



1. **PURPOSE:** This Management Directive (MD) establishes the Transportation Security Administration (TSA) Information Security (INFOSEC) Program and provides policy, assigns responsibility and implements Executive Order 12958 “Classified National Security Information” as amended by Executive Order 13292 and its implementing directive 32 C.F.R. Part 2001.
2. **SCOPE:** This Directive applies to all TSA personnel and contractor personnel using Classified National Security Information and/or participating in classified activities impacting national security.
3. **AUTHORITIES:**
  - A. Executive Order 12958, Classified National Security Information dated April 20, 1995, as amended by Executive Order 13292, dated March 28, 2003.
  - B. 32 C.F.R. Part 2001, Classified National Security Information Directive No. 1.
  - C. 6 C.F.R. Part 7, DHS “Classified National Security Information.”
  - D. Department of Homeland Security (DHS) Delegation Number 8100.1, “Delegation of Original and Derivative Classification Authority.”
4. **DEFINITIONS:**
  - A. Access: The ability or opportunity to gain knowledge of classified information.
  - B. Classification: The act or process by which information is determined to be classified information.
  - C. Classification Guide: A documentary form of classification guidance issued by an original classification authority 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.
  - D. Classified National Security Information: Information that has been determined pursuant to Executive Order 12958, as amended, and its implementing directive, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.
  - E. Classified Security Custodian (CSC): An individual charged with responsibility for safeguarding or accounting for classified information. The CSC must have a security clearance equal to or greater than the highest level of classified information to which he/she is responsible for maintaining.

- F. Compromise: The disclosure of classified information to persons not authorized access to it.
- G. 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 applies to the source information. Derivative classification includes the classification of information based on the classification guidance. The duplication or reproduction of existing classified information is not derivative classification.
- H. Document: Any recorded information, regardless of the nature of the medium or the method or circumstances of recording.
- I. Industrial Security: That portion of information security that is concerned with the protection of classified information in the hands of U.S. industry as per Executive Order 12829, National Industrial Security Program.
- J. Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.
- K. Integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.
- L. National Security: The national defense or foreign relations of the United States.
- M. Need-to-know: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- N. Network: A system of two or more computers that can exchange data or information.
- O. Original Classification: An initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.
- P. Original Classification Authority (OCA): Means an individual authorized in writing, either by the President, or by agency heads or other officials designed by the President, to classify information in the first instance.
- Q. Security Control Point (SCP): The headquarters or field organizational element that is responsible for providing security services to a particular activity. The SCP at TSA Headquarters maintains the Classified Processing Center (CPC).
- R. Telecommunications: The preparation, transmission, or communication of information by an electronic means.

- S. Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.
- T. Violation: (Security violation) failure to comply with the policy and procedures that reasonably could result in the loss or compromise of classified information.
  - (1) Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
  - (2) Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directive; or
  - (3) Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirement of E.O. 12958.

**5. RESPONSIBILITIES:**

- A. The Secretary, Department of Homeland Security, has been delegated by the President as an original classification authority (OCA) with authority to classify eligible information up to and including TOP SECRET. The Secretary has further delegated to the Administrator of TSA the authority to originally classify information at the TOP SECRET level and below per DHS Delegation Number 8100.1.
- B. The Administrator has overall responsibility for the TSA classified national security information program. Upon recommendation by the Administrator, the Secretary will issue delegation of authority to the Chief Security Officer (CSO) and Chief Operating Officer (COO) to exercise authority in connection with the classification of national security information at the "SECRET" level. Delegation of Authority adheres to the office and may be exercised by a person acting in that capacity. In discharging this responsibility, the CSO coordinates with other TSA offices and services in the development of policies and procedures for safeguarding, controlling, and accounting for classified national security information agency-wide.
- C. The Office of Security is responsible for implementing policies and procedures relating to the TSA INFOSEC Program. The INFOSEC Program Manager will provide TSA-wide guidance and assistance in INFOSEC matters.
- D. Assistant Administrators and Office Directors shall:
  - (1) Support the INFOSEC Program in accordance with the provisions of Paragraph 6.A of this Directive and accommodate INFOSEC training for employees.
  - (2) Identify an employee in their respective areas of responsibility to serve as the INFOSEC Classified Security Custodian (CSC). The CSC will perform INFOSEC related duties and will be the focal point for INFOSEC matters and act as a liaison with the headquarters INFOSEC Program office.

- (3) Coordinate with the Credentialing Program Office to verify that the security clearance of the designated individual assuming CSC-related duties is current and equal to or greater than the highest level of classified information to which the CSC will require access.
- (4) Develop Classification Guides in accordance with procedures in the DHS “Handbook for Writing Security Classification Guides.” Program offices with particular areas in which a classification guide is required must have subject matter experts prepare the guide and coordinate it with the Chief Counsel, the Office of Security, and other impacted offices.

E. The TSA INFOSEC Program Manager shall:

- (1) Have management and auspices over the TSA Security Control Point.
- (2) Develop INFOSEC policies, procedures, and planning guidance.
- (3) Establish and chair a TSA INFOSEC working group to provide a forum to discuss generic and specific INFOSEC issues.
- (4) Establish and chair a TSA Classification Guide Working Group to facilitate the approval process for all Classification Guides.
- (5) Coordinate mutual support between Associate Administrators and other departments and agencies, as requested.
- (6) Provide INFOSEC planning, support, advice and training for TSA Headquarters and field personnel.
- (7) Support INFOSEC programs and efforts by other government departments and agencies, as requested.
- (8) Delegate authority to plan, direct and implement INFOSEC issues and matters, as appropriate, to Associate Administrators and staff elements.

F. The TSA Headquarters (HQ) Security Control Point Custodian shall:

- (1) Assign document control numbers to each new item of TOP SECRET and SECRET material received by an office and maintain accountability records for that information. Ensure that all classified documents are appropriately marked.
- (2) Verify the clearance status of recipients of incoming classified information and ensure that appropriate safeguards are provided for transferring control of the information.
- (3) Receive all incoming registered and certified mail addressed “Security Control Officer” and inspect it before opening to detect any evidence of tampering or dangerous materials. After opening, match the actual contents of the package with the enclosed receipt.
- (4) Sign and return to sender receipts for classified transmittals.

- (5) Ensure the appropriate secure methods of transmission are selected for classified material in accordance with the requirements of E.O. 12958, as amended, and its implementing directive.
  - (6) Ensure receipts are obtained for TOP SECRET and SECRET material mailed or faxed from the TSA.
  - (7) Destroy classified information or arrange for its destruction in accordance with the requirements of E.O. 12958, as amended, and its implementing directive.
  - (8) Conduct or cause to be conducted an annual audit and inventory of all TOP SECRET and SECRET documents.
- G. Classified Security Custodians (CSC) control and disseminate all classified information received. As the focal point for controlling and safeguarding classified national security information for their designated areas, the CSC:
- (1) Is responsible for all classified material contained in the GSA approved container and controls access to the container.
  - (2) Ensures that all personnel, commensurate with their positions and security clearances, are aware of the procedures for handling classified information.
  - (3) Supports the requirements for an annual review and evaluation of INFOSEC procedures to assist in the improvement of the INFOSEC Program.
  - (4) Recommends to the TSA's INFOSEC Program Manager changes to policies, procedures, or practices to the TSA INFOSEC Program.
  - (5) At the direction of the TSA HQ Security Control Point (SCP) custodian, conduct an annual audit and inventory of all TOP SECRET and SECRET documents.
- H. TSA Employees and personnel detailed to TSA with authorized access to classified information are responsible for:
- (1) Knowledge of Executive Order 12958, as amended, and its implementing Directive 32 C.F.R. Part 2001.
  - (2) Knowledge of prescribed classification markings and the importance of having classified information fully and properly marked.
  - (3) Apprising any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) to immediately report the circumstance to the Office of Security, INFOSEC Program Manager.

- (4) Protecting classified national security information from persons without authorized access, to include securing it in approved containers or facilities whenever it is not under the direct control of an authorized person.
  - (5) Ensuring that classified information is not communicated over unsecured voice or data circuits, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.
  - (6) Ensuring that classified information is stored only under conditions designed to deter and detect unauthorized access to the information. Storage at overseas locations shall be at U.S. Government controlled facilities unless otherwise stipulated in treaties or international agreements.
  - (7) Contacting the CSC for assistance to ensure that reproduction of classified material is accomplished by authorized persons knowledgeable of the procedures for copying classified information.
  - (8) Ensuring that classified information is transmitted and received in an authorized manner that ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and that provides a method that assures timely delivery to the intended recipient. Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information in accordance with this Management Directive.
  - (9) Ensuring that classified information identified for destruction is destroyed completely to preclude recognition or reconstruction in accordance with methods prescribed by the Executive Order 12958, as amended, and its implementing directive. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Contact the TSA HQ SCP for a list of National Security Agency (NSA) approved shredders.
  - (10) Ensuring that all persons receiving classified national security information from outside sources contact the CSC for classified document control and dissemination issues.
  - (11) Ensuring that all individuals transmitting classified national security information by mail contact the CSC for document control and dissemination assistance.
- I. TSA contractor personnel are responsible for:
- (1) Complying with the provisions of this directive and applicable provisions of Executive Order 12829, National Industrial Security Program dated January 6, 1993, and the National Industrial Security Program Operating Manual dated January 1995.
  - (2) Having knowledge of prescribed requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information.

- (3) Controlling authorized disclosure of classified information released by TSA and its contractors.

## **6. POLICY AND PROCEDURES:**

### **A. POLICY**

- (1) It is TSA's policy to ensure that TSA information relating to the national security is uniformly classified, protected, and declassified pursuant to all official classified information security rules.
- (2) It is TSA policy to ensure that the public has access to as much TSA information as possible, consistent with the need to protect the national security of the United States.
- (3) In accordance with Executive Order 12958, as amended, Classified National Security Information, TSA has implemented a viable and effective INFOSEC Program. TSA will also cooperate with other departments, agencies, and institutions to minimize damage to national security when INFOSEC issues arise.
- (4) In accordance with Executive Order 12958, as amended, Classified National Security Information, TSA will address INFOSEC from the beginning of all planning, programming and budgeting actions and will address INFOSEC during all operations and activities.
- (5) INFOSEC awareness will be incorporated into TSA training programs. TSA personnel, commensurate with their positions and security clearances, will be briefed on Classified National Security Information issues, policies, and procedures.
- (6) Requests to waive requirements as cited in this Management Directive will be submitted through the Chief Security Officer, attention: INFOSEC Program Manager in the Office of Security. Waiver requests must include sufficient justification to support the request and identification of countermeasures that will be implemented to mitigate deficiencies. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

### **B. PROCEDURES**

- (1) The TSA HQ Security Control Point (SCP) is where classified information is stored, processed, handled, disseminated, reproduced, and destroyed. Unless specifically authorized in writing by the Chief Security Officer, all classified information processing at TSA Headquarters, with the exception of information processed by the Transportation Security Intelligence Service (TSIS) shall be done in the SCP.
  - (a) The TSA HQ SCP is equipped with stand-alone computers; printer; GSA-approved security container; secure telecommunications equipment (STE); NSA-approved shredder; and a classified copier machine.

- (b) Computers connected to the local area network (LAN) are not approved for processing classified information.
  - (c) Reproduction of TOP SECRET, SECRET, and CONFIDENTIAL documents is strictly regulated. TOP SECRET documents shall not be reproduced without the authorization of the INFOSEC Program Manager.
- (2) Transmission of TOP SECRET, SECRET, and CONFIDENTIAL classified material:
- (a) Requires possession of a courier card/letter issued by the TSA HQ INFOSEC Manager.
  - (b) Requires preparation and retention of an itemized list of the classified material by the CSC.
  - (c) From one building to another, which requires travel on a public street shall be double wrapped and sealed in opaque envelopes and fully addressed. A locked briefcase may be used as the outer wrapper.
  - (d) Within the same building shall require the courier to have a cover sheet affixed to the document to prevent unauthorized disclosure.
  - (e) Via telecommunications shall be accomplished using secure telecommunications equipment (STE) and procedures. Classified information must not be discussed over non-secure (unencrypted) telephone or transmitted to/from non-secure facsimile machines; or transmitted to/from non-secure computers.
  - (f) All incoming and outgoing SECRET or above material that has not been assigned a control number shall be coordinated with the TSA HQ SCP or the CSC in the field.
- (3) Destruction of TOP SECRET, SECRET, and CONFIDENTIAL classified information material:
- (a) Shall be done in accordance with approved Records Disposition Schedules.
  - (b) Shall be brought to the CSC to be destroyed in an authorized manner by an approved destruction method when the information is no longer needed.
  - (c) Classified documents may be forwarded to the SCP for authorized destruction at any time.
  - (d) Questions concerning this process should be directed to the CSC or HQ SCP.
- (4) A security violation occurs when there is failure to comply with the policy and procedures, which reasonably could result in the loss or compromise of classified information. Examples of security violations include, but are not limited to, leaving a security container used for storage of classified materials open and unattended or transmitting classified information via unauthorized channels.

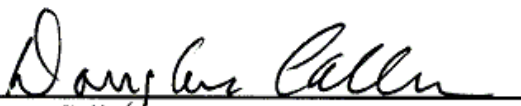


- (a) All security violations should be reported within 24 hours of the occurrence on the DHS Form 11000-11, Record of Security Violation (Appendix I) and forwarded to the SCP, ATTN: INFOSEC Program Manager.
- (b) Any TSA or contractor employee having knowledge of a violation of security regulations, or the lost, unauthorized disclosure, or actual or possible compromise of classified information shall immediately report the details to his or her immediate supervisor. The supervisor shall conduct an initial review to determine if a compromise occurred, and if appropriate, execute DHS Form 11000-11.
- (c) In determining the disciplinary action to be taken, the INFOSEC Manager will consider the overall assessment of the occurrence including the seriousness of the violation, the sensitivity of the information subjected to compromise, and evidence of disregard or continuing disregard of security regulations. At a minimum, the INFOSEC Manager will recommend to the employee's supervisor that the following penalties be imposed if security violations occur within a two-year period:
  - (i) First Violation: Letter of Warning advising of future penalties for additional violations;
  - (ii) Second Violation: Letter of Reprimand; and
  - (iii) Third and Future Violations: Adverse personnel action and/or revocation of security clearance.

**7. EFFECTIVE DATE AND IMPLEMENTATION:**

This directive is effective immediately upon signature.

**APPROVAL**

  
\_\_\_\_\_  
Douglas I. Callen  
Chief Security Officer

5/14/04  
Date

Filing Instructions: File with Office of Security Directives.  
Effective Date: May 14, 2004  
Review Date: May 14, 2005  
Distribution: TSA Assistant Administrators, Office Directors  
Point Of Contact: Office of Security, Denise Esquilin, 571-227-1602

APPENDIX I

DEPARTMENT OF HOMELAND SECURITY  
**RECORD OF SECURITY VIOLATION**

PART I (TO BE EXECUTED BY REPORTING OFFICIAL)				
VIOLATION DISCOVERED BY:	DATE:	TIME: AM <input type="checkbox"/>	HIGHEST CLASSIFICATION INVOLVED: Secret	
3:30 PM <input type="checkbox"/>				
BUILDING:	ROOM NUMBER:	OFFICE/DIVISION:	PHONE NUMBER:	STATION NUMBER:
SUBJECT OF REPORTED VIOLATION				
UNSECURED SECURITY CONTAINER	<input type="checkbox"/>	UNSECURED BARLOCK CABINET	<input type="checkbox"/>	UNSECURED VAULT/SECURE ROOM <input type="checkbox"/>
CLASSIFIED DOCUMENT(S) UNSECURED	<input type="checkbox"/>	CLASSIFIED WASTE IN TRASH RECEPTACLE	<input type="checkbox"/>	CLASSIFIED BURNBAG UNSECURED <input type="checkbox"/>
IMPROPER TRANSMISSION	<input type="checkbox"/>	CLASSIFIED COMSEC	<input type="checkbox"/>	OTHER (Use Narrative) <input type="checkbox"/>
SECURITY CONTAINER CHECK SHEET – Standard Form (SF) 702				
SF 702 displayed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Security Container/Cabinet Number: _____	
All columns used?	Yes <input type="checkbox"/>	No <input type="checkbox"/>		
OPEN/CLOSED sign?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Date of last SF 702 entry: _____	
NARRATIVE DESCRIPTION OF VIOLATION: <i>(Use Reverse if Necessary)</i>				
_____ <i>Name and Title of Reporting Official (Type or Print)</i>		_____ <i>Signature</i>		_____ <i>Date</i>
PART II (TO BE EXECUTED BY INDIVIDUAL RESPONSIBLE FOR VIOLATION)				
STATEMENT OF INDIVIDUAL RESPONSIBLE FOR VIOLATION: <i>(Use Reverse Side or Continuation Sheet, if Necessary)</i>				
_____ <i>Name of Individual Responsible (Type or Print)</i>		_____ <i>Signature</i>		_____ <i>Date</i>
PART III (TO BE EXECUTED BY INDIVIDUAL'S SUPERVISOR)				
ESTIMATED TIME INFORMATION WAS WITHOUT REQUIRED PROTECTION:			FROM:	TO:
EVALUATION OF POSSIBILITY OF COMPROMISE: <i>(Use Reverse Side if Necessary)</i>				
CORRECTIVE ACTION TO PREVENT RECURRENCE HAS BEEN INITIATED AS FOLLOWS: <i>(Use Reverse Side if Necessary)</i>				
_____ <i>Name of Individual Responsible (Type or Print)</i>		_____ <i>Signature</i>		_____ <i>Date</i>
FOR USE OF SECURITY OFFICE ONLY			VALID VIOLATION: YES <input type="checkbox"/> NO <input type="checkbox"/>	