Department of Homeland Security
Management Directives System
MD Number: 11056.1
Issue Date: 11/03/2006

SENSITIVE SECURITY INFORMATION (SSI)

I. Purpose

This Management Directive (MD) establishes the Department of Homeland Security (DHS) policy regarding the recognition, identification, and safeguarding of Sensitive Security Information (SSI).

II. Scope

This MD is applicable to all persons who are permanently or temporarily assigned, attached, detailed to, employed, or under contract with DHS.

III. Authorities

A. Department of Homeland Security Appropriations Act, 2007, Public Law 109-295

B. Department of Homeland Security Appropriations Act, 2006, Public Law 109-90

C. Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (2002), as amended

D. Aviation and Transportation Security Act, Public Law 107-71, 115 Stat. 597 (2001)

E. Maritime Transportation Security Act of 2002, Public Law 107-295, 116 Stat. 2064 (2002), as amended

F. 49 U.S.C. § 114(s), Nondisclosure of Security Activities

G. 49 C.F.R. Part 1520, Protection of Sensitive Security Information, May 18, 2004

H. DHS Management Directive 0010.2, Management Directives System

I. DHS Management Directive 0460.1, Freedom of Information Act Compliance

J. DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information

IV. Definitions

A. ***Access***: The ability or opportunity to gain knowledge of information.

B. ***Classified National Security Information ("Classified Information")***: Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor or successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

C. ***Component***: All entities that report directly to the Office of the Secretary, which is made up of the Secretary and his or her staff, Deputy Secretary and his or her staff, Chief of Staff and his or her staff, and Counselors and his or her staff, in accordance with the DHS Management Directive 0010.2, Management Directives System.

D. ***Designate/Designation***: As used in this MD and as it applies to the identification of SSI, the original determination made by the Secretary, the Assistant Secretary for the Transportation Security Administration (TSA), or the Director of the TSA SSI Office, pursuant to 49 C.F.R. § 1520.5(b)(16), that information not otherwise categorized as SSI under 49 C.F.R. § 1520.5(b)(1) through (15), warrants designation as SSI. It also includes a determination to protect detailed information about screening locations in accordance with 49 C.F.R. § 1520.5(b)(9)(iii).

E. ***DHS Covered Person***: As used in this MD, a "DHS covered person" is an individual or entity that (1) falls within the definition of "covered person" set out at 49 C.F.R. Section 1520.7; and (2) is permanently or temporarily assigned, attached, detailed to, employed, or under contract with DHS (pursuant to Section II above).

F. ***For Official Use Only (FOUO)***: Unclassified information of a sensitive nature, as defined in DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. For purposes of this MD, SSI is not considered as FOUO information, since it is governed by statute and regulation.

G. ***Lawful Request***: Any formal request for information or records that is made under the auspices of existing statute or regulation, for example, information or records requested under the Freedom of Information Act (FOIA).

H. ***Mark/Marking***: As used in this MD, the application of the SSI protective marking and distribution limitation statement to records containing SSI, as required by 49 C.F.R. § 1520.13, this MD, and other implementing guidance approved by the TSA SSI Office.

I. ***Need-to-know***: As used in this MD, an individual or entity has a Need-to-know SSI when they require access to specific SSI to perform a lawful and authorized governmental function related to transportation security, as determined by an authorized holder of SSI in accordance with 49 C.F.R. § 1520.11.

J. ***Record***: As defined in 49 C.F.R. § 1520.3, includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format, including any draft, proposed or recommended change to any record.

K. ***Redact***: As used in this MD, the permanent obscuring of SSI from a record to permit appropriate release to non-covered persons (e.g., individuals not within the definition provided at 49 C.F.R. Section 1520.7).

L. ***Sensitive Security Information (SSI)***: As defined in 49 C.F.R. Section 1520.5, information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would (1) constitute an unwarranted invasion of privacy (including , but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

M. ***SSI Coordinator***: An official within an office who has been delegated responsibility for administration, coordination, and oversight of SSI within the applicable office. SSI Coordinators shall be appointed by supervisors or managers of offices that access and/or generate SSI. Supervisors or managers shall serve as SSI Coordinators for their respective office until appointment of an SSI Coordinator.

N. ***SSI Program Manager***: An official, appointed pursuant to Sections V.B, V.D, or V.G of this MD, to oversee the administration and management of SSI within a Component or directorate.

V. Responsibilities

A. The DHS Chief Security Officer shall:

1. Promulgate Department-wide policy governing the recognition, identification, and safeguarding of SSI.

2. Coordinate with the Director of the TSA SSI Office the development of any security classification guide that may identify information that requires protection as SSI.

3. Serve as a permanent member and provide technical advice and assistance to the DHS SSI Oversight Committee. Such appointment may be delegated.

B. The Assistant Secretary for the Transportation Security Administration shall:

1. Serve as the authority for implementation, management, and oversight of SSI, pursuant to 49 U.S.C. Section 114(s).

2. Coordinate with other government agencies, such as the Department of Transportation, to ensure effective management and practical application of SSI, and consistent and appropriate application and use of SSI.

3. Administer implementation, management, and oversight of SSI within TSA, and to the extent defined within this MD, within DHS, through appointment of a senior official to serve as the Director of the TSA SSI Office.

4. Shall review and approve or deny requests to designate, pursuant to 49 C.F.R. Section 1520.5(b)(16), new types of SSI that would be detrimental to the security of transportation, if publicly disclosed, where the information is not otherwise protected as SSI under 49 C.F.R. Section 1520.5(b)(1) through (15), and to review and approve or deny requests to protect information as SSI pursuant to 49 C.F.R. Section 1520.5(b)(9)(iii).

5. Ensure that periodic and random reviews of TSA are conducted for effective management and practical application, and consistent and appropriate application and use of SSI, and notify the DHS Office of Security about these reviews. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding. The DHS Office of Security may also conduct SSI reviews of TSA, as it deems appropriate.

6. Ensure appointment of at least one employee in each TSA office that generates/accesses SSI to serve as SSI Coordinator, and grant each SSI Coordinator authority to make determinations on behalf of DHS that records generated by that office are appropriately marked SSI.

7. Ensure that when a lawful request to publicly release a record containing information determined to be SSI is received, the record is reviewed in a timely manner to determine whether any information contained in the record meets the criteria for continued SSI protection under applicable law and regulation. Portions that no longer require SSI protection shall be released subject to applicable laws and regulations, including sections 552 and 552a of Title 5, United States Code.

8. Ensure that SSI information that is three years old or older shall be released upon lawful request unless the information meets the standards cited in Section VI.E of this MD.

C. Director of the TSA SSI Office shall:

1. Serve as the SSI Program Manager for TSA pursuant to Section V.E below.

2. Assist in the promulgation of regulations and procedural guidance for the implementation and management of SSI.

3. Serve as the approval authority for publication of Component-level SSI guidance and procedures.

4. Issue or approve detailed SSI identification guidance, with common and extensive examples of SSI cited under 49 C.F.R. Section 1520.5(b)(1) through (16).

5. To the extent possible, ensure that all information topics that are SSI are included in SSI identification guidance, as identified in V.C.3, above, and monitor guides to ensure they are current.

6. Establish, provide guidance for, and approve training programs for DHS persons who access or generate SSI records.

7. Establish and implement specialized training programs for DHS officials designated as SSI Program Managers or with designation authority.

8. In coordination with the DHS Office of Security, establish, provide guidance for, and approve processes and programs for the audit, oversight, and inspection of the management and practical application of SSI, to include random reviews of SSI records for consistent and appropriate application and use of SSI within DHS.

9. Establish, implement, and serve as Chair of the DHS SSI Oversight Committee, as discussed in Section V.H below.

10. Conduct periodic reviews and self-inspections of TSA for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G of this MD.

11. Ensure appointment of the appropriate number of TSA office-level SSI Coordinators in order to effectively implement and manage SSI recognition, identification, and safeguarding within the respective TSA offices.

12. Maintain an up-to-date record of all TSA SSI Coordinators.

D. The Under Secretary for Science and Technology, the Under Secretary for Preparedness, the Assistant Secretary for Intelligence and Analysis, the Assistant Secretary for Immigration and Customs Enforcement (ICE), the Commissioner for U.S. Customs and Border Protection (CBP), and the Commandant, U.S. Coast Guard (USCG) shall:

1. Administer implementation and management of SSI within the respective Components through written appointment of a Government official to serve as the SSI Program Manager for each respective Component. The appointed SSI Program Manager shall represent their respective Component on the DHS SSI Oversight Committee. Copies of the appointment record shall be forwarded to the Director of the TSA SSI Office and the DHS Chief Security Officer.

2. Ensure appointment of at least one employee in each office that generates or accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations that records generated by this Component are appropriately marked SSI.

3. Ensure that periodic and random reviews of the respective Components are conducted for effective management and practical application, and consistent and appropriate application and use of SSI, and notify the DHS Office of Security about these reviews. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding. The DHS Office of Security may also conduct SSI reviews of these Components, as it deems appropriate.

4. Where necessary, develop and implement supplemental internal Component SSI procedures and guidance specific to the management and administration of SSI within the Component. Such supplemental procedures and guidance shall be approved by the Director of the TSA SSI Office, in coordination with the DHS Office of Security prior to implementation.

5. Ensure that when a lawful request to publicly release a record containing information determined to be SSI is received, the record is reviewed in a timely manner to determine whether any information contained in the record meets the criteria for continued SSI protection under applicable law and regulation. Portions that no longer require SSI protection shall be released subject to applicable laws and regulations, including sections 552 and 552a of Title 5, United States Code. Any records containing SSI originating from another DHS Component shall be referred to the appropriate Component for review and response. Any information originally designated as SSI pursuant to 49 C.F.R. Sections 1520.5(b)(9)(iii) or 1520.5(b)(16) shall be referred to the Assistant Secretary for the Transportation Security Administration.

E. SSI Program Manager shall:

1. Serve as the Component official responsible for management, implementation, and oversight of SSI within the Component.

2. Represent the Component to the DHS SSI Oversight Committee.

3. Conduct self-inspections of the respective Component for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G of this MD.

4. Ensure appointment of an appropriate number of office-level SSI Coordinators in order to effectively implement and manage SSI within the respective offices.

5. Maintain an up-to-date record of all Component SSI Coordinators and provide a copy to the Director of the TSA SSI Office on a semi-annual basis (January 15 and July 15 of every year).

6. Develop Component-specific SSI identification and procedural guidance as necessary to implement and manage SSI within the respective Components.

F. SSI Coordinator shall:

1. Facilitate the administration and oversight of SSI within the applicable office.

2. Assist office personnel in the appropriate use and application of SSI and make determinations that records generated by that office are appropriately marked SSI.

3. Conduct self-inspections of the respective office for effective management and practical application of SSI, and consistent and appropriate application and use of SSI. Self-inspections shall be conducted in accordance with Section VI.G of this MD.

4. Ensure training of office personnel who access and/or generate SSI.

5. Keep abreast of SSI policies and procedures and maintain liaison with the Component SSI Program Manager.

G. Heads of Other DHS Components (not previously referenced above) shall:

1. Ensure compliance with the standards for recognition, identification, and safeguarding of SSI as cited in 49 C.F.R. Part 1520, this MD and other MDs.

2. Where appropriate, based on the extent of contact and use of SSI, appoint a Government official to serve as the Component SSI Program Manager. The appointee shall represent the Component on the DHS SSI Oversight Committee and fulfill additional responsibilities as cited in Section V.E above.

3. Where appropriate, conduct periodic reviews of the respective Component for effective management and practical application of SSI, and consistent and appropriate application and use of SSI, and notify the DHS Office of Security about these reviews. The DHS Office of Security may also conduct reviews of these Components, as it deems appropriate.

4. Where appropriate, appoint at least one employee in each office that generates or accesses SSI to serve as SSI Coordinator, and grant each Coordinator authority to make determinations on behalf of DHS that records generated by this Component are appropriately marked SSI.

H. DHS SSI Oversight Committee shall:

1. Be chaired by the Director of the TSA SSI Office, with membership

consisting of the DHS Chief Security Officer (pursuant to Section V.A.3) and Component SSI Program Managers appointed pursuant to this MD.

2. Establish a committee charter that outlines the authority, scope, and responsibilities of the committee. Development of the charter shall be a coordinated effort of the membership and approved by the Assistant Secretary for the Transportation Security Administration.

3. Be used as a forum for the discussion of policies and procedures related to the implementation, management, and oversight of SSI within DHS and an exchange of information related to lessons learned and best practices.

I. DHS employees, contractors, consultants, and other DHS Covered Persons to whom access to SSI is granted shall:

1. Be aware of and comply with the recognition, identification, and safeguarding requirements for SSI as outlined in this MD, 49 C.F.R. Part 1520, and approved implementing regulations, directives, procedures, and guidance.

2. Be aware that divulging SSI without proper authority could result in enforcement or corrective action.

3. Participate in training sessions presented to communicate the requirements for recognizing, identifying, and safeguarding SSI.

VI. Policy

A. General

1. TSA, through its SSI Office, shall issue, provide, and/or approve appropriate regulations, directives, procedures, and other guidance pertinent to the effective management and practical application, and consistent and appropriate application and use of SSI.

2. MDs and guidance issued by other Components for implementation within their respective Components shall be coordinated through and approved by the TSA SSI Office prior to publication.

3. SSI shall only be used to protect information that would be an unwarranted invasion of privacy; reveal trade secrets or privileged or confidential information obtained from any person; or detrimental to the security of transportation, if publicly disclosed. It is not intended to be used to conceal Government mismanagement or other circumstances embarrassing to a Government agency. Pursuant to 49 U.S.C § 114(s)(2) and 49 C.F.R. § 1520.15(c), SSI may not be withheld from authorized committees of Congress. Further, pursuant to 49 C.F.R. § 1520.11(b)(1), SSI must be shared with members of Congress, their staffs, DHS or TSA management and legal counsel, the Comptroller General (Government Accountability Office), the TSA Office of Internal Affairs and Program Review, the DHS Office of Inspector General, Freedom of Information Act (FOIA) offices, any other official Government investigative body, or any other Federal employee if access to the information is necessary in the performance of the employee's official duties.

4. Under 49 C.F.R. § 1520.15(a), information properly marked as SSI is exempt from release under FOIA. Each Component is responsible for review and validation of SSI markings in their FOIA review process. Each Component with a FOIA office shall establish FOIA SSI review policy and procedures and submit them to the TSA SSI Office for approval. In accordance with 49 C.F.R. § 1520.15(b), to the extent practicable, redaction of the SSI shall be used to allow for the maximum release of non-SSI that is not otherwise exempt under FOIA. SSI that is three years old or older shall be released upon a lawful request unless the information meets the standards cited in Section VI.E of this MD.

5. This MD becomes effective upon the date of publication. Revised guidance issued pursuant to this MD shall be coordinated with and approved by the TSA SSI Office prior to publication.

B. SSI Guidance

1. The SSI regulation, 49 C.F.R. § 1520.5(b) provides fifteen categories [49 C.F.R. § 1520.5(b)(1) through 49 C.F.R. §1520.5(b)(15)] of information that have been determined to be SSI. The SSI regulation also has one category, 49 C.F.R. § 1520.5(b)(16), and one part of one category, 49 CFR §1520.5(b)(9)(iii), which requires an authorized official to designate as SSI.

2. The TSA SSI Office shall issue and update, as needed, guidance that significantly expands upon the descriptions for categories of information that must be marked and protected as SSI. Such guidance shall provide DHS Covered Persons with an accurate source for recognizing when and when not to apply the SSI marking. It will also include common and extensive examples of the individual categories of SSI cited under 49 C.F.R. Section 1520.5(1) through (16). This guidance, when used in conjunction with the SSI regulation, serves as the primary authority and source for the recognition and marking of SSI by DHS Covered Persons.

3. DHS Components shall issue and update Component-specific SSI guidance, as needed. Component-specific guidance shall be approved by the TSA SSI Office.

C. Original Designation of Information as SSI

1. The Secretary, the Assistant Secretary for the Transportation Security Administration, and the Director of the TSA SSI Office are authorized to designate information as SSI, pursuant to 49 C.F.R. § 1520.5(b)(16), which is not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15). This designation authority also includes a determination to protect detailed information about screening locations in accordance with 49 C.F.R. § 1520.5(b)(9)(iii). No other officials shall have the authority to designate information as SSI that is not otherwise covered under 49 CFR §1520.5(b)(1) through (15).

2. If information is identified or developed that would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged of confidential information obtained from any person, or be detrimental to the security of transportation if publicly disclosed, but it is not otherwise categorized as SSI under 49 C.F.R. § 1520.5(b)(1) through (15), it shall be transmitted through the applicable Component SSI Program Manager to the Director of the TSA SSI Office, for review and determination as to whether or not the information warrants protection as SSI. Such information shall be marked and protected as SSI on an interim basis in accordance with policies and procedures issued or approved by the TSA SSI Office, pending a final assessment by the Director of the TSA SSI Office.

3. A record shall be maintained of each original SSI designation made. The record shall include the date, title or subject of the document, and a detailed synopsis of the information. A copy of the record and the information to be protected shall be transmitted to the TSA SSI Office within thirty (30) days following designation. Whenever possible, to maintain consistency, such designations should be done in consultation with the TSA SSI Office prior to designation.

4. Information designated as SSI shall be marked in accordance with 49 C.F.R. § 1520.13. To the extent practicable, the front page, title page, and/or the first page shall include the notation *"Designated SSI Pursuant to 49 C.F.R. § 1520.5(b)(16),"* or*, "Designated SSI Pursuant to 49 C.F.R. § 1520.5(b)(9)(iii),"* as applicable. Where the official making the SSI designation is not otherwise evident, the additional notation *"Designated by (Name and Position of authorized official)"* shall be added.

5. Once information is properly designated as SSI under 1520.5(b)(9)(iii) or 1520.5(b)(16), the designation must be communicated to appropriate parties with a Need-to-know.

D. Marking SSI

1. A DHS Covered Person shall mark information as SSI if it meets the criteria for SSI as cited in 49 C.F.R. §1520.5(b) and implementing guidance. Where there is doubt as to the applicability of an SSI category, the information shall be marked as SSI on an interim basis and submitted to the applicable office SSI Coordinator or Component SSI Program Manager for final assessment. If the information is believed to warrant protection as SSI but is not governed by a category of information under 1520.5(b)(1) through (15), the SSI Program Manager shall refer the information as cited in VI.C.3 of this MD.

2. Information meeting the SSI criteria shall be marked in accordance with 49 C.F.R. § 1520.13. Additionally, the following markings shall be applied:

a. Subjects, titles, paragraphs, subparagraphs, charts, graphs, and similar portions (portion markings) need not be portion marked unless (1) the record contains other types of information that requires portion marking, e.g., classified information; or (2) the information is to be transmitted outside of DHS to Congress, and Congressional Committees. All SSI records submitted by DHS to Congress or Congressional Committees must be portion-marked. When used, such portion markings shall be reviewed by the Component SSI Program Manager prior to dissemination. The parenthetical abbreviation (SSI) shall be used.

b. Portion markings will be applied to unclassified portions of a record within a classified record that contain SSI. The parenthetical abbreviation (SSI) shall be used.

c. Based upon studying the feasibility of using portion markings for SSI, the DHS SSI Oversight Committee will issue its report regarding this issue by December 16, 2006, pursuant to the requirements of the Department of Homeland Security Appropriations Act, 2006, Public Law 109-90.

E. Duration of SSI and SSI Reviews

1. Information designated or appropriately marked as SSI will remain SSI unless determined releasable by the Assistant Secretary for the Transportation Security Administration, the Commandant of the USCG, the Director of the TSA SSI Office, or other authorized officials, in accordance with policies and procedures issued or approved by the TSA SSI Office.

2. SSI information that is three years old or older will be subject to release upon request, unless the DHS Office of Security, TSA SSI Office, or appropriate Component SSI Program Manager determines that one of the following conditions applies:

a. The information is incorporated in a current transportation security directive, security plan, contingency plan, or information circular.

b. The information contains current information in one of the following SSI categories: equipment or personnel performance specifications, vulnerability assessments, security inspection or investigative information, threat information, security measures, security screening information, security training materials, identifying information or designated transportation security personnel, critical aviation or maritime infrastructure asset information, systems security information, confidential business information, or research and development information.

c. The information is otherwise exempt from disclosure under applicable law.

d. If the SSI does not fall under a category cited in Section VI.E.2 of this MD, then the request for release may only be denied, in whole or in part, if the Secretary or the Assistant Secretary for the Transportation Security Administration, makes a written determination that identifies a rational reason why the information must remain SSI. Such written determination shall be provided to the party that made the request within twenty (20) business days after the determination has been made. Additionally, each written determination shall be provided to the Committees on Appropriations of the Senate and House of Representatives as part of the annual reporting requirement cited in Section VI.M of this MD.

3. Pursuant to 49 C.F.R. Section 1520.5(c), the Director of the TSA SSI Office shall coordinate with the USCG and the DHS SSI Oversight Committee to develop and implement a policy and procedures relating to the loss of an SSI designation from information that no longer meets the criteria set forth in 49 C.F.R. Section 1520.5(a).

4. In accordance with 49 C.F.R. § 1520.15(a) and (b), and Sections VI.A.5 and VI.E.2 above, Component SSI Program Managers or other authorized Component offices may review and redact SSI records upon requests for public release under the Freedom of Information Act (FOIA) in accordance with policies and procedures issued or approved by the Director of the TSA SSI Office.

5. Component offices may also redact SSI records in response to other requests, in accordance with this MD and policies and procedures issued or approved by the Director of the TSA SSI Office.

F. Challenging SSI

Any authorized holder of SSI who believes the information has been improperly or erroneously marked as SSI is encouraged to challenge the marking. Such challenges may be done either informally or formally.

1. Informal challenges may be made directly by the holder of the information to the person that applied the SSI marking who shall reevaluate the marking against the criteria cited in 49 C.F.R. § 1520.5(b)(1) through (15) and implementing guidance published or approved by the Director of the TSA SSI Office.

2. A formal challenge may be submitted, in writing, to the person that applied the SSI marking or to the applicable Component SSI Program Manager, the TSA SSI Office, the applicable office SSI Coordinator, or the DHS Office of Security. An appeal to the decision made by the recipient of the challenge may be filed with the Director of the TSA SSI Office. A further appeal to the decision made by the Director of the TSA SSI Office, may be made to the Assistant Secretary for the Transportation Security Administration. The decision of the Assistant Secretary for the Transportation Security Administration shall be final..

3. Individuals submitting a challenge shall not be subject to retribution for bringing such actions. Anonymity may be requested from any of the reviewers listed in Section VI.F.2 above, and the reviewers shall honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

G. Audits and Inspections

1. Nothing in this MD shall diminish the authority of the Office of Inspector General to conduct audits, inspections, or investigations, in accordance with the Inspector General Act of 1978, as amended, 5 USC App., and DHS Management Directive 0810.1.

2. The DHS Office of Security may conduct periodic oversight and compliance reviews of SSI within DHS, as it deems appropriate.

3. The Director of the TSA SSI Office, shall develop, issue, and approve policies, procedures, and guidance for the implementation and management of self-inspection programs for Components that access or generate SSI. The TSA SSI Office shall create, publish and approve appropriate guidance and checklists to facilitate the conduct of self-inspections by SSI Program Manager's and SSI Coordinators. The DHS Office of Security shall also provide a means to monitor and track self-inspection program implementation.

4. SSI Program Managers shall conduct a self-inspection of their applicable Component SSI program at least once every eighteen (18) months. The results of self-inspections conducted pursuant to this MD shall be reported to the TSA SSI Office within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner, and the SSI Program Manager or the TSA SSI Office will take remedial action as needed.

5. SSI Coordinators shall conduct a self-inspection of the applicable office SSI program at least once every twelve (12) months. The results of self-inspections conducted pursuant to this MD shall be reported to the applicable SSI Program Manager within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner, and the SSI Coordinator or the SSI Program Manager will take remedial action as needed.

6. Self-inspections shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

H. Sharing, Dissemination and Access

1. SSI shall not be disseminated in any manner (orally, electronically, visually, or in any other manner) to unauthorized personnel. The Assistant Secretary for the Transportation Security Administration may determine in writing that information which might otherwise be considered SSI may be released publicly in the interest of public safety or in furtherance of transportation security under 49 C.F.R. Section 1520.5(b). Under 49 C.F.R. Section 1520.15(e), the Assistant Secretary for the Transportation Security Administration, and under 49 C.F.R. Section 1520.9(a)(2), the Assistant Secretary for the Transportation Security Administration and the Commandant of the USCG, may also determine in writing that specific SSI may be released to non-covered persons (e.g., individuals not within the definition provided at 49 C.F.R. Section 1520.7), in accordance with policies and procedures issued or approved by the TSA SSI Office.

2. In addition to other requirements cited previously and in 49 C.F.R. Part 1520, access to SSI is based on Need-to-know as determined by the holder of the information. Where there is uncertainty as to a person's Need-to-know, the holder of the information will request dissemination instructions from his or her next-level supervisor or the originator of the information. Need-to-know is determined in accordance with 49 C.F.R. Section 1520.11 and procedures issued or approved by the TSA SSI Office. Under 49 C.F.R. Section 1520.11(a), a DHS covered person has a Need-to-know specific SSI in the following circumstances: (a) when the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT; (b) when the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT; (c) when the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT; (d) when the person needs the information to provide technical or legal advise to a covered person regarding transportation security requirements of Federal law; and (e) when the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements. Pursuant to 49 C.F.R. Section 1520.11(b), a Federal employee has a Need-to-know SSI if access to the information is necessary for performance of the employee's official duties, and a person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant. Pursuant to 49 C.F.R. Section 1520.11(d), for some specific SSI, DHS may make a finding that only specific persons or classes of persons have a Need-to-know, in accordance with procedures issues or approved by the Director of the TSA SSI Office.

3. A security clearance is not required for access to SSI. However, in accordance with 49 C.F.R. Section 1520.11(c), TSA or USCG may make an individual's access to SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI. The TSA SSI Office must approve any SSI background check or processing requirements or procedures developed by the USCG or any other Component.

4. SSI shall be shared with other agencies, state, tribal, or local governments and law enforcement officials, provided a Need-to-know has been established in accordance with 49 C.F.R. Section 1520.11, and the information is shared in support of transportation security or in the furtherance of a coordinated and official governmental activity.

5. In accordance with 49 C.F.R. Sections 1520.11(b)(1) and 1520.15(c), SSI shall be shared with Congress, Congressional Committees, the Comptroller General (Government Accountability Office), the Office of Inspector General, and other similar entities acting within their official governmental capacities.

I. Storage and Handling

1. When unattended, SSI will, at a minimum, be stored in a locked container or in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a Need-to-know, such as a locked room, or an authorized area where access is controlled by a guard, cipher lock, or card reader. Additional guidance can be obtained through the TSA SSI Office.

2. Information Technology (IT) systems that store SSI will be certified and accredited for operation in accordance with Federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, or additional guidance published by the TSA SSI Office for more detailed information.

3. When removed from an authorized storage location and persons without a Need-to-know are present, or where casual observation would reveal SSI to unauthorized persons, measures such as an unmarked folder, envelope, or SSI cover sheet shall be used to prevent unauthorized or inadvertent disclosure.

J. Transmission

1. When transmitting SSI, the SSI marking must be applied to the transmittal document (letter, memorandum, or fax). The transmittal document must contain, if applicable, a disclaimer noting that it is no longer SSI when it is detached from the SSI it is transmitting (transmittal e-mails do not need to contain this disclaimer), and a warning that if received by an unintended or different recipient, the sender must be notified immediately.

2. When discussing or transmitting SSI to another individual(s), DHS Covered Persons must ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid Need-to-know. In addition, DHS Covered Persons must ensure that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise accessing the information.

3. SSI shall be mailed in a manner that offers reasonable protection of the sent materials and sealed in such a manner as to prevent inadvertent opening and show evidence of tampering.

4. SSI may be mailed by U.S. Postal Service First Class Mail or an authorized commercial delivery service such as DHL or Federal Express.

5. SSI may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.

6. Electronic Transmission.

a. Transmittal via Fax. Unless otherwise restricted by the originator, SSI may be sent via non-secure fax. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

b. Transmittal via E-Mail or Other Electronic Messaging Systems

(1) SSI transmitted via e-mail should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, SSI may be transmitted over regular e-mail channels in accordance with policies and procedures issued or approved by the TSA SSI Office.

(2) SSI shall not be sent to personal e-mail accounts except under unique and urgent circumstances when immediate transmission of information is required in the interest of transportation security and transmittal through approved means is unavailable or impractical.

(3) The use of other electronic messaging systems must be approved by the TSA SSI Office, responsible IT security offices, and appropriate Component SSI Program Managers.

c. DHS Internet/Intranet and Secure Portals

(1) SSI will not be posted on a DHS or any other internet (public) website or unprotected DHS or Component Intranet site.

(2) SSI may be posted on approved government-controlled or -sponsored encrypted or otherwise protected portals (applications or data networks), such as the Homeland Security Information Network (HSIN), USCG HomePort, or TSA's WebBoards. Such posting shall be in accordance with guidance published or approved by the TSA SSI Office and appropriate IT security offices.

K. Destruction

In accordance with 1520.19(b), SSI will be destroyed when no longer needed and its continued retention is not otherwise required under records retention laws and regulations. Destruction may be accomplished as follows:

1. "Hard Copy" materials will be destroyed by shredding, burning, pulping, or pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

2. Electronic records may be deleted in accordance with policies or procedures issued or approved by the TSA SSI Office. Electronic storage media (compact discs, personal computers, etc.) shall be sanitized appropriately by overwriting or degaussing. Contact the TSA SSI Office or the local IT security personnel for additional guidance.

3. Paper products containing SSI will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of SSI must be reported to the DHS Office of Security or the TSA SSI Office. Incidents involving SSI in DHS IT systems will be reported to the Component Computer Security Incident Response Center in accordance with IT incident reporting requirements. The TSA SSI Office shall, in coordination with the DHS SSI Oversight Committee, develop, publish or approve procedures for reporting, mitigating, and investigating incidents involving the improper handling, suspicious or inappropriate requests for, or unauthorized disclosures of SSI.

2. Each Component shall have its own delegated authority to pursue enforcement action of violations of the SSI regulation in accordance with Part 1520.17, other applicable statutes and regulations, and procedures issued or approved by the TSA SSI Office.

M. Program Status Reporting

1. No later than January 15 of each year, each SSI Program Manager shall report, through the TSA SSI Office to the DHS Office of Security, the total number of SSI records that were generated as SSI in their entirety for the preceding calendar year. SSI in their entirety means any record, the entire content of which the creator of the record believes to be SSI. Any record that the creator of the record believes contains a combination of SSI and information that is not SSI is not considered SSI in its entirety and therefore not reportable. The report shall include information as cited in Sections VI.C.4 and VI.E.2.d of this MD. DHS Office of Security shall compile this information into a single report for submission to the House and Senate Committees on Homeland Security no later than January 31 of each calendar year.

2. In addition to the information provided per VI.M.1 above, each SSI Program Manager shall report the number of SSI Coordinators within their respective Components through the TSA SSI Office to the DHS Office of Security.

VII. Questions

Questions or concerns regarding this MD should be addressed to the DHS Office of Security or the TSA SSI Office at ssi@dhs.gov.