Department of Homeland Security
Management Directive System
MD Number: 11056
Issue Date: 12/16/2005

SENSITIVE SECURITY INFORMATION (SSI)

I. Purpose

This Management Directive (MD) establishes 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. Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135 (2002), as amended

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

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

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

E. 49 CFR § 1520, Protection of Sensitive Security Information, May 18, 2004

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

G. DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, January 6, 2005.

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 order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

C. ***Component***: As used in this MD, directorates, agencies, and offices that comprise DHS.

D. ***Designate/Designation***: As used in this MD and as it applies to the identification of SSI, designate/designation refers to the original determination made by the Secretary, the Administrator, Transportation Security Administration (TSA), or the TSA Director of the SSI Program Office, pursuant to 49 CFR §1520.5(b)(16), that information not otherwise categorized as SSI under 49 CFR §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 CFR §1520.5(b)(9)(iii).

E. ***DHS Covered Person***: As used in this MD, a DHS covered person is a DHS individual or entity covered or regulated by the SSI regulation, specifically an individual or entity with DHS transportation security or transportation security-related responsibilities in accordance with 49 CFR §1520.7(h). DHS covered persons have the authority to access and/or generate SSI and are subject to the requirements of this MD and other SSI implementing MD's, procedures, and guidance.

F. ***For Official Use Only (FOUO)***: The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest. Information affecting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information. SSI is not FOUO as SSI is governed by statute.

G. ***Mark/Marking***: As used in this MD, mark/marking refers to the application of the SSI protective marking and distribution limitation statement required by 49 CFR §1520.13 and other associated markings by any DHS covered person to qualified information based on the criteria cited in 49 CFR §1520.5(b), the extraction of SSI information from existing SSI-marked source documents for use in a newly created document, or in accordance with other SSI Program Office-issued and/or approved implementing guidance.

H. ***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 accomplish assigned transportation security or transportation security-related tasks, as determined by an authorized holder of SSI in accordance with 49 CFR §1520.11.

I. ***Record***: As defined in 49 CFR §1520.3, the term record includes any document, presentation, spreadsheet, database, report, etc., used to present information regardless of media or format.

J. ***Redact***: As used in this MD, the permanent obscuring of SSI from a record to permit appropriate release to non-covered persons.

K. ***Sensitive Security Information (SSI)***: SSI is information that would be detrimental to transportation security if publicly disclosed, and is defined in 1520.5(b), as amended. SSI requires protection against public disclosure. 49 U.S.C. 114(s) limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to transportation security. SSI is an information management system of sharing transportation security information with covered persons who have a need to know, without compromising security.

L. ***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/Managers of offices that access and/or generate SSI. Supervisors/Managers shall serve as SSI Coordinators for their respective office until appointment of an SSI Coordinator.

M. ***SSI Program Manager***: Senior official, appointed pursuant to Section V.D. or V.G. of this MD, to oversee the administration and management of SSI within a Component or directorate. For TSA, the Director, SSI Program Office serves as the SSI Program Manager.

V. Responsibilities

A. The DHS Chief Security Officer shall:

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

2. Conduct periodic reviews of Components that access and/or generate SSI for effective management and practical application of SSI, to include random reviews of SSI records for consistent and appropriate application and use of SSI.

3. Coordinate with the Director, SSI Program Office, the development of any security classification guide that may identify information that would warrant protection as SSI.

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

B. TSA Administrator shall:

1. Serve as the delegated authority for implementation, management, and oversight of SSI within DHS pending a reevaluation of authorities and functional responsibilities to be completed by December 31, 2006. Such authority may be delegated.

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. Such coordination may be delegated.

3. Administer implementation, management, and oversight of SSI within TSA, and to the extent defined within this directive, within DHS, through appointment of a senior official to serve as the Director, SSI Program Office. Such official shall have the authority to review and approve or deny requests to designate, pursuant to 49 CFR §1520.5(b)(16), new types of SSI that would be detrimental to security if publicly disclosed, where that information is not otherwise protected as SSI under 49 CFR §1520.5(b)(1) through (15), and to review and approve or deny requests to protect information as SSI pursuant to 49 CFR §1520.5(b)(9)(iii).

4. 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. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

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

C. Director, SSI Program Office shall:

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

2. Participate in the coordination and publication of regulations and procedural guidance for the implementation and management of SSI within DHS. Serve as the approval authority for publication of Component- level SSI guidance and procedures.

3. Issue or approve detailed guidance, with common but extensive examples, on what type of information requires protection as SSI. Such guidance, when issued, shall serve as the primary basis and authority for the recognition and marking of information as SSI by DHS covered persons.

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

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

6. 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.

7. Establish, implement, and serve as Chair of the DHS SSI Oversight Committee.

8. 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.

9. Ensure appointment of TSA office-level SSI Coordinators. TSA SSI Coordinators shall be appointed as necessary within sixty (60) days of publication of this MD. As many SSI Coordinators may be appointed as are necessary to effectively implement and manage SSI recognition, identification, and safeguarding within the respective TSA offices.

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

D. Under Secretary, Science and Technology; Under Secretary, Preparedness; Under Secretary for Policy; Assistant Secretary, Office of Intelligence and Analysis; Assistant Secretary, Immigration and Customs Enforcement (ICE); Commissioner, 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 appointment of a senior official to serve as the SSI Program Manager for each respective Component. The appointed SSI Program Manager shall represent their respective entity on the DHS SSI Oversight Committee. SSI Program Managers shall be appointed within thirty (30) days of the publication of this MD.

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

3. Ensure that periodic and random reviews are conducted for effective management and practical application, and consistent and appropriate application and use of SSI. Such reviews shall assess compliance with regulations, policies, procedures, and guidance governing SSI recognition, identification, and safeguarding.

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

E. SSI Program Manager shall:

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

2. Represent the Component to the SSI Oversight Committee.

3. Conduct periodic reviews and 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 office-level SSI Coordinators. SSI Coordinators shall be appointed as necessary within sixty (60) days of publication of this MD. As many SSI Coordinators may be appointed as are necessary to effectively implement and manage SSI within the respective offices. Maintain an up-to-date record of all Component SSI Coordinators and provide a copy to the TSA Director, SSI Program Office.

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 periodic reviews and 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 Components shall:

1. Ensure compliance with the standards for recognition, identification, and safeguarding of SSI as cited in this MD and other implementing MDs.

2. Where appropriate based on the extent of contact and use of SSI, appoint a senior 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 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.

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

H. DHS SSI Oversight Committee shall:

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

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 marking and safeguarding requirements for SSI as outlined in this MD and TSA-published or approved implementing regulations, directives, procedures, and guidance.

2. Be aware that divulging SSI without proper authority could result in administrative or disciplinary action, civil penalty, or other enforcement or corrective action.

3. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for recognizing, identifying, and safeguarding SSI.

VI. Policy

A. General

1. Statutory and regulatory history: Prior to September 11, 2001, the Department of Transportation (DOT) Federal Aviation Administration (FAA) promulgated the regulation protecting SSI at 14 CFR Part 191 beginning in 1976, in accordance with anti-terrorism legislation passed by Congress in 1974. Following the terrorist attacks on the United States, Congress passed the Aviation and Transportation Security Act (ATSA), which established the Transportation Security Administration (TSA) and transferred the responsibility for civil aviation security to TSA. Among the statutory authorities previously administered by FAA that ATSA transferred was the authority in 49 U.S.C. § 40119, governing the protection of certain sensitive but unclassified information related to transportation security, which was transferred to 49 U.S.C. § 114(s). On February 22, 2002, TSA published a final rule transferring the bulk of FAA's aviation security regulations, including FAA's SSI regulation, to TSA. The TSA SSI regulation is now codified at 49 CFR Part 1520. In November 2002, Congress enacted the Homeland Security Act of 2002 (HSA), which transferred TSA to the newly established DHS. In connection with this transfer, the HSA also amended Section 40119 to vest similar SSI authority in the Secretary of DOT. Following the enactment by Congress of the Maritime Transportation Security Act in November 2002, TSA and DOT expanded the SSI regulation to incorporate maritime security measures implemented by USCG regulations and clarified preexisting SSI provisions in an interim final rule (IFR) issued on May 18, 2004, and effective June 17, 2004. The DOT SSI regulation is at 49 CFR Part 15, and the TSA SSI regulation remains at 49 CFR Part 1520. TSA and DOT subsequently issued a technical amendment to the SSI regulation on January 7, 2005, clarifying that land mode covered persons also have a need to know SSI.

2. TSA, through the SSI Program 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 DHS-wide.

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

4. SSI shall only be used per the intent of Congress to protect information that would be detrimental to transportation security 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 CFR. §1520.15(c), SSI may not be withheld from authorized committees of Congress. Further, pursuant to 49 CFR §1520.11(b)(1), SSI must be shared with members of Congress, their staffs, DHS or TSA management, 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.

5. Under 49 CFR §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 shall draft FOIA SSI review policy and procedures and submit them to the SSI Program Office for approval within six (6) months of the publication of this MD. In accordance with 49 CFR §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.

6. This MD becomes effective upon the date of publication. Standards cited in existing SSI guidance published by Components prior to publication of this MD that are less than those cited in this MD are null and void. Any documents containing such standards shall be revised within six months of publication of this MD. Revised guidance issued pursuant to this MD shall be coordinated with and approved by the SSI Program Office prior to publication.

B. SSI Guidance

1. The SSI regulation, 49 CFR §1520.5(b)(1) through (16), provides fifteen categories [49 CFR §1520.5(b)(1) through 49 CFR §1520.5(b)(15)] of information that have been determined to be SSI. The SSI regulation also has one category, 49 CFR §1520.5(b)(16), and one part of one category, 49 CFR §1520.5(b)(9)(iii), under which an official, authorized pursuant to this MD, may designate that certain information not otherwise falling within the SSI categories represented in (b)(1) through (b)(15) is SSI.

2. The SSI Program Office shall issue guidance that significantly expands upon the descriptions for categories of information that must be marked and protected as SSI as cited in 49 CFR §1520.5(b)(1) through (15). To the extent possible, such guidance shall provide DHS covered persons with an accurate source for recognizing when and when not to apply the SSI marking and shall include common examples of specific types of information to be marked and protected as SSI. When published, this guidance shall serve as the primary authority and source for the recognition and marking of SSI by DHS covered persons.

C. Original Designation of Information as SSI

1. The Secretary, the TSA Administrator, and the TSA Director of the SSI Program Office, are authorized to designate information as SSI, pursuant to 49 CFR §1520.5(b)(16), that is not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15). This authority includes a determination to protect detailed information about screening locations in accordance with 49 CFR §1520.5(b)(9)(iii).

2. Only delegated officials as cited in C.1. above shall have the authority to designate information as SSI that is not otherwise covered under 49 CFR §1520.5(b)(1) through (15).

3. If information is identified or developed that would be detrimental to transportation security if publicly disclosed but it is not otherwise categorized as SSI under 49 CFR §1520.5(b)(1) through (15), it shall be transmitted through the applicable Component SSI Program Manager to the Director, SSI Program Office or the appropriate official cited in Section VI.C.1. above, 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 SSI Program Office, pending a final assessment by the Director, SSI Program Office.

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

5. Information designated as SSI shall be marked in accordance with 49 CFR §1520.13. Additionally, the front page, title page, and/or the first page shall include the notation *"Designated SSI Pursuant to 49 CFR §1520.5(b)(16),"* or, *49 CFR §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.

6. 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. Any DHS covered person shall mark information as SSI if it meets the criteria for SSI as cited in 49 CFR §1520.5(b) and implementing guidance issued or approved by the SSI Program Office. 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 substantially 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 CFR §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 the record contains other types of information that does require portion marking, i.e., classified information, or, the information is to be transmitted outside of DHS to Congress or Congressional committees. When used, such portion markings shall be reviewed by the Component SSI Program Manager (in the case of TSA, the TSA Director, SSI Program Office) prior to dissemination. The parenthetical abbreviation (SSI) shall be used.

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

c. The Director, SSI Program Office, with the participation of the SSI Oversight Committee, shall conduct a study on the application of an authority line and the feasibility of using portion markings for all SSI records. No later than one year following publication of this MD the Director, SSI Program Office, through the SSI Oversight Committee, shall submit to the TSA Administrator and DHS Office of Security, a report detailing the results of the study and recommendations and justifications for the use or non-use of portion markings.

E. Duration of SSI and SSI Reviews

1. Information designated or marked as SSI will remain SSI unless determined releasable by the responsible designating agency official: TSA Administrator, the Commandant of the USCG, the TSA Director, SSI Program Office, or other authorized offices, in accordance with policies and procedures issued or approved by the SSI Program Office.

2. The TSA Director, SSI Program Office, shall coordinate with the USCG and the SSI Oversight Committee on the development and implementation of appropriate policy and procedures for the loss or removal of the SSI designation from information that has no current or future security implications under 49 CFR §1520.5(c).

3. In accordance with 49 CFR §1520.15(a) and Section VI.A.5 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 SSI Program Office.

4. Such offices may also redact SSI records in response to other public requests, e.g., litigation (civil, criminal, or employment), reports intended for public release, and other requests, in accordance with policies and procedures issued or approved by the SSI Program Office

F. Challenging SSI

1. 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.

a. 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 CFR §1520.5(b)(1) through (15) and implementing guidance published or approved by the TSA Director, SSI Program Office.

b. 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 SSI Program 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 TSA Director, SSI Program Office. A further appeal to the decision made by the TSA Director, SSI Program Office, may be made to the TSA Administrator. The decision of the TSA Administrator shall be final.

c. Individuals submitting a challenge shall not be subject to retribution of any kind for bringing such actions. Anonymity can be requested by processing the challenge through the SSI Program Office or the DHS Office of Security. The SSI Program Office or the DHS Office of Security shall honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

G. Audits and Inspections

1. Nothing in this directive 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 shall, either independently or in conjunction with reviews conducted pursuant to DHS MD 11041, Protection of Classified National Security Information/Program Management, conduct periodic oversight and compliance reviews of SSI within DHS.

3. The TSA Director, SSI Program Office, shall develop, issue, or approve policies, procedures, and guidance for the implementation and management of self-inspection programs for Components that access or generate SSI. No later than sixty (60) days after publication of this MD, the SSI Program Office shall create, under the auspices of the SSI Oversight Committee, and publish or 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 no later than ninety (90) days from the publication of this MD and not later than every eighteen (18) months thereafter. The results of self-inspections conducted pursuant to this MD shall be reported to the SSI Program Office within thirty (30) days after completion. Discrepancies cited during the self-inspection shall be reconciled in a timely manner and follow-up by the SSI Program Manager or the SSI Program Office will be accomplished as needed.

5. SSI Coordinators shall conduct a self-inspection of the applicable office SSI program no later than 120 days from publication of this MD and no later than every twelve (12) months thereafter. 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 follow-up by the SSI Coordinator or the SSI Program Manager will be accomplished 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 TSA Administrator may determine in writing that information that might otherwise be considered SSI may be publicly released in the interest of transportation security or public safety under 1520.5(b) in accordance with procedures issued or approved by TSA. Under 1520.9(a)(2), the TSA Administrator and the Commandant of the USCG may also determine in writing that specific SSI may be released to non-covered persons in accordance with policies and procedures issued or approved by the SSI Program Office.

2. 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 1520.11 and procedures issued or approved by the SSI Program Office. 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 has a need to know SSI if access to the information is necessary to performance of the contract or grant. For specific SSI, DHS may make a finding under 1520.11(d) in accordance with procedures issued or approved by the SSI Program Office that only specific persons or classes of persons have a need-to-know. Under 1520.11(a), a DHS covered person has a need to know specific SSI if they need the SSI to: (1) "...carry out transportation security activities ...; (2) ... [receive] training to carry out transportation security activities ...; (3) ... supervise ... transportation security activities ...; (4) ... provide technical or legal advice to a covered person regarding transportation security requirements ...; or (5) ... represent a covered person in connection with any judicial or administrative proceeding regarding [transportation security]...".

3. A security clearance is not required for access to SSI. However, in accordance with 1520.11(c), a security background check or other procedures may be required by TSA or the USCG to receive specific SSI. The SSI Program 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, Federal, state, tribal, or local governments and law enforcement officials, provided a need-to-know in accordance with Part 1520.11 has been established 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 1520.11(b)(1) and 1520.15(c), SSI shall be shared with Congress, Congressional committees and staffers, the 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 SSI Program Office.

2. 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 Program 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 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), all 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, and 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 email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, SSI may be transmitted over regular email channels in accordance with policies and procedures issued or approved by the SSI Program Office.

(2) SSI shall not be sent to personal email 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 SSI Program 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 SSI Program Office and appropriate IT security offices.

K. Destruction.

1. 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 regulations. Destruction may be accomplished by:

a. "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.

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

c. 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. 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 SSI Program 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 SSI Program Office.

M. Program Status Reporting

1. No later than January 15 of each year, each SSI Program Manager shall report, through the SSI Program 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 document, the entire content of which the creator of the document believes to be SSI. Any document that the creator of the document 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 Section VI.C.4. 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 M.1. above, each SSI Program Manager shall include the number of SSI Coordinators within their respective Components.

VII. Questions

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