SSI Training for Rail and Mass Transit Stakeholders

Information as of March 2024

Objectives

This briefing will focus on the following topics:

- The differences between Classified National Security Information and Sensitive Security Information (SSI)
- Which portions of the SSI Federal Regulation apply to Rail and Mass Transit stakeholders
- The proper means of marking and protecting SSI

Brief History of SSI

- SSI was developed pre-9/11
- Created in response to hijackings in the early 1970s
- The Air Transportation Security Act of 1974:
  - Required the Federal Aviation Administration (FAA) to establish a regulation for sharing sensitive information with airlines and airports
  - The FAA published the first SSI regulation in the Federal Register in 1976
- After 9/11, SSI applies to all modes of transportation.

Where SSI Fits

All information held by the Federal government falls into two categories:

- Classified National Security Information
  (Confidential, Secret, Top Secret)

  or

- Unclassified
  (SSI, For Official Use Only (FOUO), Public Information, etc.)

Classified Information

Information whose “unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security” (Executive Order 13526, Dec. 2009)

Example:
An U.S. Special Operations team conducts a raid, driven by intelligence, overseas. The identity of the “source” and “methods” that provided information that led to the raid would both be classified.

Unclassified Information Falls into Two Categories

- **Sensitive But Unclassified**

  A broad category that includes a federally regulated means of protecting information such as SSI and unregulated means of protecting information such as FOUO

- **Public Information**

  All Other Information

Sensitive Security Information

Information obtained or developed which, if released publicly, would be detrimental to transportation security.

Examples:

- Mass Transit Operator Security Program
- Baseline Assessment for Security Enhancement (BASE)
- TSA Intelligence Products (marked as SSI)

For Official Use Only

Information not protected by regulation that could adversely affect a Federal program if publicly released without authorization (DHS Management Directive 11042.1).

Example*:*

Federal building security plans

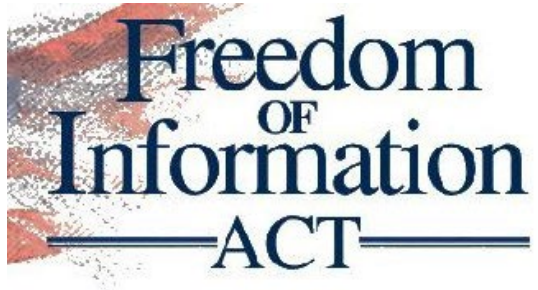
What are the Differences?

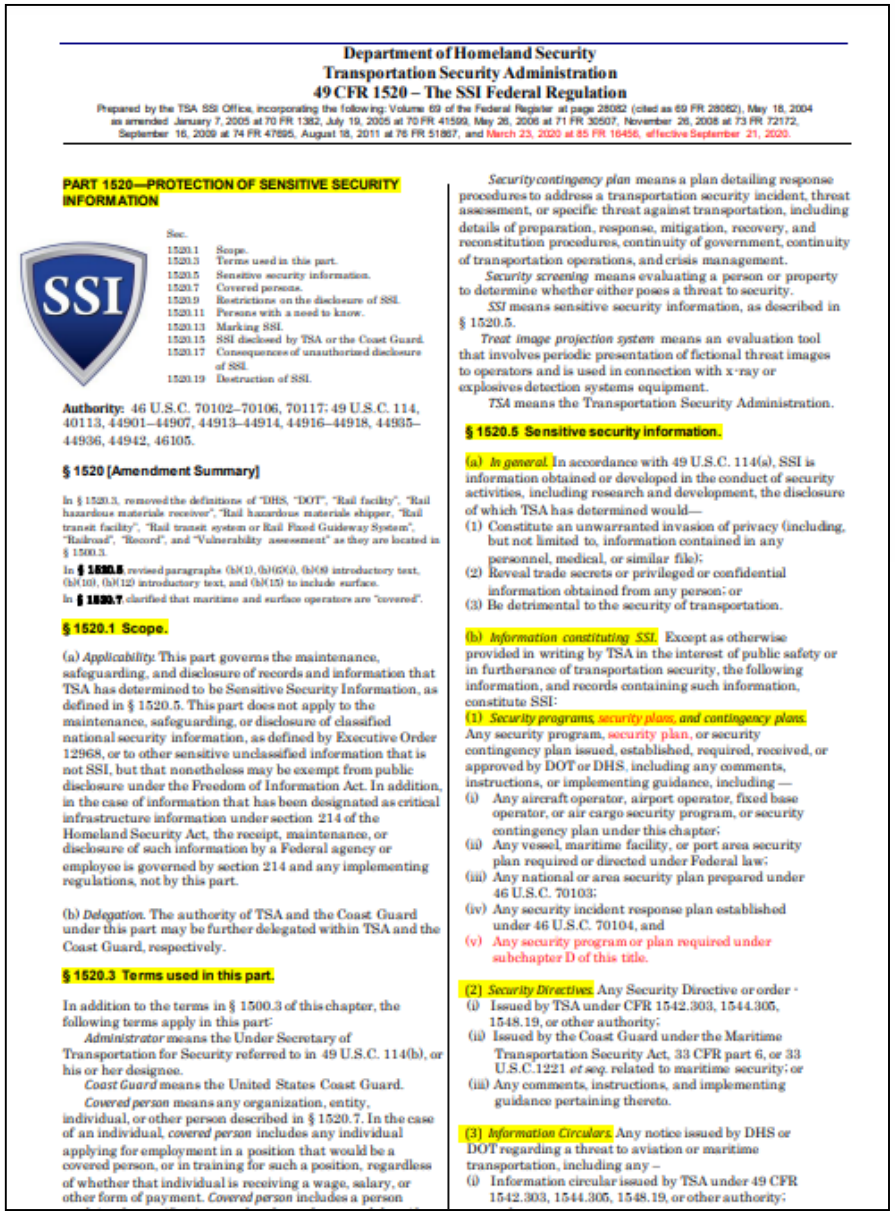
FOUO and SSI are categories of Sensitive But Unclassified information, but:

- SSI is based on U.S. law and protected by a Federal regulation; FOUO is not
- SSI protects information related to transportation security; FOUO has no subject matter limitations
- Unauthorized SSI disclosure may result in a civil penalty; FOUO breaches cannot

What are the Differences (cont'd)?

- In litigation, SSI has stronger protection from court-ordered production requests while documents marked only as FOUO have little or no protection at all
- SSI protected from public release under a Freedom of Information Act (FOIA) request; FOUO may be either protected or released under FOIA
- Documents that contain SSI must be marked as SSI – not as FOUO. When information is pulled from reports marked FOUO and SSI, the new report must be marked as SSI – Not FOUO/SSI





Department of Homeland Security
Transportation Security Administration
49 CFR 1520 – The SSI Federal Regulation

Prepared by the TSA SSI Office, incorporating the following: Volume 69 of the Federal Register at page 28082 (cited as 69 FR 28082), May 18, 2004 as amended January 7, 2005 at 70 FR 1382, July 19, 2005 at 70 FR 41599, May 26, 2006 at 71 FR 30507, November 26, 2008 at 73 FR 72172, September 16, 2009 at 74 FR 47695, August 18, 2011 at 76 FR 51867, and March 23, 2020 at 85 FR 16456, effective September 21, 2020.

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.
1520.1 Scope.
1520.3 Terms used in this part.
1520.5 Sensitive security information.
1520.7 Covered persons.
1520.9 Restrictions on the disclosure of SSI.
1520.11 Persons with a need to know.
1520.13 Marking SSI.
1520.15 SSI disclosed by TSA or the Coast Guard.
1520.17 Consequences of unauthorized disclosure of SSI.
1520.19 Destruction of SSI.

Authority: 46 U.S.C. 70102–70106, 70117; 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

§ 1520 [Amendment Summary]

In § 1520.3, removed the definitions of "DHS, "DOT", "Rail facility", "Rail hazardous materials receiver", "Rail hazardous materials shipper, "Rail transit facility", "Rail transit system or Rail Fixed Guideway System", "Railroad", "Record", and "Vulnerability assessment" as they are located in § 1500.3.

In **§ 1520.5** revised paragraphs (b)(1), (b)(6)(i), (b)(8) introductory text, (b)(10), (b)(12) introductory text, and (b)(15) to include surface.

In **§ 1520.7** clarified that maritime and surface operators are "covered".

§ 1520.1 Scope.

(a) *Applicability.* This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in § 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation.* The authority of TSA and the Coast Guard under this part may be further delegated within TSA and the Coast Guard, respectively.

§ 1520.3 Terms used in this part.

In addition to the terms in § 1500.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in § 1520.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in § 1520.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

§ 1520.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which 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.

(b) *Information constituting SSI.* Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:
(1) *Security programs, security plans, and contingency plans.* Any security program, security plan, or security contingency plan issued, established, required, received, or approved by DOT or DHS, including any comments, instructions, or implementing guidance, including —
(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;
(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;
(iii) Any national or area security plan prepared under 46 U.S.C. 70103;
(iv) Any security incident response plan established under 46 U.S.C. 70104, and
(v) Any security program or plan required under subchapter D of this title.

(2) *Security Directives.* Any Security Directive or order -
(i) Issued by TSA under CFR 1542.303, 1544.305, 1548.19, or other authority;
(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C.1221 *et seq.* related to maritime security; or
(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any –
(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

Focus on the SSI Federal Regulation (49 CFR Part 1520)

Other Ways To Think About SSI

Another way of thinking about SSI is would this information assist an adversary who is planning an attack against a transportation system?

How *useful* would the information be to terrorists?

How *detailed* is it?

Has DHS *officially released* it in the past?

Is it *obvious*?

Is it still *current*?

How Do We Know Its SSI?

In order for information to be SSI, the information must be related to transportation security, its release must be detrimental, and it must fall under the one of the 16 categories of SSI defined by the Federal Regulation (49 CFR Part 1520.5(b)).

This training will discuss the relevant categories that apply to Rail and Mass Transit stakeholders.

Category 1

(1) <u>Security Programs, Security Plans, and Contingency Plans</u> – Any security plan or security contingency plan issued, established, required, received or approved by DHS or DOT…

<u>Examples of records protected under this category:</u>

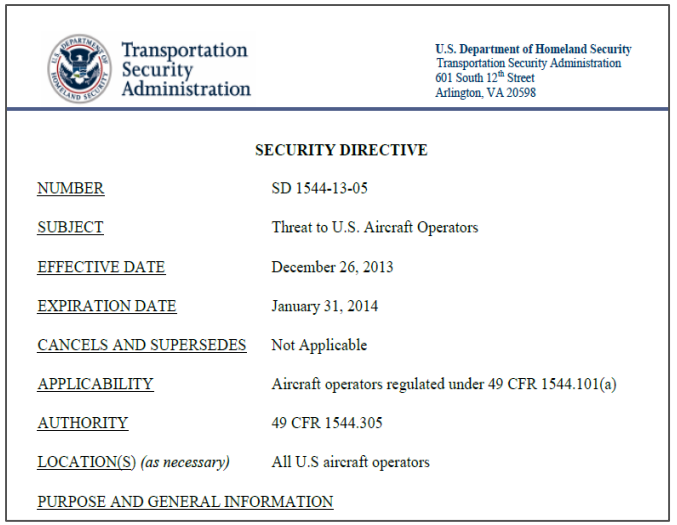
- Security plan for Rail Operator
- Security plan for Mass Transit Operator

Category 2

(2) Security Directive – Any Security Directive or order issued by TSA

Examples of records protected under this category:

TSA had issued Security Directives (SDs) to the Rail Industry. Not all were marked as SSI This was very deliberate. On the whole, SDs are usually marked as SSI.



Transportation Security Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

SECURITY DIRECTIVE

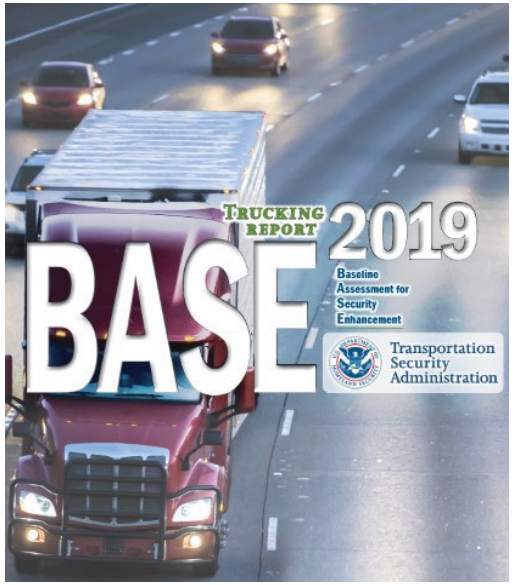
NUMBER	SD 1544-13-05
SUBJECT	Threat to U.S. Aircraft Operators
EFFECTIVE DATE	December 26, 2013
EXPIRATION DATE	January 31, 2014
CANCELS AND SUPERSEDES	Not Applicable
APPLICABILITY	Aircraft operators regulated under 49 CFR 1544.101(a)
AUTHORITY	49 CFR 1544.305
LOCATION(S) *(as necessary)*	All U.S aircraft operators
PURPOSE AND GENERAL INFORMATION	

Category 5

(5) Vulnerability Assessments– Any vulnerability assessment directed, created, held, funded or approved by DHS or DOT…

Examples of records protected under this category:

- Vulnerability assessment created by Rail companies and shared with TSA
- Baseline Assessment for Security Enhancement (BASE) conducted by TSA



Category 6

(6) Security Inspection or Investigative Information – Reports of inspections or investigations that could reveal a security vulnerability

Examples of records protected under this category:

Raw data and reports generated related to the transfer of rail hazmat cars between rail companies

Category 7

(7) Threat Information – Information held by the government concerning threats to *any* mode of transportation including cyber

Examples of records protected under this category:

TSA Intelligence Products marked as SSI.
Note: DHS/TSA Intelligence Products are not always marked as SSI. This is very deliberate on our part.

Categories 8 and 10

(8) Security measures – Specific details of transportation security measures including:

(i) Security measures or protocols recommended by the Federal government including cyber security measures

(10) Security Training Materials – Records created or obtained for training persons to carry out security measures

Categories 11-12

(11) Identifying Information of Certain Security Personnel –

(i) Lists of names that identify persons as –

(A) Having an unescorted access to a secure or restricted areas of a rail secure area (i.e., list of personnel who are assigned a Transportation Worker Identification Credential (TWIC card) at a particular facility)

(12) Critical Transportation Infrastructure Asset Information – Any list identifying systems or assets, whether physical or virtual, so vital to surface transportation that the incapacity or destruction of such assets would have a debilitating impact on transportation security if the list is

(i) Prepared by DHS or DOT; or

(ii) Prepared by as State or Local government and submitted to DHS/DOT

Categories 15 - 16

(15) Research and Development – Research results that were approved, accepted, funded, recommended or directed by DHS/DOT

(16) Other Information – The TSA Administrator (or their designee) can determine information to be SSI that is not otherwise defined in 1520.5(b)(1) – (15)

Note: (16) is rarely used.

Common Rail and Mass Transit Information That is SSI

- Rail Operators Security Programs
- Mass Transit Security Programs
- TSA Security Directives (SDs) marked as SSI
- Vulnerability Assessments of systems or facilities
- Raw data and reports related to the transfer of hazmat rail cars
- Baseline Assessment for Security Enhancement (BASE) conducted by TSA
- Reports of inspections or investigations that could reveal a security vulnerability
- TSA Security Action Items
- TSA Security Guidelines and Annexes
- TSA Intelligence Products marked as SSI

Note – this is not an all inclusive list.

What information is NOT SSI?

- Safety information is not SSI
- Fire Evacuation Plans are not SSI
- Construction Plans are not SSI
- Training materials for employees on safety measures are not SSI
- Safety inspections of infrastructure are not SSI

Covered Persons

According to the SSI Federal Regulation, covered persons may access SSI. This includes airport and airline personnel, maritime operators, rail, pipeline and surface operators, Federal and state personnel, among others.



Persons With a Need to Know

Covered persons have a “need to know” SSI if access to information is necessary for the performance of, training for, or managing of personnel’s official duties. DHS or DOT may limit access to specific SSI to certain employees or covered persons.

Example:

A Mass Transit Operator does not need access to the flying schedules of Federal Air Marshals.

Requests from the Media for SSI

Under the SSI Federal Regulation, members of the news media are not covered persons and do not have a “need to know” SSI.

SSI and Cyber Security

Information Related to Cybersecurity That May Be SSI

Why Should SSI be Protected? (Part I)

- SSI can protect information that an adversary can use to compromise sensitive transportation Information Technology (IT) or Operational Technology systems (OT).
  - Not protecting or otherwise mishandling this information would put transportation security at risk because it could cause vulnerabilities and allow someone to gain access to or manipulate the system.
- SSI may be used to protect both internal (i.e., for company use) and external (e.g., for reporting and collaborating) documentation.

Information Related to Cybersecurity That May Be SSI (cont.)

Why Should SSI be Protected? (Part II)

- SSI protects a variety of information related to these critical cyber systems as another layer of protection.
- Critical Cyber Systems/Critical Systems may include systems which:

  1. could be used to compromise or exploit transportation safety or security or
  2. contain SSI as it is a critical measure used to protect information essential to transportation security.

- Lists of Critical Cyber Systems/Critical Systems may be marked and protected as SSI.

Planning and Design Documents

Planning and Design Documents (often contain exploitable data such as):

- Security documentation
- System security plans
- IT network design documents
- System configurations
- Ports, Protocols, and Services (PPS)
- Firewall rules
- Intrusion Detection Systems (IDS) rules
- Security auditing triggers
- Contingency plans/Cybersecurity Contingency Response Plans

Note – List not all-inclusive

Compliance Documentation

Compliance Documentation (related to critical cyber systems/critical systems):

- Threats against stakeholders reported to the Federal government (to the extent it is not classified)
- Documents revealing vulnerabilities
- System assessments and risk assessments
- System auditing
- Regulatory oversight reports
- Remediation Plans
- Incident Response Plans
- Requests for Alternative Measures
- TSA response to Alternative Measures requests

Note – List not all-inclusive

System Access and Control Information

System Access and Control Information (which could be used to compromise a system)

- User names
- IP addresses (non-published routable)
- Computer names
- Domain names
- Vulnerabilities
- Passwords
- Password hashes and salts
- Private keys
- Specific software and firmware patch levels

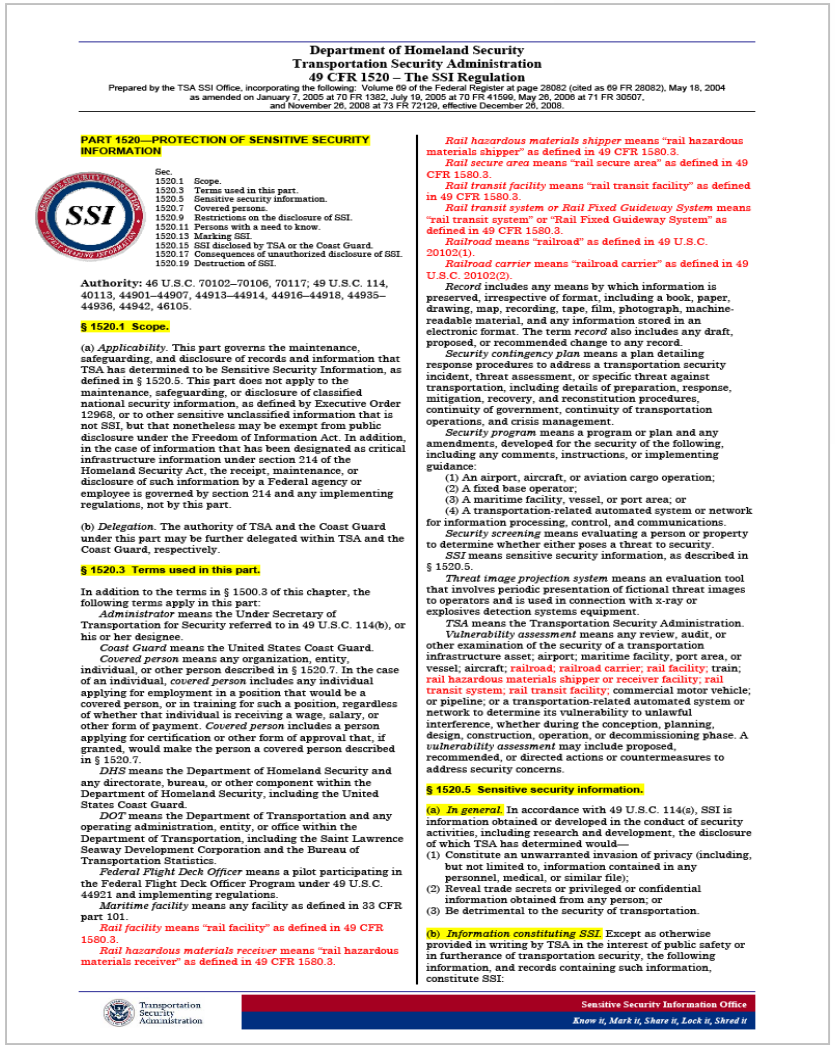
Note – List not all-inclusive

Cyber Security Incident Intrusion Information

Cyber Security Incident Intrusion Information

- Impacted IP addresses/ports
- Malicious IP addresses
- Malicious domains
- Malware hashes and/or samples
- Abuse of legitimate software or accounts

Note – List not all-inclusive



Department of Homeland Security
Transportation Security Administration
49 CFR 1520 – The SSI Regulation

Prepared by the TSA SSI Office, incorporating the following: Volume 69 of the Federal Register at page 28082 (cited as 69 FR 28082), May 18, 2004 as amended on January 7, 2005 at 70 FR 1382, July 19, 2005 at 70 FR 41599, May 26, 2006 at 71 FR 30507, and November 26, 2008 at 73 FR 72129, effective December 26, 2008.

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.
1520.1 Scope.
1520.3 Terms used in this part.
1520.5 Sensitive security information.
1520.7 Covered persons.
1520.9 Restrictions on the disclosure of SSI.
1520.11 Persons with a need to know.
1520.13 Marking SSI.
1520.15 SSI disclosed by TSA or the Coast Guard.
1520.17 Consequences of unauthorized disclosure of SSI.
1520.19 Destruction of SSI.

Authority: 46 U.S.C. 70102–70106, 70117; 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

§ 1520.1 Scope.

(a) *Applicability.* This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in § 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation.* The authority of TSA and the Coast Guard under this part may be further delegated within TSA and the Coast Guard, respectively.

§ 1520.3 Terms used in this part.

In addition to the terms in § 1500.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person described in § 1520.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in § 1520.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Rail facility means "rail facility" as defined in 49 CFR 1580.3.

Rail hazardous materials receiver means "rail hazardous materials receiver" as defined in 49 CFR 1580.3.

Rail hazardous materials shipper means "rail hazardous materials shipper" as defined in 49 CFR 1580.3.

Rail secure area means "rail secure area" as defined in 49 CFR 1580.3.

Rail transit facility means "rail transit facility" as defined in 49 CFR 1580.3.

Rail transit system or Rail Fixed Guideway System means "rail transit system" or "Rail Fixed Guideway System" as defined in 49 CFR 1580.3.

Railroad means "railroad" as defined in 49 U.S.C. 20102(1).

Railroad carrier means "railroad carrier" as defined in 49 U.S.C. 20102(2).

Record 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. The term *record* also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments, developed for the security of the following, including any comments, instructions, or implementing guidance:
(1) An airport, aircraft, or aviation cargo operation;
(2) A fixed base operator;
(3) A maritime facility, vessel, or port area; or
(4) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in § 1520.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, or vessel; aircraft; railroad; railroad carrier; rail facility; train; rail hazardous materials shipper or receiver facility; rail transit system; rail transit facility; commercial motor vehicle; or pipeline; or a transportation-related automated system or network to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A *vulnerability assessment* may include proposed, recommended, or directed actions or countermeasures to address security concerns.

§ 1520.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which 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.

(b) *Information constituting SSI.* Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

Transportation Security Administration

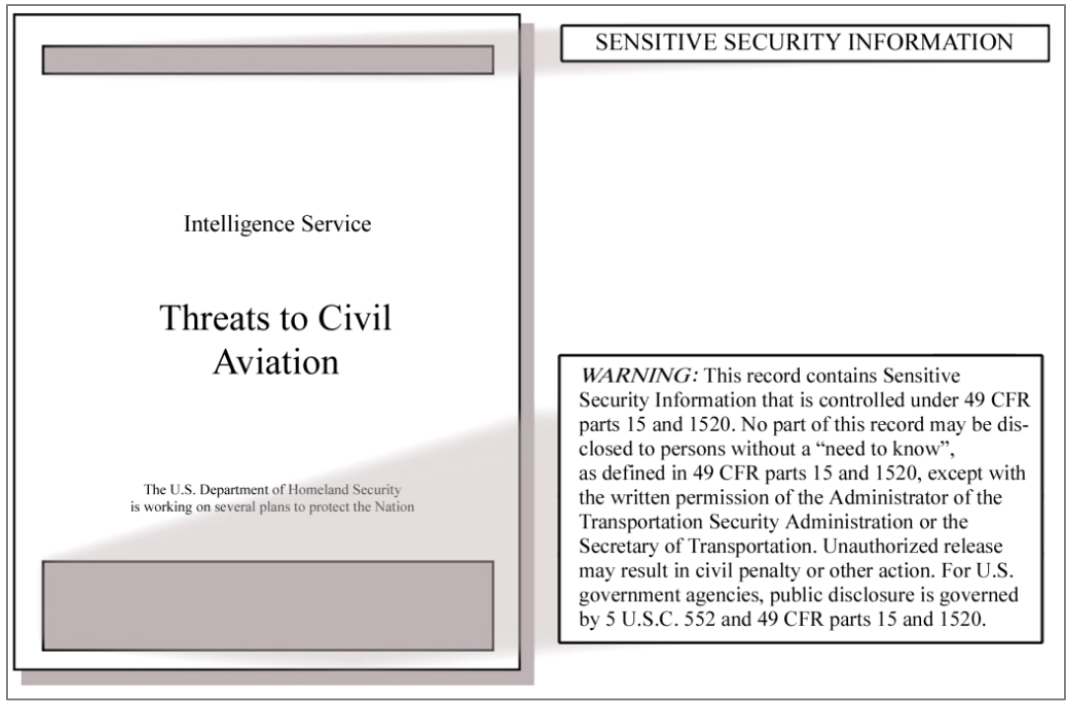
Sensitive Security Information Office
Know it, Mark it, Share it, Lock it, Shred it

SSI Federal Regulation Outlines Procedures for Marking and Handling SSI

Regulatory Requirement
SSI – Protective Marking

Each page of the SSI record must include an SSI header and footer.

Even if there is only one sentence containing SSI in a 50-page document, every page must have an SSI header and footer.



Regulatory Requirement
SSI – Protective Marking

- The SSI footer informs the viewer that the record must be protected from unauthorized disclosure.
- No modification of the SSI Footer is authorized.

"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."

Who Can Mark Records as SSI?

Stakeholders are permitted to mark information as SSI as long as they believe the record meets specific criteria under the SSI Federal Regulation:

- It is related to transportation security (not safety);
- Its release would be detrimental to transportation security (i.e., an adversary could use the information to plan an attack against the transportation system); and
- It falls under one of the 16 SSI Categories that are listed in the slides above.

SSI Records

It is important to remember that SSI is information which should be marked and protected in all forms of communication. This includes emails, Word documents, presentations, training, etc.

Storing SSI: Lock it Up!!!!

When not actually working with an SSI record (lunch break, end of the day, etc.), store the SSI record in a locked desk drawer or in a locked room to prevent unauthorized access by persons who do not have a “need to know.”

<u>ALL RECIPIENTS OF SSI ARE MANDATED TO LOCK IT UP!!!</u>

Protecting Electronic Data

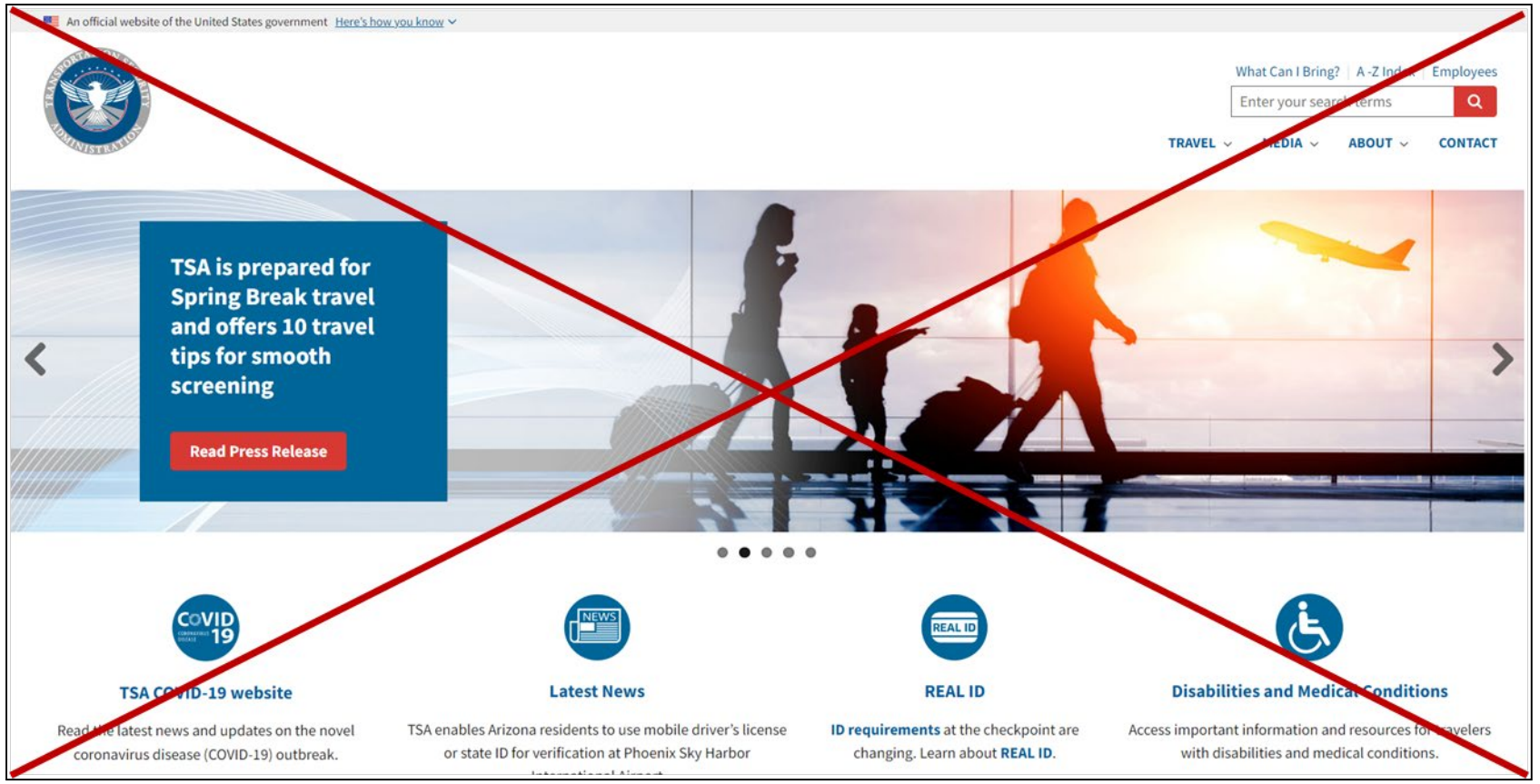
The SSI Regulation instructs:

"*Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure*" (49 CFR §1520.9(a)(1)).

Safeguarding methods may include:

- logging off from or locking unattended computers,
- applying encryption, and/or
- physically restricting access to electronic devices such as USB flash drives or other portable devices.

Posting SSI: Never Post SSI on the Internet



Duty to Report Unauthorized Disclosure of SSI

The SSI Federal Regulation (49 CFR §1520.9(c)) states “when a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA...” *

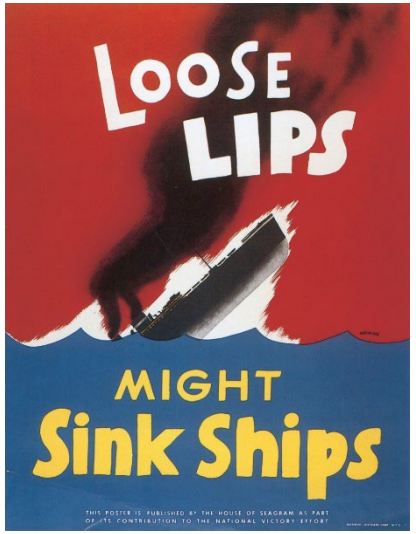
- This usually involves lost paper copies of SSI or SSI available on the Internet.
- Stakeholders may contact their TSA point of contact or the TSA SSI Program office at SSI@tsa.dhs.gov.

Discussing SSI in Public Areas is Inappropriate

Personnel must be very careful when discussing SSI in public areas.

You never know who is listening and not everyone has a “need to know” the information.

Remember: Adversaries do not care how they receive SSI as long as they get the information they need to plan an attack.



Consequences of Unauthorized Disclosure of SSI

- Lost money – TSA can impose a civil penalty with amounts into the tens of thousands of dollars per offense against covered persons and companies

- Lost jobs – for Federal employees, appropriate personnel action up to termination

- Lost contract – TSA can decide whether to end a contract with a Federal vendor whose employees did not properly protect the SSI entrusted to their care

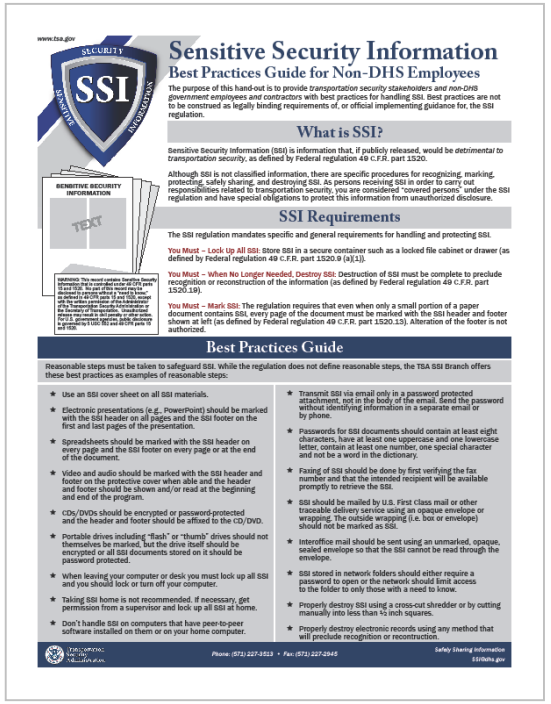
“Best Practices” for Non-DHS Employees to Protect SSI

Best Practices for Non-DHS Personnel

DHS stakeholders (i.e., regulated entities) and other covered parties are mandated under the SSI regulation to take "reasonable steps" to prevent unauthorized disclosure of SSI.

The next set of slides describes "Best Practices" that stakeholders may use in handling and protecting SSI.

These "Best Practices" are based on policies and procedures developed for DHS personnel to protect SSI.



www.tsa.gov

Sensitive Security Information

Best Practices Guide for Non-DHS Employees

The purpose of this hand-out is to provide *transportation security stakeholders and non-DHS government employees and contractors* with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be *detrimental to transportation security*, as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI. As persons receiving SSI in order to carry out responsibilities related to transportation security, you are considered "covered persons" under the SSI regulation and have special obligations to protect this information from unauthorized disclosure.

SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

You Must – Lock Up All SSI: Store SSI in a secure container such as a locked file cabinet or drawer (as defined by Federal regulation 49 C.F.R. part 1520.9 (a)(1)).

You Must – When No Longer Needed, Destroy SSI: Destruction of SSI must be complete to preclude recognition or reconstruction of the information (as defined by Federal regulation 49 C.F.R. part 1520.19).

You Must – Mark SSI: The regulation requires that even when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown at left (as defined by Federal regulation 49 C.F.R. part 1520.13). Alteration of the footer is not authorized.

Best Practices Guide

Reasonable steps must be taken to safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Branch offers these best practices as examples of reasonable steps:

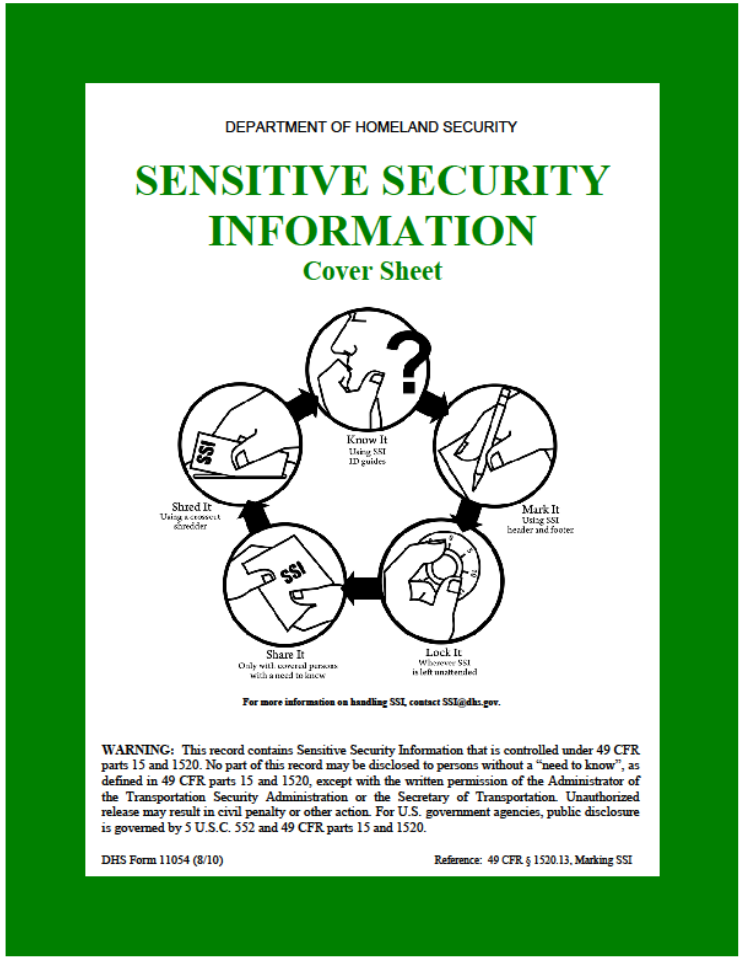
- Use an SSI cover sheet on all SSI materials.
- Electronic presentations (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation.
- Spreadsheets should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document.
- Video and audio should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program.
- CDs/DVDs should be encrypted or password-protected and the header and footer should be affixed to the CD/DVD.
- Portable drives including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all SSI documents stored on it should be password protected.
- When leaving your computer or desk you must lock up all SSI and you should lock or turn off your computer.
- Taking SSI home is not recommended. If necessary, get permission from a supervisor and lock up all SSI at home.
- Don't handle SSI on computers that have peer-to-peer software installed on them or on your home computer.
- Transmit SSI via email only in a password protected attachment, not in the body of the email. Send the password without identifying information in a separate email or by phone.
- Passwords for SSI documents should contain at least eight characters, have at least one uppercase and one lowercase letter, contain at least one number, one special character and not be a word in the dictionary.
- Faxing of SSI should be done by first verifying the fax number and that the intended recipient will be available promptly to retrieve the SSI.
- SSI should be mailed by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping. The outside wrapping (i.e. box or envelope) should not be marked as SSI.
- Interoffice mail should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope.
- SSI stored in network folders should either require a password to open or the network should limit access to the folder to only those with a need to know.
- Properly destroy SSI using a cross-cut shredder or by cutting manually into less than ½ inch squares.
- Properly destroy electronic records using any method that will preclude recognition or recontruction.

Phone: (571) 227-3513 • Fax: (571) 227-2945

Safely Sharing Information

SSI@tsa.gov

Best Practices – 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

The SSI Cover sheet is NOT required by the SSI Federal Regulation but it is recommended to place everyone on notice they are dealing with SSI and can be added as needed.

Best Practices – Sharing SSI in Email

SSI information transmitted by e-mail should be *encrypted* or sent in a separate password-protected record and not in the body of an e-mail. Passwords should be sent separately, and should:

- Have eight-character minimum length
- Have at least one upper-case and one lower-case letter
- Contain at least one number
- Contain at least one symbol (e.g., @#$%?!)
- Not be a word in the dictionary or a portion of the file name

Best Practices – Managing Sensitive Data in Webinars

Taking the following steps will help minimize the risk of unauthorized disclosure of SSI.

- Verify that all attendees of the meeting are covered persons with a the SSI to be presented
- Manage policies to ensure only members from your organization or desired group can attend
- Enable “waiting room” features to see and vet attendees before granting them access
- Lock the event once all intended attendees have joined

Best Practices – Managing Sensitive Data in Webinars (cont.)

- Ensure that the host can manually admit and remove attendees
- Be mindful of how (and to whom) you disseminate invitation links
- Consider sensitivity of data before exposing it via screen share or uploading it during video conferences
- Do not discuss information that you would not discuss over regular telephone lines

Best Practices - No SSI on Personally Owned Electronic Devices

SSI should not be stored, sent to, or printed to personal devices including home, public, or personal:

- Computers or tablets
- Fax machines
- Printer or copy machines
- Smart phones
- Thumb drives, external drives, or disks
- Email accounts

Best Practices – Closing the Gaps

- Change default password to strong, complex passwords for your router and Wi-Fi network
- At a minimum, ensure your router is configured to use WPA2 or WPA3 wireless encryption
- Avoid using public hotspots and networks
- Only use secure video conferencing tools approved by your organization
- Use official company email when sending SSI
- Ensure that any virtual assistants (e.g., Alexa) will not pick up your conversations

Best Practices – Closing the Gaps (cont.)

Remember, while conducting business, be conscious of your surroundings:

- Do not work in locations where your computer screen may be visible to others
- Take measures to prevent eavesdropping, especially when discussing SSI

Best Practices - Traveling with SSI

- Laptops containing SSI should be kept with you to the maximum extent possible
- Avoid transporting laptops containing SSI in checked baggage
- Laptops containing SSI and any SSI paperwork should be kept locked and out of sight (e.g., trunk) when unattended in vehicles
- In hotel rooms, use hotel room safes for laptops containing SSI and any SSI paperwork

Best Practices – Destruction of SSI

The most common methods used to destroy SSI material include:

- Cross-cut shredders
- Contract with a shredding company
- Any method approved for the destruction for classified national security information

Frequently-Asked Questions

Q: How Do We Handle Requests for SSI Information?

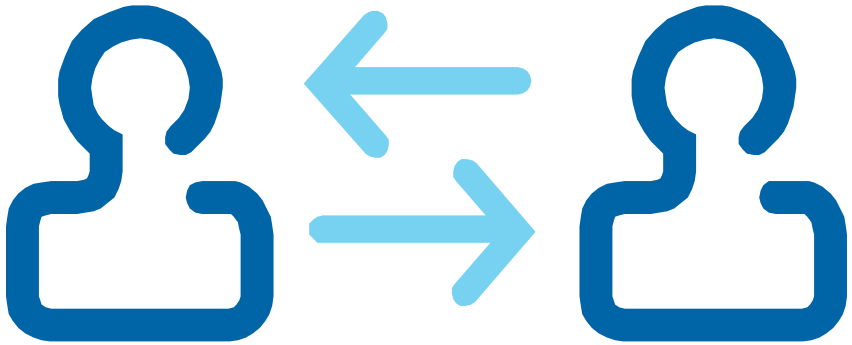
Answer: Request for SSI falls into two categories:

- Sharing
- Releasing

Sharing SSI

To share SSI is to provide a record that contains SSI to another covered person. The record is marked as SSI and remains SSI.

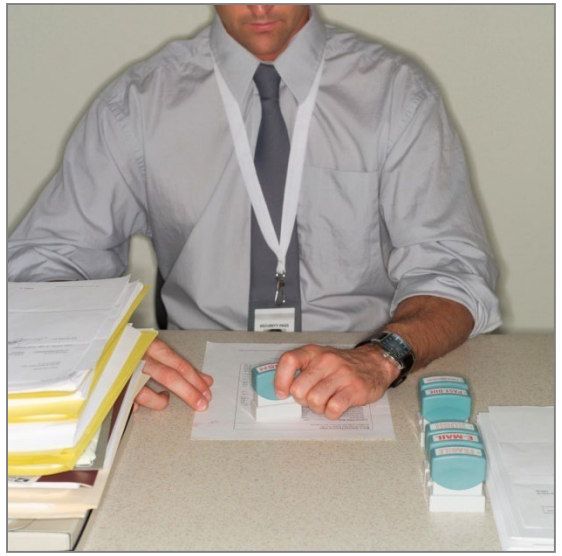
The covered person with a “need to know” is now obligated by the SSI Federal Regulation to protect the SSI record entrusted to their care.



Releasing Records

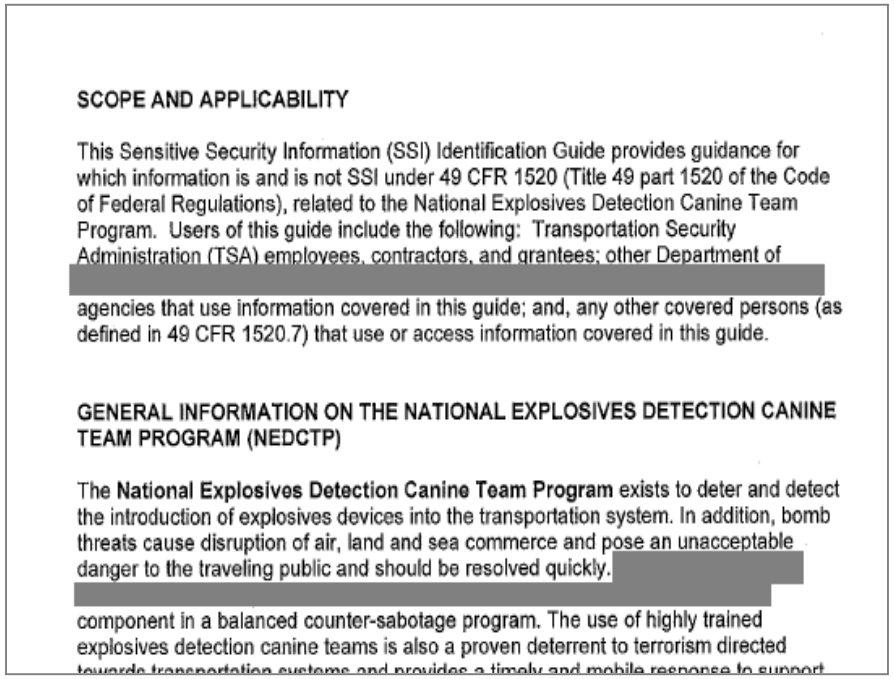
Prior to releasing records containing SSI to persons who are not authorized to access SSI under the SSI Federal Regulation, the SSI language must be removed/redacted by the TSA SSI Program office. The redacted record may be released to the general public.

The redacted record should have the SSI header and SSI footer removed or crossed out.



SSI Redactions

- SSI Records that are produced due to Freedom of Information Act (FOIA) requests, court-order production requests, or other requests are reviewed by the TSA SSI Program office.
- TSA then produces a redacted copy of the record with all of the SSI removed.



SCOPE AND APPLICABILITY

This Sensitive Security Information (SSI) Identification Guide provides guidance for which information is and is not SSI under 49 CFR 1520 (Title 49 part 1520 of the Code of Federal Regulations), related to the National Explosives Detection Canine Team Program. Users of this guide include the following: Transportation Security Administration (TSA) employees, contractors, and grantees; other Department of [redacted] agencies that use information covered in this guide; and, any other covered persons (as defined in 49 CFR 1520.7) that use or access information covered in this guide.

GENERAL INFORMATION ON THE NATIONAL EXPLOSIVES DETECTION CANINE TEAM PROGRAM (NEDCTP)

The **National Explosives Detection Canine Team Program** exists to deter and detect the introduction of explosives devices into the transportation system. In addition, bomb threats cause disruption of air, land and sea commerce and pose an unacceptable danger to the traveling public and should be resolved quickly. [redacted] component in a balanced counter-sabotage program. The use of highly trained explosives detection canine teams is also a proven deterrent to terrorism directed towards transportation systems and provides a timely and mobile response to support

Q: How Do We Get SSI Redacted before a Record is Released?

- The SSI Federal Regulation states that
  - "Except as otherwise provided in this section… records containing SSI are not available for public inspection or copying, nor does TSA… release such records to persons without a "need to know" (49 CFR § § 1520.15(a))
  - "(I)f a record contains both SSI and information that is not SSI, TSA…may disclose the record with the SSI redacted…" (49 CFR § 1520.15(b))
- TSA addresses these requirements by providing an official SSI Review process through its SSI Program office.

Q: *What about State Open Record Act Requests?*

- Similar to Federal Freedom of Information Act (FOIA), many state and local laws (e.g., “Sunshine” laws) provide citizens the right to access government records.
- While laws providing exemptions vary by state, 49 CFR § 1520.9(a)(3) requires that covered persons “Refer requests by other persons for SSI to TSA.”
- This requirement for referral includes requests for access to SSI made under State, local, tribal or territorial public information and related laws.
- SSI falls under the SS Federal Regulation, which preempts conflicting State, local, tribal and territorial law.

Q: *What about State Open Record Act Requests? (cont.)*

- Requests for TSA's own records made through State Open Records requests must be referred to TSA FOIA (FOIA@tsa.dhs.gov).
- Requests for records that may contain SSI belonging to the state or airport authority should be submitted for full SSI Review to the SSI Program office.
- While the SSI Program office will attempt to work within the law's time constraints, it is not always possible. Interim responses may be made to the requestor indicating the need for SSI Review by TSA.
- Requests may be submitted to TSA Field Counsel, local SSI Coordinators, or to the SSI Program office directly at SSI@tsa.dhs.gov.

Q: If we mark a Record as SSI, does that mean it's always SSI?

- All covered persons are permitted to mark information they believe is SSI, but it is possible it was over-marked.
- The TSA Administrator is authorized to determine whether information pertaining to transportation security constitutes SSI. That authority is delegated from the Administrator to the Chief of the SSI Program.
- Using this authority, the SSI Program determines what information is designated as SSI or not SSI within a record. The SSI Program is the final arbiter and authorized to make SSI determinations on both federal records and records produced by stakeholders.
- If necessary, the SSI Program will provided redacted versions (i.e., all of the SSI blacked out) for public consumption.

Q: Who Do We Contact for Additional Assistance?

- Additional SSI resources are posted to https://www.tsa.gov/for-industry/sensitive-security-information

- Questions may be directed to your TSA point of contact or TSA Policy, Plans and Engagement (PPE) representative at TSA-Surface@tsa.dhs.gov

- The SSI Program office is also available to answer questions about SSI and receive SSI Review Requests through its SSI Inbox at SSI@tsa.dhs.gov

Safely Sharing Information

SSI Program Office

Security and Administrative Services
Enterprise Support
Transportation Security Administration
6595 Springfield Center Drive, MS-31
Springfield, VA 20598-6031

E-Mail: SSI@tsa.dhs.gov


TRANSPORTATION SECURITY
ADMINISTRATION