U.S. Department of Homeland Security
Transportation Security Administration
Sensitive Security Information Program
Presents:

SSI Training for DHS Stakeholders
Everyone is Responsible for SSI!

Everyone is responsible for properly marking, handling, protecting, storing, and destroying SSI.
Objectives

By the end of this training, you will know the:

• Differences between Sensitive Security Information (SSI) and the following three types of information:
  1. Classified National Security
  2. For Official Use Only (FOUO)
  3. Law Enforcement Sensitive (LES)

• Requirements listed in the SSI Federal Regulation (49 CFR Part 1520), and

• “Best Practices” for safely sharing and protecting SSI
Brief History of SSI

• SSI was not developed post-9/11
• Created in response to hijackings occurring in the early 1970s

The *Air Transportation Security Act of 1974*:

• Required the FAA to establish regulation for sharing SSI with airlines and airports
• The FAA published the first regulation regarding SSI in the Federal Register in 1976

After 9/11, SSI applies to all modes of transportation
Classified Information vs. Sensitive Security Information (SSI)
All information held by the 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”*

Example:
A U.S. Special Operations team conducts a raid, driven by intelligence, on an al-Qa'ida compound on the Afghanistan border. The identity of the “source” of data and the information he provided would both be classified.

Unclassified Information Falls into Two Categories

- **Sensitive But Unclassified (SBU)**
  A broad category that includes a federally regulated means of protecting information such as *SSI* and unregulated means of protecting information such as *For Official Use Only (FOUO)* and *Law Enforcement Sensitive (LES)*

- **Public Information**
  All other information
Sensitive Security Information

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

Examples:

• No-Fly List and Selectee List
• Screening Standard Operating Procedures (SOPs) used by Transportation Security Officers (TSOs)
• Aircraft Operator Standard Security Program (AOSSP)
Information not protected by regulation that could adversely affect a Federal program if publicly released without authorization.

*Example:*

Federal building security plans

*Source: DHS Management Directive 11042.1*
Law Enforcement Sensitive (LES)

Documents marked LES are intended for official use only. No portion of the document should be:

- Released to the media or the general public
- Posted to or sent via non-secure Internet servers

Release of LES material could adversely affect or jeopardize investigative activities.*

* Source: FBI’s Web site

Example:

FBI Intelligence Bulletins
What are the differences?

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

- SSI is based on U.S. law and protected by a Federal regulation; FOUO and LES are not;

- SSI protects information related to transportation security; FOUO and LES have no subject matter limitations;

- Unauthorized SSI disclosure may result in a civil penalty; FOUO and LES breaches cannot
What Are the Differences? (cont.)

- Documents that contain SSI must be marked as SSI
- When information is pulled from reports marked Law Enforcement Sensitive (LES), For Official Use Only (FOUO), and SSI, the new report must be marked as SSI
Focus on SSI Regulation

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

PART 1520 – PROTECTION OF SENSITIVE SECURITY INFORMATION

1520.1 Scope

(a) This part provides a framework for the protection of sensitive security information (SSI) and sensitive counterintelligence information (SCII) as defined in 18 U.S.C. 3710 and 3711, respectively. This part applies to all departments and agencies of the Federal Government.

(b) The Secretary of Homeland Security and other designated officials shall ensure the implementation of the requirements of this part.

1520.2 Definitions

(a) The following definitions apply:

(1) Sensitive security information (SSI) means “sensitive security information” as defined in 49 U.S.C. 1520a.

(2) Sensitive counterintelligence information (SCII) means “sensitive counterintelligence information” as defined in 49 U.S.C. 1520a.

(3) Sensitive security information and sensitive counterintelligence information (SSI/SCII) means sensitive security information and sensitive counterintelligence information, as defined in 18 U.S.C. 3710 and 3711, respectively.

1520.3 The Department of Homeland Security

The Department of Homeland Security (DHS) is responsible for protecting the nation from terrorist attacks and natural disasters. DHS is also responsible for ensuring the safety and security of U.S. airports, seaports, and other transportation systems. DHS is headed by the Secretary of Homeland Security, who is appointed by the President and confirmed by the Senate.

1520.4 Protection of Sensitive Security Information

A. The Department of Homeland Security shall ensure the protection of SSI and SCII.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.

1520.5 Sensitive Security Information

A. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

E. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

1520.6 Sensitive Counterintelligence Information

A. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

E. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

1520.7 Protection of Sensitive Security Information

A. The Department of Homeland Security shall ensure the protection of SSI and SCII.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.

1520.8 Protection of Sensitive Counterintelligence Information

A. The Department of Homeland Security shall ensure the protection of SSI and SCII.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.

1520.9 Protection of Sensitive Security Information and Sensitive Counterintelligence Information

A. The Department of Homeland Security shall ensure the protection of SSI and SCII.

B. The Secretary of Homeland Security shall ensure that SSI and SCII are protected from unauthorized disclosure.

C. The Department of Homeland Security shall establish procedures for the handling of SSI and SCII.

D. The Department of Homeland Security shall ensure that SSI and SCII are protected from unauthorized access.
16 SSI Categories

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 each category and provide examples of information protected under that category.
16 SSI Categories (cont.)

(1) **Security Programs and Contingency Plans** – The Airport Security Program (ASP), Aircraft Operator Standard Security Program (AOSSP), or other modal security programs/plans

(2) **Security Directives (SDs)** – TSA sends out SDs to transportation stakeholders advising them of developing threats and provides security measures they must put into effect to counteract the security threat.

(3) **Information Circular (ICs)** – TSA sends out ICs to stakeholder advising them of threats to transportation (rarely used).
16 SSI Categories (cont.)

(4) **Performance Specifications** – Specifications for any checkpoint or checked baggage screening equipment deployed at airports (including specs for communications equipment)

(5) **Vulnerability Assessments** – Assessments for or by DHS/DOT for any mode of transportation including the vulnerability of airports to a shoulder-fired missile attack
16 SSI Categories (cont.)

(6) Security Inspection or Investigative Information
Unplanned (incident or violation) inspection or investigation that could reveal a security vulnerability may include TSA incident reports, Transportation Security Inspectors (TSIs) PARIS reports, and Federal Air Marshal (FAM) incident reports

(7) Threat Information – Information held by the government concerning threats to any mode of transportation
16 SSI Categories (cont.)

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

(i) Security measures or protocols recommended by the Federal government (airport access control measures)

(ii) Information concerning the deployments, numbers, and operations of FAMS

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers (FFDOs)
(9) Security Screening Information –

(i) Standard Operating Procedures (SOPs) to screen passengers, their baggage, cargo and U.S. mail

(ii) Names on the No-Fly List and Selectee List

(iv) Any security screener test and scores of such tests

(v) Performance data from screening equipment includes info related to covert testing

(vi) Electronic images shown on any screening equipment monitor
16 SSI Categories (cont.)

(10) **Security Training Materials** – Records created or obtained for purposes of training personnel

(11) **Identifying Information of Certain Security Personnel** –

(i) Lists of names that identify persons as –

(A) Having an airport SIDA badge

(B) Complete list of all TSOs at an airport

(D) Holding a position as Federal Air Marshal

(ii) name that identifies a person as current, former, or applicant of Federal Flight Deck Officer
16 SSI Categories (cont.)

(12) Critical Aviation, Maritime or Rail Infrastructure Asset Information – List prepared by DHS or DOT identifying assets so vital to transportation that incapacity or destruction would have a debilitating impact on transportation security

(13) Systems Security Information – Security plans or vulnerability assessment of IT systems for vital systems

(14) Confidential Business Information – Proprietary Business Information (rarely used)
16 SSI Categories (cont.)

(15) **Research and Development** – Research results that were funded or directed by DHS/DOT

(16) **Other Information** – The TSA Administrator (and only the TSA Administrator) can determine information to be SSI that is not otherwise defined in 1520.5(b)(1) – (15) *(rarely used)*
Covered Persons

According to the SSI Federal Regulation, covered persons may access SSI. This includes airport and airline officials, maritime operators, Federal employees, contractors, and grantees, 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 official duties. DHS or DOT may limit access to specific SSI to certain employees or covered persons.

Example:

A screening equipment vendor does not need access to the FAM schedules.
Requests from the Media for SSI

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

Requests for SSI from the media should be forwarded to TSA for review.
Proper Marking and Handling of SSI

MARK IT
Using the SSI Header and Footer

SHARE IT
Only With Covered Persons With a Need to Know

LOCK IT
Whenever SSI is Left Unattended

SHRED IT
Using a Cross-cut Shredder

KNOW IT
Using SSI ID Guides

For more information on Safely Sharing Information: SSI@DHS.GOV

Poster created by LTSO David Riel - DTW
SSI – Protective Marking

Any person who creates a record containing SSI 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.
SSI Footer

The SSI footer informs the viewer that the record must be protected from unauthorized disclosure.

“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.”
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.’

ALL RECIPIENTS OF SSI ARE MANDATED TO LOCK IT UP!!!
“Best Practices” for DHS Stakeholders in Protecting SSI
Other than locking SSI in a locked drawer or cabinet, which is a requirement, DHS stakeholders and other non-DHS 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.
SSI information transmitted by e-mail should be in a separate password-protected record, and not in the body of an e-mail. Passwords should be sent separately, and should:

- Be at least eight characters in length
- Have at least one letter capitalized
- Contain at least one number and one special character
- Not be a word in the dictionary
“Best Practices for Stakeholders”
Web Posting SSI

TSA does NOT post SSI on its public website or the agency-wide Intranet portal areas that have open access for all TSA employees and contractors.
“Best Practices for Stakeholders”
SSI Transmission: Facsimile

The sender of faxed SSI should confirm that the fax number of the recipient is current and valid and the intended recipient can promptly retrieve and secure the document.
“Best Practices for Stakeholders”

Mailing SSI

SSI may be mailed to covered persons via U.S. Postal Service (First Class only) or reliable commercial delivery services (FedEx, UPS, etc.).

When using Interoffice Mail to send SSI to covered persons, SSI should be placed in an opaque, sealed envelope. Do not write “SSI” on the outside of the envelope.
“Best Practices for Stakeholders”
Storing SSI on CDs

SSI documents saved on compact discs (CDs) must be password protected.

The CD’s outside jacket must be marked with a label that contains the SSI footer.

CDs must be protected as though they were documents (i.e., store the CD in a locked drawer.)
“Best Practices for Stakeholders”
Storing SSI on Flash Drives

Personnel should only use encrypted thumb drives or password-protect documents that contain SSI.

Portable drives are convenient, small, and can store a large volume of information. They are also easily lost or misplaced.

Be careful about what information is placed on these devices, how they are stored, and who is walking out the door with them.
“Best Practices for Stakeholders”

Taking SSI Home

It is not recommended!

However, if taking SSI out of the office is necessary, employees should have the permission of the supervisor and should ensure that SSI is locked away at night to prevent unauthorized access of persons who do not have a “need to know.”
Destruction of SSI
Regulation for Destruction of SSI

“A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures.”

49 CFR Part 1520.19(b)(1)
“Best Practices of Stakeholders”
Destruction of SSI

The most common methods used to destroy SSI material include:

- Cross-cut shredders
- Contract with a shredding company
- Cutting or tearing into pieces that are no longer than ½ inch on a side and mixing with other trash
Summary
Discussing SSI in Public Areas

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.
“Best Practices for Stakeholders”
DO’s – SSI Safeguarding

Do – **Lock up** material containing SSI.

Do – **Turn off** or lock computer whenever left unattended.

Do – **Properly destroy** all SSI when no longer needed.

Do – **Be conscious** of surroundings when discussing SSI; remember not everyone has a “need to know” SSI.
Best Practices for Stakeholders: DON’T’s – SSI Safeguarding

Don’t – Leave SSI unattended.

Don’t – Discuss SSI with individuals who do not have a “need to know.”

Don’t – Put SSI in the body of an e-mail.
Consequences of Unauthorized Disclosure of SSI

- **Lost lives** – terrorists could use the information to plan an attack
- **Lost jobs** – for Covered Persons employees, appropriate personnel action may be a letter of reprimand, suspension, or even dismissal depending on the circumstances
- **Lost money** – the government can impose a $10,000 civil penalty per offense
More Information about SSI

The SSI Program maintains SSI site on TSA website: www.tsa.gov/SSI
Safely Sharing Information

SSI Program
Office of Security Services and Assessments
Office of Law Enforcement/
Federal Air Marshal Service
Transportation Security Administration
601 S. 12th Street, East Tower
Arlington, VA 20598-6031

E-Mail: SSI@dhs.gov
Phone: 571-227-3513
Fax: 703-603-0902