Report. If the CDC is materially involved in the security incident, the Business Unit will appoint an Inquiry Official.
 - b. Inquiries must be completed within 30 calendar days of the initial report. An extension beyond the 30 calendar days needs to be requested with justification in writing to the CDCs management appointing authority within the Business Unit with a courtesy copy to the CNSI PMs via *FMSS Classified Information Security Team.
 - c. The Inquiry Report is unclassified, and care must be taken to ensure no classified information is included.
 - d. The Inquiry Report must be marked and protected as Sensitive but Unclassified and include:
 - i. A summary of the findings. The summary should be as long as required to provide the head of the activity with a reasonably good picture of what occurred and should support the recommendations provided. In addition, it should document what is not known about the event in question.
 - ii. An unclassified summary of the highest classification level involved, what agency owns the CNSI, identification of the material (i.e., message, letter, staff study, imagery, magnetic media, etc.) to include document control numbers, and what the CNSI pertains to, i.e., as part of a FBI case, tax examination, etc.
 - iii. A detailed timeline of the events that clearly shows the sequence of events, dates and times, and names of persons involved.
 - iv. Contact information of all personnel contacted as part of the Inquiry. Include names, grade, title, Office, Bureau, unclassified email, and phone number.
 - v. Any identified deficiency or vulnerability on security policy or procedures. Describe how the deficiency or vulnerability led or contributed to the incident. Include any assessment regarding systemic weaknesses or vulnerabilities in established security practices (e.g., non-existent, out-of-date, or ineffective policies, procedures, or training) that must be corrected; suggest the corrective actions required to correct deficiencies or vulnerabilities.
 - vi. A list of corrective actions taken by management of the Business Units involved, if any have been put in place.
 - vii. Recommendations for the office, business unit, and/or Bureau that may be taken to immediately mitigate the risk of a similar security incident from happening in the future.

- viii. Interview statements and/or records, documentary evidence, exhibits, etc. as attachments.
 - e. Upon completion of the Inquiry the Inquiry Official will provide the CNSI PMs the final report via *fmss.classified.information.security.team@irs.gov* and the Senior managers of those Business Units involved.
 - f. The CNSI PMs will forward the report to:
 - i. AD, Security
 - ii. Treasury OSP for further review.
 - iii. IRS Personnel Security. At the conclusion of the Inquiry Report the CNSI PMs will forward the report to the Personnel Security Office via the email: *hco.ps.national.security.programs@irs.gov*.
 - g. Reporting. The Inquiry Official must notify the following when applicable.
 - i. TIGTA. If the security incident gives an indication of an insider threat, espionage, criminal, or employee misconduct, then the Treasury Inspector General for Tax Administration (TIGTA) must be notified immediately via their hotline (800-366-4484) or email *complaints@tigta.treas.gov*. The Classified Document Custodian, or Inquiry Official, must discuss with TIGTA whether TIGTA should proceed with the inquiry or not.
 - ii. OCA. The OCA or originator of the information must be notified immediately of a potential loss, compromise, or unauthorized disclosure.
 - iii. CSIRC. For spillage incidents involving IRS personnel other than CI, CSIRC must be contacted immediately by the Inquiry Official in an unclassified manner for further instructions via *CSIRC@irs.gov*, CSIRC Security Operations Center Lead, and Associate Director, Cyber Threat Fusion Center in an unclassified manner
 - iv. IRS CI. For spillage incidents involving IRS CI, *CIDATASPILL@ci.irs.gov* must be contacted promptly in an unclassified manner by the Inquiry Official. The Inquiry Official may be directed by Treasury to notify IRS CI for other security incidents if criminal activity is indicated.
 - v. CNSI PMs. All security incidents must be reported to the CNSI PMs. If, during the Inquiry, the Inquiry Official finds the security incident has potential for media interest, the CNSI PM must be made aware with an unclassified description of pertinent facts of the potential risks of media interest. The CNSI PM will brief the issue for disposition by the AD, Security.
 - vi. Treasury SSO. If the incident involved NATO information or FGI, the Inquiry Official must report it in an unclassified manner to the Treasury's SSO via *SSO@treasury.gov*.
 - vii. Treasury OCIO. If the incident involves TSDN, then Treasury's OCIO must be notified on one of the three options: the unclassified side via *secureservicedesk@treasury.gov*, up to Secret CNSI via *secureservicedesk@tsdn.treasury.gov*, or unclassified phone (202) 927-1111.
 - viii. COR, CO. If the incident involved a contractor in a material way, the COR and CO must be notified. Upon completion of the Inquiry Report, the CNSI PM will submit notification of the incident and final inquiry report can be submitted to the DCSA.
- (3) Debriefing. In cases where unauthorized access to classified information has occurred, a debriefing may be called for. The CNSI PMs will coordinate the debriefing with IRS Personnel Security.

- a. If the unauthorized access was by an employee with the appropriate security clearance, but without need-to-know, the debriefing will only consist of ensuring the employee understands the information involved in the unauthorized disclosure is classified.
 - b. If the unauthorized access was by an uncleared employee or contractor, the employee or contractor will be advised of the responsibility to prevent further dissemination of the information, as well as the administrative sanctions and criminal penalties that might follow if he or she fails to do so. The debriefing shall emphasize why the protection of the information is important.
- (4) There are two types of security incidents, Security Infractions and Security Violations.
 - a. Security Infractions are incidents involving a deviation from governing security regulations that does not result in an unauthorized disclosure, loss, or compromise of CNSI, yet increases the probability of an actual security violation. Examples of security infractions include but are not limited to the following actions/inactions involving CNSI:
 - i. Not using security forms for safeguarding/accounting for CNSI, such as document cover sheets when removed from the security container, SF 700, 701, or 702, open/closed signs, as applicable.
 - ii. Not having an end-of-day check to ensure that CNSI work areas before close of business and/or assuming "someone else" will protect CNSI.
- (5) After Treasury OSP receives the Inquiry Report, follow on actions may be requested to include a Security Investigation or a Damage Assessment. In the case of a Security Investigation, Business Unit management will appoint a senior employee who was uninvolved with the incident and possesses a security clearance. In the event of a Damage Assessment, as IRS lacks OCA Treasury would appoint the employee responsible for its conduct.

10.9.1.15
(11-06-2023)

Self-Assessments

- (1) Periodicity
 - a. 32 CFR 2001, TD P 15-71 and this IRM prescribe the annual self-assessment of the CNSI programs be conducted, at minimum, annually.
- (2) Frequency
 - a. The CNSI PM will disperse the lines of inquiry across the first three quarters of each FY. The Classified Document Custodians will have the entirety of the quarter to conduct that portion of the self-assessment which will split the workload of the annual self-assessment program.
 - b. The fourth quarter of the FY will be dedicated to the completion of the SF 311 response in the timelines specified by Treasury.
- (3) Coverage
 - a. Over the course of each FY, each of the following areas will be reviewed in its entirety.
 - i. Management and Oversight. Performed by CNSI PMs.

1. Reviewing relevant security directives and instructions to ensure compliance and updates that correct system findings or security incidents,
2. Reviewing field submissions to ensure self-assessments are being conducted with integrity and monitor findings, corrective actions and trends,
3. Evaluating the methodology the Classified Document Custodians use in their performance of their self-assessments, as well as the relevant security policies.

- ii. Derivative Classification. Performed by Classified Document Custodians; CNSI PMs reviewing only as it pertains to ensuring self-assessments done by Classified Document Custodians are being conducted with integrity.
- iii. Declassification. Performed by Classified Document Custodians; CNSI PMs reviewing only as it pertains to ensuring self-assessments done by Classified Document Custodians are being conducted with integrity.
- iv. Safeguarding. Performed by Classified Document Custodians; CNSI PMs reviewing only as it pertains to ensuring self-assessments done by Classified Document Custodians are being conducted with integrity.
- v. Security Incidents. Performed by Classified Document Custodians; CNSI PMs reviewing only as it pertains to ensuring self-assessments done by Classified Document Custodians are being conducted with integrity.
- vi. Security Education and Training. Performed by CNSI PMs.

(4) Process

a. Design

- i. The CNSI PMs will create lines of inquiry, discreet, assessable elements, from this IRM.
 - ii. The lines of inquiry will be organized into three, logical portions or “banks”, ensuring that all lines of inquiry are covered once per FY.
1. In addition to all lines of inquiry being covered in a FY, every security container under a Classified Document Custodian must be involved in some portion of that quarter’s assessment.
- iii. The Classified Document Custodians will be given one of the three banks of lines of inquiry, the same one across the Classified Document Custodians, no later than the 5th business day of the quarter in each of the first three quarters of a FY. The lines of inquiry will be in an editable spreadsheet.
 - iv. Classified Document Custodians will be offered training by the CNSI PMs on that quarter’s bank of lines of inquiry at the start of each quarter. Multiple sessions will be offered to ensure maximum opportunities for attendance. CNSI PMs will remain available throughout the quarterly cycle to discuss issues or answer questions in an unclassified manner.
 - v. Classified Document Custodians will have the entirety of the quarter in which to complete the self-assessment, with the results being reflected on the lines of inquiry spreadsheet. The spreadsheet must be returned to the CNSI PMs by the end of the first week of the next quarter (e.g., the assessment period is October through December, results would be due by the end of the first week in January).

vi. If a finding is discovered during the self-assessment, see the Resolution of Findings subsection below.

vii. After the accumulation of the results for the first three quarters of the FY, the CNSI PMs will perform an analysis across the complex to determine best practices, gaps, and areas requiring policy.

b. Embassies and Consulates

i. Security containers used by CI personnel working at Embassies or Consulates are maintained and inspected physically by the Department of State's Regional Security Office.

ii. CI personnel are responsible for the inspection of the markings of the documents stored within the container.

iii. CI personnel at Embassies or Consulates will not be surveyed in person by the CNSI PMs or other authorized holder in the U.S.

c. CNSI PM Analysis

i. Management and Oversight Portion of the lines of inquiry. CNSI PMs will perform the applicable portion of management and oversight lines of inquiry concerning the overall program. The applicable portions will constitute the review of the following for compliance with National, Treasury and IRS policies: IRM and required training, the conduct of security incidents inquiries, required appointments, the rating clearance holders with the CNSI critical element at the end of each rating period, etc.

ii. Independent Assessments. CNSI PMs will perform independent assessments of Classified Document Custodians to ensure the integrity of the self-assessment process.

1. Facilities within local commuting distance (50-mile radius) will be inspected annually.

2. Facilities frequently storing CNSI outside of the local commuting distance will be inspected every two years. The preferred method of assessment will be in person, as travel funding allows and is considered 'reasonable' by FMSS. Virtual assessments will be conducted when in-person assessment are not reasonable as determined by FMSS.

a. "Frequently" is defined as 30 calendar days, consecutive or non-consecutive, per year.

b. An in-person self-assessment will be considered "reasonable" based on, at minimum, a determination of how many security containers exist in a location, approximations on how much CNSI is stored in said container(s) (e.g., 1 document vs. 35), frequency of storage, if other CNSI equipment (e.g., copiers, TSDN, etc.) is stored, the last time an in-person assessment was completed, etc. CNSI PMs will compile this data and FMSS management will make a final decision as to which facilities will be an in-person assessment based on funding.

3. Facilities infrequently storing CNSI outside of commuting distance will be inspected virtually every two years.

iii. Consolidation of Responses. Upon receipt of the prior FY's self-assessment results, the CNSI PMs will consolidate the entirety of the data received to:

1. Track non-compliance and deviations with CNSI program requirements.
2. Track Corrective Actions Plans being implemented on a facility level by the business units in order to determine whether corrective actions need to be implemented on a programmatic level.
3. Perform trend analysis to detail the weaknesses within the program for future training opportunities and potential IRM 10.9.1 updates,
4. Review the data for best practices that could be applied,
5. Present the results of the analysis to the Chief, Protection Management, by the end of August each FY.

d. Resolution of Findings

- i. Findings are defined as non-compliance with National, Treasury, or IRS policy. When a non-compliance occurs, the Classified Document Custodian must institute a corrective action plan to remedy the non-compliance to a compliant status.
- ii. The corrective action plan must be unclassified and contain: a summary of the issue, a remedy, a timeline for the corrective actions to be complete. The goal of remedies is to prevent recurrence of the finding and can include, but is not limited to:

1. Training personnel,
2. Correcting the issue on the spot,
3. Instituting controls to prevent recurrence,
4. Physical measures (these must be coordinated **prior to institution** with the CNSI PMs and local SSC to ensure compliance with requirements).

iii. The corrective action plan will be documented and sent to the CNSI PMs for tracking.

iv. If a trend of findings appears, the CNSI PMs will create policy to address the issue on a programmatic level.

(5) External Reporting

- a. External reporting to the Treasury SAO is completed via the SF 311 annually per Treasury's specified timeline, but no later than October 15 annually.
- b. CNSI PMs will request the information required of the Business Units for completion of the SF 311 to the CI Security Specialist and directly to personnel holding CNSI in other Business Units. The aggregate data from the self-assessments must be used as applicable in the response to the CNSI PMs.
- c. Compilation of all responses will be completed by the CNSI PMs and sent to the SAO for signature and transmission to Treasury.

