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

SSI Training for Fusion Centers

As of May 2022
Objectives

This briefing will focus on the following topics:

- The differences between Classified National Security Information and Sensitive Security Information (SSI)
- Recognizing SSI Records
- 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”*

Example:
A U.S. Special Operations team conducts a raid, driven by intelligence, overseas. The *identity* of the “source” of data and the *information* he or she 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:

- TSA Intelligence Products marked as SSI
- TSA Security Directives marked as SSI
- TSA Incident Reports
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.*

* Example: FBI Intelligence Bulletins

* Source: FBI’s Web site
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.)

- In litigation, SSI has stronger protection from court-ordered production requests than LES, while documents marked only as FOUO have little or no protection.

- SSI is protected from public release under a Freedom of Information Act (FOIA) request; FOUO or LES may be either protected or released under FOIA.

- Documents that contain SSI must be marked as SSI – not as FOUO or LES. When information is pulled from reports marked LES, FOUO, and SSI, the new report must be marked as SSI.
Focus on the SSI Federal Regulation (49 CFR Part 1520)
Sensitive Security Information

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 one of the categories of SSI defined by the Federal Regulation (49 CFR Part 1520.5(b)).
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*?
SSI that May Appear at a DHS Fusion Center*

- TSA Encounter Reports & Reviews (monthly, quarterly)
- TSA Modal Threat Assessments (aviation, mass transit, etc.)
- TSA Intelligence Products marked as SSI
- TSA Country Threat Assessments (CTAs)
- Transportation Suspicious Incident Reports (TSIR)
- KST traveler information from TSA No-Fly, Selectee Notification Reports (NFNRs, SNRs)
- Strategic Transportation Threat Awareness Report (ST²AR)
- After-Action Report following a major aviation incident
- Transportation Intelligence Study (TIS)
- Any record that states Federal Air Marshals (FAMs) ARE or ARE NOT flying on a particular flight

* List not all-inclusive
Threat Information

49 CFR 1520.5(b)(7) Threat Information

Any information held by the federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure
SSI and Intelligence

TSA often marks intelligence products as SSI. This is very deliberate and may not be re-marked as FOUO without review by the SSI Program office.

Some of TSA’s intelligence products are protected as FOUO. This is because most of the raw intelligence is gathered by other agencies and the information is sent to TSA already marked.
SSI in Vetting
Terrorist Screening Database

The federal government consolidated various terrorist watch lists into one watch list known as the Terrorist Screening Database (TSDB), maintained by the Terrorist Screening Center (TSC) and administered by the FBI.

Names for No-Fly, Selectee, and eSelectee Lists are drawn from the TSDB.
TSDB Information That is NOT SSI

• Names on the TSDB are not SSI
• Records that state a person that is being vetted is or is NOT on the TSDB is FOUO/LES
  – This includes whether or not a person also has a TIDE record
No-Fly List and Selectee List

The No-Fly List and Selectee List are subsets of the Terrorism Screening Database (TSDB) and consist of persons who pose, or are suspected of posing, a threat to civil aviation or national security, or have links to terrorism.

Passengers’ names are compared against the No-Fly and Selectee List by TSA’s Secure Flight program and works with TSC to resolve any matches.
No-Fly, Selectee, and Rules-Based List Information That Is SSI

- Records that state a person that is being vetted is or is NOT on the No-Fly List, Selectee List, or other TSA rules-based list (e.g., Quiet Skies/Silent Partner)
- The actual names of persons on the lists and number of names on the lists
- Any demographic characteristics of the lists (for example, % in a specific age range or gender)
- Specific criteria for being placed on the lists and on which list
Other Categories of SSI
Other SSI Categories at Fusion Centers

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

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

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

(ii-iii) Information concerning the deployment, number, and operation of FAMs and Federal Flight Deck Officers (armed pilots)
Other SSI Categories at Fusion Centers (cont.)

(9) (i) Any procedures for screening of persons, their property, U.S. mail, stores, and cargo that is conducted by the Federal government or any other authorized person (TSA Standard Operating Procedures)

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated system (Names from TSA No-Fly List or Selectee List)

(iv) Performance or testing data from security (covert testing)
Other SSI Categories at Fusion Centers

(11) Identifying Information of Certain Security Personnel –

(i) Lists of names that identify persons as –

(D) Holding a position as a FAM
   (any record that contains two or more FAMs names is SSI)

(ii) Name that identifies a person as current FFDO
   (any record that contains two or more FFDO names is SSI)
How to Recognize SSI?

The Transportation Security Administration (TSA) Presents:

Deployment of TSA Federal Air Marshals (FAMS)

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 6 U.S.C. 562 and 49 CFR parts 15 and 1520.
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.
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.”
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.
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 SSI Categories that are listed in the SSI Federal Regulation.
Who Can Mark Records as SSI? (cont.)

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.
Derivative Marking

- Derivative use is the act of incorporating, paraphrasing, restating, or generating in new form, information that is already sensitive or classified.

- The newly developed material must be marked consistent with the markings of the source information.

- Any material developed using SSI must retain the SSI markings on the new file.

- Highly encourage use of portion-marking within the file when there are varying protection requirements (e.g., SSI, LES, FOUO, Classified)
SSI Federal Regulation Outlines Procedures for Marking and Handling SSI
Everyone is Responsible for Protecting SSI!!!

Personnel who work in transportation whether they are airport employees, airline employees, law enforcement, Federal, state or local government employees or contractors are responsible for properly marking, handling, protecting, storing, and destroying SSI per the SSI Federal Regulation (49 CFR Part 1520).
SSI is SSI regardless of who is holding the record

The SSI Federal Regulations allows SSI to be protected whether it is held by Federal employees, state law enforcement employees who work in the transportation industry (e.g., airport law enforcement), employees of private companies who work in transportation industry (e.g., airline employees).

In addition, private companies create SSI records (such airline security plans) and may mark and protect the records as SSI without authorization from the Federal government.
Covered Persons

According to the SSI Federal Regulation, covered persons may access SSI. This includes airport and airline officials, maritime operators, rail and pipeline operators, Federal, State and Local government employees, and contractors 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 screening equipment vendor does not need access to the flying schedules of FAMs.
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.
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!!!
Protecting Electronic Data

• The SSI Regulation instructs: “Take reasonable steps to safeguard SSI in that person’s possession or control from unauthorized disclosure.”

• 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.

* 49 CFR § 1520.9(a)(1)
Posting SSI: Never Post SSI on the Internet
Duty to Report Unauthorized Disclosure of SSI

The SSI Federal Regulation 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.
- TSA SSI Program office’s email address is SSI@tsa.dhs.gov.

* 49 CFR § 1520.9(c)
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.”*

In other words, throwing SSI in a garbage can or recycling bin violates the SSI Federal Regulation.

* 49 CFR § 1520.19(b)(1)
Discussion 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
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.
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.

- Manage policies to ensure only desired members can attend; for example, verify attendees are covered persons with a “need to know,” or enable a waiting room to vet attendees
- Lock the event once all intended attendees have joined
- Ensure that the host can manually admit and quickly remove unwanted attendees, if necessary
- Be mindful of how (and to whom) the links are disseminated
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 “need to know” 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 you (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 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 of classified national security information
Frequently-Asked Questions
Q: How Do We Handle Requests for SSI Information?

A: Requests for SSI fall into two categories:

• Sharing SSI
• Releasing SSI
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.
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.”” *
  – “(I)f a record contains both SSI and information that is not SSI, TSA...may disclose the record with the SSI redacted...” *

• TSA addresses these requirements by providing an official SSI Review process through its SSI Program office.

* 49 CFR § 1520.15(a) & (b)
Processing Record 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 C.F.R. § 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 SSI Federal Regulation, which preempts conflicting State, local, tribal and territorial law.
• Requests for TSA records made through State Open Records requests must be referred to TSA FOIA (FOIA@tsa.dhs.gov).

• Requests for records belonging to the state or airport authority should be submitted for full SSI Review to the SSI Program office at HQ if it is possible that the records contain SSI.

• While the SSI Program office will attempt to work within the law’s time constraints, it is not always possible. Interim responses back to the Requestor may be made indicating the need for SSI Review.

• 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 Sensitive Security Information (SSI). That authority is delegated from the Administrator to the Chief of the SSI Program.
- Using this authority, the SSI Program office determines what information is designated as SSI or not SSI within a record. The SSI Program office is the final arbiter and authorized to make SSI determinations on both Federal records and records produced by stakeholders.
- If necessary, the SSI Program office will provided redacted (i.e., all of the SSI blacked out) versions 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
- The SSI Program office is 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