APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1300 I Street, NW, Suite 1200 East, Washington, DC 20005

APTA SS-ISS-RP-003-23
First Published: May 23, 2023

Transit Infrastructure Security Working Group

Sensitive Security Information Policy

Abstract: This document establishes minimum standards for handling Sensitive Security Information (SSI) in a transit agency environment.

Keyword: Sensitive Security Information (SSI)

Summary: Transit agencies are charged with making improvements to the country's transportation security systems and protecting against terrorist attacks. SSI is a specific category of information that requires protection against disclosure in order to protect the safety of passengers in transportation.

Scope and purpose: The purpose of this document is to explain minimum standards for handling SSI in order to minimize the risk of threats and ensure that all employees and contractors understand and implement the agency's requirements for marking, storing, controlling, transmitting, destroying and managing the release or withholding of SSI. The SSI procedure must be implemented by the transit agency's employees and contractors and applies to SSI in every form in which it is stored, including paper, electronic, magnetic and other media. This recommended practice is not intended to be the authoritative source for all SSI policy considerations. Agencies should consult with their legal department to ensure that any actions the organization undertakes comply with 49 CFR part 1520 and all other federal, state and/or local laws governing protection of information.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **APTA Transit Infrastructure and Systems Security Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Lurae Stuart, *Chair*
Mark Uccardi, *Vice Chair*

Ryan Chelski, *Sound Transit*
Neil Crosier, *King County Metro*
Dean Fajerski, *TSA*
Kevin Franklin, *BART*
Erin Gorrie, *ADS Safety*
Stephan Parker, *Transportation Research Board*
Rob Pascoe, *King County Metro*
Jacob Peltier, *Community Transit*
John Plante, *METRA*
Branden Porter, *Sound Transit*
Jason Powell, *Metro St. Louis*
Charles Rappleyea, *WSP USA*
Harry Saporta, *WSP USA*
Lurae Stuart, *WSP USA*
Kirsten Tilleman, *WSP USA*

Project team

Polly Hanson, *American Public Transportation Association*
Eric Halzel, *Eagle Hill Consulting*

Introduction

This introduction is not part of APTA SS-ISS-RP-003-23, "Sensitive Security Information Policy."

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Sensitive Security Information Policy

1. Overview

1.1 Background

Sensitive Security Information (SSI) is a specific category of information that if released to the public would be harmful to transportation security. TSA issued an extension of SSI protections through all systems of transportation.

SSI is a form of sensitive information but is not considered to be classified information. It is imperative that SSI be handled accordingly, and there are certain policies that must be followed in depth to accurately mark, protect and destroy SSI documents.

SSI regulations are set by the government to prevent harm to an organization or its customers.[1] At risk of penalty, information should not be designated as SSI only to conceal law violations or errors, avoid embarrassment, impede competition, or prevent/delay the release of non-sensitive information.[2]

1.2 Applicability to transit agencies

Not all transit agencies qualify under federal law to have an SSI program. Therefore, smaller transit agencies and agencies in rural areas may not have a need to possess or come in contact with SSI. At the time of publication, transit agencies need only establish an SSI program for the following:[3]

1. Security programs and contingency plans issued, established, required, received or approved by the Department of Homeland Security (DHS) or Department of Transportation (DOT)
2. Vulnerability assessments that are directed, created, held, funded or approved by DHS or DOT, or that will be provided to either agency in support of a federal security program
3. Threat information held by the federal government concerning transportation, transportation systems and cyber-infrastructure, including sources and methods used to gather or develop the information

Applicability may change over time. Agencies should continuously reevaluate their status to determine if they qualify under federal law to have an SSI program.

Any transit agency that accepts grant funding from DHS or DOT must determine if its records qualify as SSI and must appropriately categorize, mark and control them.

If the information above does not apply to a transit agency, then it is not authorized to designate documents as SSI.

1.3 Designation authority for SSI

The person who has the ultimate authority to declare whether or not information is SSI is the TSA administrator. With this said, any person who is an authorized recipient (i.e., a covered person with a need to

[1] As defined in 49 CFR 1520
[2] As defined in 49 CFR 114 (r)
[3] As outlined by Federal Transit Administration, “SSI: Designation, Markings, and Control - Resource Document for Transit Agencies”

know[4]), may mark information that they believe constitutes SSI as specified in regulation.[5] Any documentation that is designated as SSI or contains SSI must adhere to government regulation for marking, sharing, protecting and handling SSI.[6] Organizations are not given their own discretion with how to manage or declare this information to the extent that it is specified in regulation.

2. Elements of an SSI program

A successful SSI program establishes roles, covers step-by-step development and contains specific procedures. Failure to include any of these elements will lead to the creation of an SSI program that is not in compliance with federal requirements.

A successful SSI program is also scalable and flexible while still meeting regulatory requirements. Agencies should continuously review and reevaluate their SSI programs to ensure that they meet the evolving needs of their organizations.

2.1 Develop SSI protocols

When developing an SSI program, it is important for a public transit agency to gather references and resources that enable timely, efficient and effective progress. Among the items that should be gathered are (1) the Model SSI Policy; (2) a copy of 49 CFR §1520; (3) the Federal Transit Administration's "SSI: Designation, Markings, and Control - Resource Document for Transit Agencies"; (4) the TSA's Sensitive Security Information Stakeholder Best Practices Quick Reference Guide"; and (5) information concerning the processing of Freedom of Information Act and/or state and local "Sunshine Law" requests. In certain circumstances, additional information will be needed, such as how the agency currently handles such information requests.

Once a policy and program have been developed for an agency, they should be reviewed by legal staff or other legal resources. SSI protocol development is an ongoing activity, with the policy being updated and improved to reflect changes in federal statutes and regulatory guidance and to include information gathered during periodic reviews as well as incident investigations.

2.2 Assign roles and responsibilities

2.2.1 SSI program manager

Every SSI policy should include the creation of an SSI program manager. Larger agencies may have an SSI program manager for component subdivisions, while smaller agencies may only have a single SSI program manager for the entire agency. This individual may be part-time or full-time equivalent.

The SSI program manager serves as the official responsible for management, implementation and oversight of SSI within the agency or component. This official conducts self-inspections to ensure effective SSI management, proper practical implementation of SSI policy and adherence to SSI protocols. The SSI program manager should have security training/expertise.

2.2.2 Additional roles, as needed

Given size, need and available resources, the SSI program manager may elect to appoint additional personnel to implement and manage the agency's SSI program. The role may be permanent or project-specific.

For example, the SSI program manager may create a role responsible for administering and overseeing the SSI program within a particular office. Responsibilities could include assisting other office personnel in the

[4] As defined by 49 CFR 1520
[5] As defined by § 1520.5(b)(1) through (16)
[6] As defined by 49 CFR 1520

appropriate use and application of SSI materials, determining whether documents are to be designated as SSI, conducting self-inspections at the office level, and liaising with the SSI program manager.

2.3 Designate covered persons

The approval for requests for designation as covered persons will usually be performed by the SSI program manager or a member of their staff. Under certain circumstances, there will be requests for designation that come from outside an agency.[7] In those circumstances, the SSI designation will normally be handled at the agency level, and the individual(s) requesting covered persons designation may be required to pass a federal security background check prior to receiving such a designation. All covered persons are to be expected to fulfill the previously enumerated responsibilities and obligations in regard to SSI. The determination of need-to-know status would also be made at the same level as the original covered persons designation. In questionable cases, it is always best to request assistance from the next highest level of SSI program management.

2.4 Establish SSI training program

Agencies using and/or generating SSI are mandated to have an SSI training program. This training program should be tailored to the specific needs of the agency and provide different levels of training depending upon the designation of a given trainee. For example, SSI program managers and any additional SSI staff will need far more thorough and intensive training than a covered person, while a non–covered person would realistically only need to be trained to identify SSI documents by their markings, in the event of accidental disclosure or loss, and how to report such incidents. SSI training should be mandatory for agency staff.

2.5 Evaluate and improve procedures

The SSI program manager should perform self-inspections at the agency/component level at least once every 18 months. If applicable, self-inspections at the office level should be performed at least once every 12 months. If performed by any additional SSI staff, the results of self-inspections should be reported to the SSI program manager. Any discrepancies, problems or issues should be reconciled in a timely manner and remedial action taken as needed. Each agency should establish specific guidelines for conducting a self-inspection, as well as create a uniform standard for reporting the results. These guidelines should ensure that self-inspections assess compliance with regulations, policies, procedures and guidance concerning SSI recognition, identification, dissemination and protection. Agencies should also create policies instituting the creation and tracking of Corrective Action Plans (CAPs) in response to these inspections. If any reportable incidents are discovered that had not been previously reported, those incidents should be handled immediately.

3. Protective marking and limited distribution statement for SSI

3.1 Responsibility

If one manages any documents containing SSI, it is pertinent that they first properly mark the item as SSI. They must also follow all protocols regarding the document to keep it guarded from the public, as it could possibly be detrimental to the transportation agency and its passengers. If the document containing SSI is to be distributed (following proper protocols for distribution) and it does not possess proper markings, the recipient must apply the proper marks and notify the sender of this error.

[7] For example, a civil litigant requesting designation to allow access to SSI deemed necessary by the court for the purposes of that litigation only

3.2 Document designation principle

One of the many difficulties that come with governing possible SSI is the process of determining whether the information meets the standards for SSI.[8] See Appendix A for ideal principles that may help to identify if a document should be considered SSI.

Information received from another agency, to include TSA, must retain the SSI markings and handling instructions unless reviewed by TSA for potential release.

3.3 Requirements

SSI documents have specific requirements that must be followed when this information is being handled. These requirements are federally regulated and set by TSA. The requirements below are to be applied to all information deemed to be SSI:

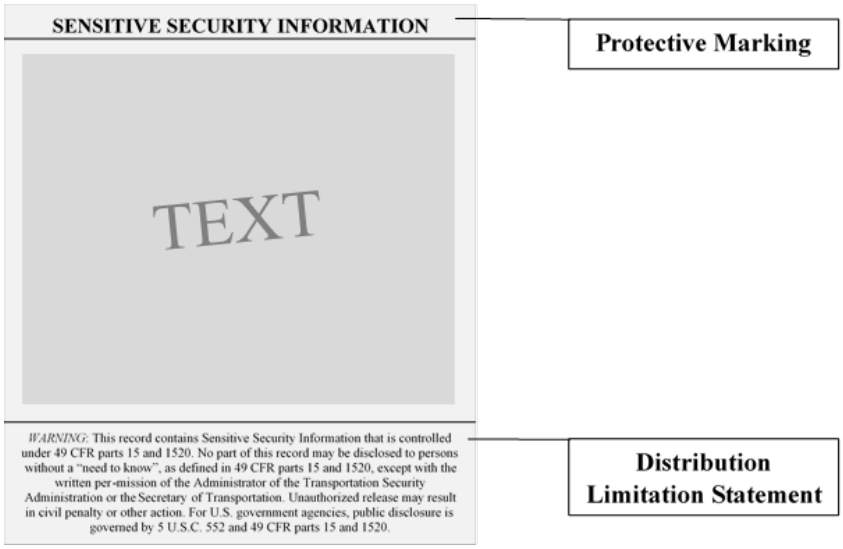
- **Protection.** Any documents which include SSI must be safeguarded. Physical copies of documents must be kept in a secured location such as a locked file cabinet. Only people with a need to know should have access to or knowledge of this information unless otherwise stated in writing by organizations such as the DOT or TSA.
- **Marking.** There is no exception to this rule. Every page of the record should include an SSI header (i.e., protective marking) and footer (i.e., Distribution Limitation Statement). See **Figure 1**.
    - **Protective marking.** When marking a document containing SSI, it is required that it include "SENSITIVE SECURITY INFORMATION" in the header of the record.
    - **Distribution Limitation Statement.** This is the statement that specifies directions as to what is on the records and belongs in the footer of the record. *This statement is specified by regulation and must not be modified*:

      WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

- **Destruction of SSI.** Documents containing SSI that are no longer needed should be properly destroyed in such manner that they cannot be reconstructed.

[8] As mentioned in 49 CFR 15 and 1520

FIGURE 1
Sample Record with SSI Header and Footer



3.4 Categories of protected information

3.4.1 Categories of SSI[9]

There are 16 different categories of SSI that have been created over its legislative and regulatory history. Review the full list of categories (Appendix C) when making SSI determinations.

3.4.2 Other categories of protected information

Should information at a transit agency not rise to the level of SSI, it may consider the multiple additional categories of protected information routinely used by the federal government. These categories include, but are not limited to, Law-Enforcement Sensitive (LES) Information, Protected Critical Infrastructure Information (PCII) and For Official Use Only (FOUO) Information.[10]

Other sensitive information may require protection as confidential, secret or top secret and is classified to prevent the exposure of things such as national defense, agency plans or public safety. There are also other types of information that are sensitive but unclassified, now known as Controlled Unclassified Information (CUI). CUI is a marking regime specifically required of the federal government which may start to be seen by transportation agencies as federal agencies advance its implementation.

Transit agencies should consult with their legal departments or other legal resource to determine the most appropriate category of protected information for their materials.

3.5 SSI marking requirements[11]

Although marking of records is specified by SSI regulation (see Section 3.3), different formats may have unique considerations. Suggested marking for various record formats are indicated in the sections that follow.

[9] All quotations within this section are direction from 49 CFR §1520.5(b)(1)–(16).
[10] As defined in DHS Management Directive 11042.1
[11] SSI marking requirements per 49 CFR 15.13 and 1520.13

3.5.1 Documents

- **Protective marking.** SSI documents should have an SSI coversheet (see Appendix D). The title page, as well as each page of the document, must contain proper markings. This is also inclusive of the front and back cover of the document.
- **Distribution Limitation Statement.** This is the statement that specifies direction as to what is on the record. There is only one distribution record, but it is specific to the type of SSI document.
    - **Paper records.** Must be included at the bottom of every page including the binder covers, front and back covers and title pages. It must be larger than the text of the document.
    - **Electronic records.** Must be marked in a similar manner, on every page.
    - **Non-paper records.** Must be placed clearly and visibly so that it can be seen or heard by the recipient. Any containers should be marked on the outside.

3.5.2 Charts, maps and drawings

- **Protective marking.** SSI documents that may be designated as charts, maps and drawings are to have the appropriate protective marking propped in a manner that is plainly visible.
- **Distribution Limitation Statement.** Charts, maps and drawings must have the appropriate Distribution Limitation Statement affixed in a manner that is plainly visible.

3.5.3 Video recordings

- **Protective marking and Distribution Limitation Statement.** The protective marking and Distribution Limitation Statement must be applied at the beginning and end of each video recording and affixed in such a manner that it is fully visible on the screen or monitor. Videotape recordings that contain SSI must include, on the recordings, conspicuous visual protective marking and Distribution Limitation Statement at both the beginning and the end, if practicable. Protective marking and the Distribution Limitation Statement must also be applied on the front, back and each side of the video case and storage container(s).

3.5.4 Electronic and magnetic media

- **Information extracted from.** The protective marking is not required on the information in the form of compiled lists of SSI information extracted from electronic and magnetic media. However, it must have the Distribution Limitation Statement affixed on the bottom of each page containing SSI and to any cover page and back page. The Distribution Limitation Statement may be applied by the equipment itself on the face of the page, provided that the Distribution Limitation Statement is clearly distinguishable from the printed text.
- **Information contained on.** SSI contained on electronic and magnetic media must have protective marking, and the Distribution Limitation Statement must be applied at the beginning and end of the electronic and magnetic text. The protective marking and Distribution Limitation Statement must be displayed in such a manner that both are fully visible on the screen or monitor when the text is viewed. The protective marking and Distribution Limitation Statement must also be applied to each side of the disk and the disk sleeve/jacket, on the non-optical side of the CD-ROM and both sides of the CD-ROM case. If the electronic/magnetic text has a soundtrack, then audible warnings that describe the protective marking and Distribution Limitation Statement must, if possible, be included in the introduction and at the end of this text.

3.5.5 Systems

- **Protective marking.** Information systems which hold, process or store SSI should contain marking of some kind, such as tagging or user notice on system entry. Likewise, the system owner shall use reasonable standards for protecting the information accordingly, such as limiting SSI access only to those with a need to know and following industry standards for protecting sensitive information in systems (e.g., password protecting documents and workstations).

See Appendix E for a high-level checklist on SSI marking requirements.

3.6 Transmittal documents

Documents that are used to transfer SSI but do not themselves contain SSI must be marked with the Distribution Limitation Statement. In addition, the following statement must be affixed to the front page of the transmittal document:

> The protective marking SENSITIVE SECURITY INFORMATION and/or the Distribution Limitation Statement on this document are canceled when the attachments containing SSI are removed.

4. Storage of SSI

4.1 Requirement

All agency employees and contractor employees possessing SSI are responsible for ensuring that the information, records and systems containing SSI are safeguarded at all times from disclosure to unauthorized people. When the SSI for which an individual is responsible is not under the individual's direct physical control, the individual is responsible for ensuring that it is safeguarded and protected in such a way that it is not physically or visually accessible to people who do not have a need to know, as defined in "Definitions" at the end of this document. For example, when unattended, SSI must be secured in a locked container, office or other restricted-access area.

4.2 Key and combination control

When an individual responsible for SSI places the material in a locked container, the individual is responsible for ensuring that positive measures are in force to restrict access to the container keys or combination to only individuals with a need to know.

5. Control and release of SSI

5.1 Authority to release and/or withhold SSI documents/information

If the information was designated SSI by the transportation agency, the SSI program manager is the only individual with the authority to determine that the information was erroneously marked and can be released. The SSI program manager may consult any additional SSI staff before making a decision. Alternately, the transportation agency could create a different version of the document redacting any information that might be sensitive (see Section 5.2).

If information was designated SSI by TSA or another entity, it may not be released by the SSI program manager without coordination with TSA. Information received from another agency, to include TSA, must retain the SSI markings and handling unless reviewed by TSA for potential release. The transportation agency may disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA.[12] Transportation agencies must refer requests by other persons for SSI to TSA.[13]

5.2 Request for information designated SSI

All requests for SSI must be submitted to the SSI program manager for approval prior to release, except for SSI preapproved for regulatory agencies (see Section 5.5).

- **Release of records containing both SSI and non-SSI.** If a record contains information that may not be disclosed but also contains information that may be disclosed, the latter information will be supplied in response to a request, provided that the record is not otherwise exempt from disclosure

[12] § 1520.9(a)(2)
[13] § 1520.9(a)(3)

under applicable public records disclosure laws. The SSI-critical information must be redacted from the record. If it is not practical to do so, then the entire record will be withheld from public disclosure. TSA provides redaction services to remove SSI from documents prior to public disclosure by emailing SSI@tsa.dhs.gov.

5.3 Contractor access to SSI

Prior to a contractor gaining access to SSI, the department director must notify the SSI program manager and recommend approval. Contracts should specify regulatory requirements for protection of SSI and other transportation agency policy requirements. Use of nondisclosure agreements is strongly encouraged.

5.4 Control and release of contractor-copied SSI

Contractors must provide prior notification in writing, through the contract manager and/or Procurement Department, to the originator of SSI when the contractor needs to make copies of SSI. This written notification must contain the following minimum information:

- positive identification of SSI (title, document numbers as applicable, etc.)
- the purpose of making the copies
- number of copies
- dissemination of copies (the contractor must verify and ensure that all recipients are authorized to receive SSI)

5.5 Release of SSI to government officials/employees and regulated parties

Release of SSI is permitted to federal, state and municipal government officials/employees and regulated parties who have a need to know as established by regulation or authorized by DOT, Coast Guard or TSA.

Release of SSI is permitted to federal, state and local law enforcement officials, or to federal intelligence agencies that have a need to know as established by regulation or authorized by the SSI program manager.

5.6 Requests for SSI from a foreign government and/or other foreign or international entity

Requests for SSI must be referred to the DOT and TSA.

5.7 Inadvertent release of SSI

An employee with knowledge of an inadvertent release of SSI must immediately notify the SSI program manager. When a transportation agency becomes aware that SSI has been released to unauthorized people, the transportation agency must promptly inform TSA or the applicable DOT or DHS component or agency.[14]

6. Packaging and transmitting SSI

6.1 Responsibility

The term “SSI transmission” refers to the means used to transfer SSI from one location to another. A transfer may involve physical relocation or the electronic transmission of information. In either case, the individual responsible for the SSI is also responsible for ensuring that the material is packaged and/or transmitted in accordance with the requirements in this procedure to guard the information from unauthorized disclosure to people who do not have a need to know.

[14] 49 CFR § 1520.9(c)

6.2 Packing and transmission requirements for SSI

When assembling a package containing SSI for transmission, it is the responsibility of the individual preparing the package to ensure that all SSI has the appropriate protective marking and the Distribution Limitation Statement.

- **Mail.** SSI may be transmitted by U.S. Postal Service First-Class Mail or regular parcel post, or by other delivery services (FedEx, UPS, etc.). SSI that is to be sent by mail or by a delivery service must be wrapped in opaque envelopes, wrappings or cartons. Addressing the package with an attention line containing the name and office of the recipient helps to ensure that the SSI material is received and opened only by authorized personnel.
- **Interoffice mail.** When sent by interoffice mail, SSI must be transmitted in a sealed envelope in such a manner as to prevent inadvertent visual disclosure.
- **Hand-carrying within or between buildings.** SSI that is carried by hand within or between buildings must be protected (by a cover sheet, protective folder, distribution pouch, etc.) to prevent inadvertent visual disclosure.
- **Packaging material.** Envelopes or containers must be of such strength and durability that they will provide physical protection during transit and will prevent items from breaking out of the containers or envelopes.

6.3 Electronic transmission of SSI

- **Electronic mail or web posting.** SSI transmitted by email must be in a password-protected attachment. SSI is not authorized for posting on the internet/intranet except for postings on secure sites as specifically authorized by the SSI program manager (see Appendix B).
- **Facsimile.** Facsimile is discouraged from use. In instances where facsimile is necessary, the sender must confirm that the facsimile number of the recipient is current and valid.
    - If the recipient has a facsimile machine in a controlled area where unauthorized people cannot intercept the SSI facsimile, the sender may send the SSI facsimile without requiring that the recipient be there to receive it promptly. Otherwise, the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information.
    - If the facsimile machine stores transmitted information, then clear the data immediately after use.
    - The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that if the message is received by anyone other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.
- **Telephone.** The caller must ensure that the person receiving the SSI is an authorized recipient. The risk of interception and monitoring of conversations is greater when using cellular telephones and cordless telephones, which transmit the conversation to a base unit. Individuals needing to pass SSI by telephone must avoid these devices unless the circumstances are exigent, or the transmissions are encoded or otherwise protected.
- **Videoconferencing.** Secure videoconferencing relies on both the transportation agency and the user participation in security. Transportation agencies should verify and enable videoconferencing security and encryption settings on tools approved for business use.
    - Meeting hosts must take steps to ensure that only authorized recipients/participants can access a meeting where SSI will be shared or discussed.
    - Ensure that meetings are set to private. Consider using an access code and "waiting room" to vet participants before they are given access and/or manual admission/removal of attendees.
    - Use only videoconferencing tools approved by the transportation agency for business use.
    - Use only secure networks (e.g., VPN) or secure Wi-Fi networks (i.e., encrypted and restricted) to connect to meetings. Avoid using public hotspots and networks.

See Appendix E for a high-level checklist on SSI packing and transmission requirements.

7. Destruction of SSI

7.1 Requirement

When copies of records containing SSI are no longer needed, they must be promptly and completely destroyed.

7.2 Methods

The objective of a selected destruction method is to destroy the material so the recovery of the sensitive information is difficult, if not impossible. Material containing SSI must be destroyed by one of the following methods, listed in order of preference:

1. Any means approved for the destruction of designated SSI material as specified in this policy. The approved methods include confetti/crosscut shredding or irreparably destroying.
2. Tearing the SSI material into small pieces and assimilating it with other waste material.

7.3 Contractor notification of destruction of SSI

When a contractor proposes to destroy copies of records containing SSI, the contractor must first provide notification in writing, through the Procurement Department to the information originator, of its destruction. The contractor must provide the following minimum information regarding the destruction of SSI:

- identification of the information to be destroyed (title, document/copy numbers as applicable, etc.)
- number of copies destroyed
- date and place of destruction
- method of destruction
- residual SSI that is remaining in custody of the contractor

See Appendix E for a high-level checklist on SSI destruction requirements.

Definitions

covered person: Any organization, entity, individual or other person described in 49 CFR § 1520.7.

need to know (federal, state, local or tribal government employees, contractors and grantees): A federal employee has a need to know SSI when access to the information is necessary for the federal employee to perform their official duties to the best of their ability. A contractor employee has a need to know SSI when access to the information priority is in executing work to fulfill a contract or grant.

need to know (regulated parties and others): For specific SSI, the designated authority may make a finding that only specific people or classes of people have a need to know. Otherwise, a regulated party has a need to know SSI in each of the following circumstances:

- When the person needs the information to carry out transportation security duties.
- When the person needs the information to supervise or otherwise manage individuals carrying out transportation security duties.
- When the person needs the information to advise an operator, carrier or other affected entity regarding transportation security duties.
- When the person needs the information to represent an operator, carrier or other person receiving information in connection with any enforcement proceedings.

Requests for SSI from regulatory agencies concerning permits should be automatically granted, provided that requested materials are properly labeled.

record: Any writing, drawing, map, tape, film, photograph or other means by which information is preserved, regardless of format. This includes paper, electronic and magnetic media.

Sensitive Security Information (SSI): Records and information specified as a security and safety risk to the agency or people in transportation, including any information that would allow a malicious actor to select or gain information about a target without the need to physically access it. Documents produced prior to this procedure do not have to be designated SSI unless the document is revised, changed or released after the approval of this procedure. See Appendix A for a current list of designated SSI.

SSI Distribution Limitation Statement: The statement applied to SSI providing explicit direction concerning the restrictions which apply to the information or records. It states the authority for controlling distribution and specifies, when appropriate, the distribution approval procedures.

Abbreviations and acronyms

CAP Corrective Action Plan
CFR Code of Federal Regulations
CUI Controlled Unclassified Information
DHS Department of Homeland Security
DOT Department of Transportation
FAA Federal Aviation Administration
FOUO For Official Use Only
NATSA North American Transportation Services Association
SSI Sensitive Security Information
TSA Transportation Security Administration
TVA Threat Vulnerability Assessment

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	June 6, 2021	July 9, 2021	January 24, 2022	June 22, 2022	May 23, 2023
First revision	—	—	—	—	—

Appendix A: Information constituting SSI

The following list provides examples of information constituting SSI:

- any approved, accepted or standard security program relating to the agency
- any security contingency plan or information and any comments, instructions or implementing guidance pertaining to the agency
- technical specifications of any security communications equipment and procedures.
- any documents containing facility capacities and emergency measures (e.g., redundant capabilities, emergency power-down procedures)
- information concerning threats against public transportation
- any draft proposed or recommended change to the information and records identified in this section
- information in a vulnerability or risk assessment that has been authorized and approved by the SSI program manager
- information, policies or procedures concerning:
    - compressed natural gas
    - liquid natural gas
    - gasoline and diesel fuel usage and storage
    - above ground and underground storage tanks
    - emergency power generators
    - electric panels
    - gas mains and shutoffs
    - water mains and shutoffs
- locations and specifications regarding information technology equipment, including servers, routers, telephone hubs, etc.
- identifications and passwords associated with major information technology systems used at the agency
- internet provider addresses associated with information technology equipment (server, switch, router, etc.)

Appendix B: The electronic posting/transmission of SSI

Web posting. SSI information can be posted only on agency-approved websites. Such sites must be approved by and comply with the standards established by the agency's Information Technology Department and authorized by the SSI program manager.

Electronic transmission. All SSI information transmitted via email must be password-protected via strong password standards established by agency's Information Technology Department.

The following is *sample criteria* for electronic posting/transmission of SSI. Work with your agency's SSI program manager and Information Technology Department for more specific guidance.

- **Password creation.**
  - System and/or document owners are responsible for password creation and maintenance.
  - Best practice strong password guidelines:
    - eight-character minimum length
    - at least one letter capitalized
    - contain at least one number
    - not be a word in the dictionary
- **Communicating passwords.**
  - Each SSI attachment should be password-protected by the sender.
  - If possible, the sender should transmit the password to the receiver(s) by alternate means other than email, (e.g., telephone or fax). The use of cellular or cordless phones may be restricted.
  - This procedure *should not* be used for the transmission of classified information.
- **Password duration and usage.**
  - Sites containing SSI, as approved by the Information Technology Department and SSI program manager, may request authentication when retrieving documents.
  - Password duration for user accounts may be governed by the Information Technology Department.
- **Administration of passwords.**
  - The Information Technology Department may establish common passwords.
  - One common password, subject to duration requirements, may be authorized for all SSI documents transmitted between agency employees.
  - A separate but common password, subject to duration requirements, may be authorized for all SSI documents transmitted to non-agency employees with a need to know.

Appendix C: Categories of SSI

The following are all 16 categories of SSI that have been created over its legislative and regulatory history. At the time of publication, transit agencies need establish an SSI program for only the first three categories:

1. **Security Programs & Contingency Plans:** Within this classification would fall all documents dealing with the security programs of a public transit agency, as well as such things as a transit agency's Emergency Operations Plan, Comprehensive Emergency Management Plan, Continuity of Operations Plan, Devolution Plan, etc. Much, if not most, of the SSI created by a public transit agency will fall under this category.[15]
2. **Vulnerability Assessments:** A Threat Vulnerability Assessment (TVA), the underlying data, reports based on the TVA and the CAPs are to be designated as SSI.
3. **Threat Information:** Specifics concerning actual threats are also considered SSI. A public transit agency may release to the general public only such information as is necessary in the conduct of a criminal investigation but is not required to disclose all information gathered concerning a security threat or even the existence of a security threat to a transit facility/system.

The remaining SSI categories that will not apply to transit agencies at this time are as follows:

4. **Security Directives:** A type of document within the TSA (formerly the Federal Aviation Administration [FAA]) or the Coast Guard security bulletin process, the Security Directive was created to comply with the Aviation Security Improvement Act (Pub. L. No. 101-604). As this applies to air transportation, this will not apply to transit agencies.
5. **Information Circulars:** A type of document within the DHS (formerly FAA) or DOT security bulletin process, the Information Circular was created to comply with the Aviation Security Improvement Act (Pub. L. No. 101-604). As this applies to air transportation, this will not apply to transit agencies.
6. **Performance Specifications:** The performance specifications of mechanical and electronic devices, including communications devices, used in the process of carrying out or complying with the transportation security requirements of federal law are designated as SSI. Only those portions of the specifications relating to the specific safety or security issue are SSI, however. Redacted versions, with the SSI portions removed, may be released to the public. For transit agencies, possessing performance specifications does not denote the creation of an SSI program and should not be marked as such.
7. **Security Inspection or Investigation Information:** Any inspection and/or investigatory information of an alleged violation of federal transportation security law is to be considered SSI and inspections and/or investigatory information of other security related issues should be considered for designation as SSI, as long as the purpose of the designation is not to prevent the proper disclosure of negligence, malfeasance, waste, fraud or abuse to the general public. For transit agencies, possessing security inspection or investigation information does not require the creation of an SSI program, and the information should not be marked as such.
8. **Security Measures:** All documents pertaining to the security measures taken by a transit agency are potentially considered SSI and thus are exempt from public disclosure. Examples of this would be the exact locations of security cameras, chemical detectors, patrol assignments of security staff and other such security measures. For transit agencies, possessing security measure information does not require the creation of an SSI program, and the information should not be marked as such.
9. **Security Screening Information:** This category deals with the screening procedures, information and materials used by the TSA as a part of the security procedures at U.S. airports. This will not apply to transit agencies.

[15] The SSI aspects of a security plan can be placed in an appendix. That way, if the appendix is extracted or redacted from the document, the remainder of the plan can be distributed to a wider audience as it will no longer contain SSI.

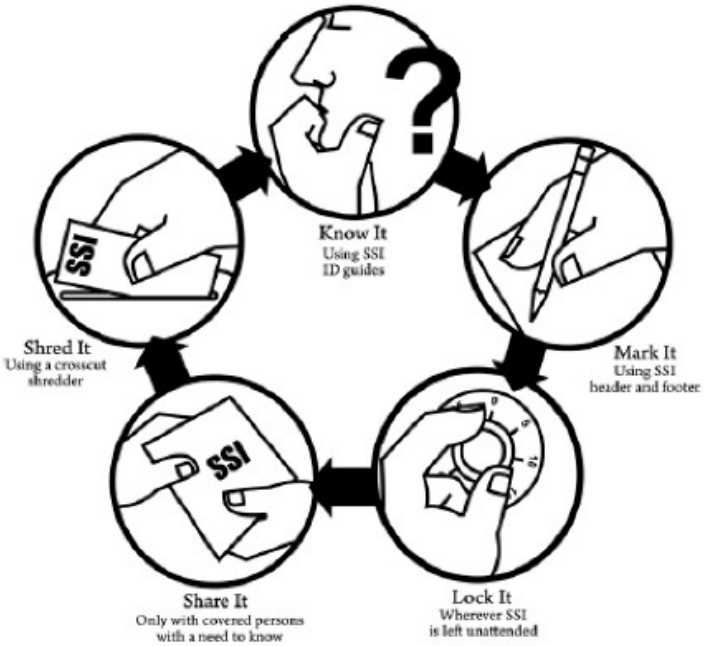
10. **Security Training Materials:** Training materials on security matters are to be considered SSI and thus exempt from disclosure. Depending on the contents of training exercises, this may even include the SSI training for covered persons in an agency. For transit agencies, possessing security training materials does not require the creation of an SSI program, and the information should not be marked as such.
11. **Identifying Information of Certain Transportation Security Personnel:** The identifying information of certain transportation security personnel, most notably air marshals, is to be considered SSI. In addition, confidential personnel files, medical files, or other files for transportation security personnel may also be considered SSI depending on the circumstances. For transit agencies, possessing identifying information of certain transportation security personnel does not require the creation of an SSI program, and the information should not be marked as such.
12. **Critical Aviation, Maritime, or Rail Infrastructure Asset Information:** "Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security," if the list is either created by DHS/DOT or is created by an agency for the submission to DHS/DOT. This will not apply to transit agencies.
13. **Systems Security Information:** Any information related to operational or administrative data systems that have been determined to be critical to aviation, maritime, or rail transportation safety or security, "including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems." For transit agencies, possessing systems security information does not require the creation of an SSI program, and the information should not be marked as such.
14. **Confidential Business Information:** All solicited or unsolicited business proposals, trade secrets and commercial or financial information that has been acquired by an agency in the course of compliance with federal safety and security laws and regulations is to be considered SSI as long as the source of the information does not routinely issue such information to the public. For transit agencies, possessing confidential business information does not require the creation of an SSI program, and the information should not be marked as such.
15. **Research and Development:** The regulation itself defines this best by saying: "Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results." For transit agencies, possessing research and development information does not require the creation of an SSI program, and the information should not be marked as such.
16. **Other Information:** TSA and DOT have the authority to designate as SSI, in writing, information not otherwise described in regulation.

Appendix D: SSI cover sheet

DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet



For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

Appendix E: SSI checklist

SSI regulation mandates requirements for marking, protecting, transmitting and destroying SSI. The following checklist was adapted from best practice guidance published by TSA.[16] Consult 49 CFR 1520 for the complete list of required actions.

Mark SSI:

✓	Task
	Confirm that all SSI is marked according to SSI regulation, including all protective markings and Distribution Limitation Statements.
	Apply an SSI cover sheet to all SSI materials, as applicable.

Protect SSI:

✓	Task
	Never share SSI with individuals who do not have a need to know.
	Lock up SSI materials, including notes, draft documents and electronic media, according to regulation.
	Report any unauthorized disclosures to your SSI program manager.
	Lock or turn off phones and computers containing SSI when not in your physical presence.
	Do not post SSI on any internet website. Post SSI on intranet websites only with prior approval.
	Do not download SSI to your personal device or to computers with peer-to-peer software.
	Do not take SSI home unless absolutely necessary and with approval from a supervisor.

Transmit SSI:

✓	Task
When emailing SSI…	
	Send as a password-protected attachment.
	Send password separately from the original message and without identifying information.
	Ensure that passwords protecting SSI content abide by strong password guidelines.

[16] "Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors" (https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf)

✓	Task
When discussing SSI…	
	Be conscious of your immediate surroundings, including people and devices.
	Protect verbal communications with the same heightened awareness as written or electronic SSI.
When physically delivering SSI…	
	Hand-deliver SSI directly to the intended recipient.
	Ensure that hand-delivered SSI is never left unattended.
	Consider using encrypted portable devices (e.g., thumb drives) to hand-deliver electronic SSI.
	Mail SSI by U.S. First-Class Mail or other traceable delivery methods using an opaque envelope or wrapping (the box or envelope should not be marked as SSI).
	Avoid faxing SSI. If unavoidable, verify the fax number and ensure that the intended recipient will be available to promptly retrieve the fax.

Destroy SSI:

✓	Task
	Destroy all SSI in your possession when no longer needed according to approved methods.
	Where available, place SSI in designated and clearly marked bins.
	Destroy electronic SSI using any method that will preclude recognition or reconstruction of content.

