SSI Policies & Procedures Handbook

Attachment to TSA MD 2810.1

Version 3.1

SSI Program
Current as of April 15, 2024

Document Change History

Version	Date	Description
1	23 April 2012	Draft Baseline Release - ***Note:*** *This revised policy superseded all SSI Program office policies and procedures dated September 29, 2006 and August 7, 2007.*
2.0	4 November 2015	This revised policy supersedes Version 1 of the SSI Policies & Procedures Handbook. Updated links to SSI Program resources; expanded guidance on *SSI Challenge and Appeals Process* (Subsection 3.8); inclusion of guidance on transmitting images in Good software (Subsection 5.2.3); added guidance on *Video Teleconferencing* (Subsection 5.2.8); updated guidance on encrypting files using Adobe® Acrobat® Professional, Microsoft® Office®, and WinZip® (Subsection 5.3.3); included provision for sharing/disclosing SSI with those receiving classified information (Subsection 6.1); added guidance *Disclosure of SSI to AFGE and Personal Representatives* (Subsections 6.1 and 6.3); included expanded guidance on delegation of authority for disclosure of SSI to Congress (Subsection 6.4); added guidance *State Open Records Requests* (Subsection 6.6); removed reference to *SSI Site Assistance Visits* (Subsection 9.7); added decision process for *Determining SSI Release to Foreign Governments* (Appendix 8); added instructions for new and certified SSI Coordinators (Appendix 9 & 10); added instructions for applying Watermarking to files (Appendix 11); added instructions for Formal Appeal Justification (Appendix 12).
3.0	15 July 2022	This revised policy supersedes Version 2 of the SSI Policies & Procedures Handbook. This Handbook has substantive edits throughout. Notable updates include, but are not limited to, updated links to SSI Program resources; requirement to transcribe audio material in *Requesting an SSI Assessment or SSI Review from the SSI Program* (Subsection 3.5); expanded guidance on portion marking in *Marking SSI* (Section 4.0) including updates to Table 1, *SSI Marking Guidance for Records & Media*, expanded guidance on Safeguarding SSI (Section 5.0) including extensive edits to *TSA Shared Network Resources*, updates to *Encrypting SSI in Transmission and Storage*, and a new section on *SSI Handling during Telework and Remote Work*; expanded guidance on *Disclosure of SSI* (Section 6.0) including

3.0 (cont.)		updates to *Determining Covered Persons with a Need to Know* (Subsection 6.1), *Non-Disclosure Agreements* (Subsection 6.2), *Congress and Government Oversight (e.g., GAO, OIG)* (Subsection 6.4), and a new section on *Vetting for Access to SSI* (Subsection 6.9); updated guidance in *Destruction of SSI* (Section 7.0); updated guidance on *SSI Training Programs* (Section 8.0); removed *SSI Coordinator Designation Instructions* (formerly Appendix 2), instructions for new and certified SSI Coordinators (formerly Appendix 9 & 10), and *Formal Appeal Justification* (formerly Appendix 12) since this information is available on iShare; updated Appendix 6 & 7 (*SSI Threshold Analysis* and *SSI Impact Assessment)* to streamline and clarify the documents; removed *Determining SSI Release to Foreign Governments* (formerly Appendix 8) since this is a matter of internal standard operating procedure. Of particular note, this Handbook update provides options for marking SSI in encrypted emails. Certificate-based encryption is currently available in email if the user publishes their own certificates. This will be further enabled by future projects to encrypt and mark SSI in email.
3.1	15 April 2024	This revised policy supersedes Version 3 of the SSI Policies & Procedures Handbook. Notable updates include the modification of 3.8.2 on the formal appeals process to add that the decision of the Administrator is only reviewable by a US Court of Appeals, updates to section 5.2.2.3 (including Table 2: SSI Posting Guidance for SharePoint) to reflect changes in handling on SharePoint, the addition of External TSA Password policy in Section 5.3.2., renumerating Sections 5.3.3 through 5.3.6, and adding references to External TSA Password, where applicable. Removed references to iShare and Skype throughout as these platforms have been disabled. Removed reference to Technical Standard 21*, General Telephony* as this standard has been archived. Updated Section 11 to clarify that SSI systems are those which SSI is processed, stored, or transmitted. This update includes updates to new SharePoint links throughout.

EFFECTIVE DATE AND IMPLEMENTATION: These changes are effective immediately upon signature.

LARRY A SMITH

Digitally signed by LARRY A SMITH
Date: 2024.05.10 15:08:47 -04'00'

05/10/2024

Larry A. Smith
Assistant Administrator
Security and Administrative Services

Date

Table of Contents

1.0 Introduction 7

2.0 Definitions 8

3.0 Identifying SSI 12

3.1 Creating SSI Identification Guidance 12
3.2 Using SSI Identification Guidance 12
3.3 Conducting SSI Assessments 13
3.4 Conducting SSI Reviews 13
3.5 Requesting an SSI Assessment or SSI Review from the SSI Program 15
3.6 Requesting an SSI Review of Classified Material from the SSI Program 15
3.7 Identifying Maritime SSI 16
3.8 SSI Challenge and Appeals Process 16

3.8.1 SSI Challenge and Informal Appeals Process 16
3.8.2 Formal SSI Appeals Process 17
3.8.3 Formal SSI Appeals Schedule 18
3.8.4 Final SSI Appeals 18

4.0 Marking SSI 19

4.1 Marking Records & Media Containing SSI 20
4.2 SSI in Presentations and Briefings 21

5.0 Safeguarding SSI 22

5.1 General Protection of SSI 22
5.2 Protecting SSI in Transmission & Storage 22

5.2.1 The Internet 22
5.2.2 TSA Shared Network Resources: Shared Drives, Systems & TSA Intranet 23

5.2.2.1 Shared Drives and OneDrive 23
5.2.2.2 TSA Systems and Applications 24
5.2.2.3 TSA Intranet (e.g., Teams, SharePoint) 24
5.2.2.4 Teleconferencing and Webinar Applications 25

5.2.3 Encrypting SSI in Transmission and Storage 26
5.2.4 Electronic Devices 26
5.2.5 Scanners, Copiers & Printers 27
5.2.6 Faxes 28
5.2.7 Telephone 28
5.2.8 Packaging & Delivering SSI 29
5.2.9 SSI Handling during Telework and Remote Work 30
5.2.10 Removing SSI from the Workplace (Traveling with SSI) 30

5.3 Passwords 31

5.3.1 Standard TSA Password 31
5.3.2 External TSA Password 31
5.3.3 Creating Passwords to Encrypt SSI 32
5.3.4 Methods for Applying Encryption to SSI 32
5.3.5 Transmitting SSI Passwords 33
5.3.6 SSI Password Incidents 33

6.0 Disclosure of SSI 34
6.1 Determining Covered Persons with a Need to Know 34
6.2 Non-Disclosure Agreements 36
6.3 Disclosure of SSI to AFGE and Personal Representatives 36
6.4 Congress and Government Oversight (e.g., GAO, OIG) 38
6.4.1 SSI Disclosure to Congress 38
6.4.2 SSI Disclosure to GAO 39
6.4.3 SSI Disclosure to OIG 40
6.5 Freedom of Information Act (FOIA) Requests 40
6.6 State Open Records Requests 40
6.7 Enforcement Proceedings 41
6.8 Other Conditional Disclosures 41
6.9 Vetting for Access to SSI 41
6.9.1 Vetting Requirements by Role 42
6.9.2 Processing SSI Security Threat Assessment (SSI STA) Requests 43

7.0 Destruction of SSI 45

8.0 SSI Training Programs 46

9.0 SSI Awareness Programs 48
9.1 SSI Coordinators 48
9.2 SSI BOLOs and Stakeholder Alerts 48
9.3 SSI Conference Calls 48
9.4 SSI Awareness Week 49
9.5 SSI SharePoint Page & Internet Page 49
9.6 Self-Inspection Program 49

10.0 SSI Incidents 50
10.1 Identifying SSI Incidents 50
10.2 SSI Incident Response & Resolution 50
10.2.1 Discovery & Initial Notification 51
10.2.2 Immediate Evaluation & Follow-Up Notification 51
10.2.3 Early Mitigation 51
10.2.4 Incident Closure 52
10.2.5 Long-Term Risk Mitigation 52
10.2.6 Incident Investigation 53
10.3 SSI Password Incident Response & Resolution 53

10.4 Penalties for Mishandling or Unauthorized Disclosure of SSI 53

11.0 Determining SSI Systems 54

12.0 Protection Requirements for SSI Systems & Other Secure Sites 54

13.0 SSI Policy Exceptions 54

Appendices

Appendix 1: SSI Program Initial Decision Flow Chart 55
Appendix 2: Determining Need to Know Flow Chart 58
Appendix 3: Instructions for Watermarking Files 59
Appendix 4: SSI Incident Response Flow Chart 60
Appendix 5: SSI Incident Reporting Instructions 61
Appendix 6: SSI Threshold Analysis 62
Appendix 7: SSI Impact Assessment 69

Addendum

Addendum 1: Appendix 4: SSI Incident Response Flow Chart 76

1.0 Introduction

Welcome to the Sensitive Security Information (SSI) Policies and Procedures (P&P) Handbook. This Handbook expands on the SSI Regulation (49 C.F.R. Part 1520, Protection of SSI); DHS MD 11056.1, Sensitive Security Information; DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*; and TSA MD 2810.1, *SSI Program*.

What is SSI?

SSI is a category of sensitive information (i.e., sensitive but unclassified [SBU] or controlled unclassified information [CUI]) that must be protected because it is information that, if publicly released, would be detrimental to the security of transportation.[1] In other words, SSI is information that could be used to bypass or defeat transportation security measures. Armed with SSI, our adversaries will be empowered. (For detailed categories of SSI, see the SSI Regulation, 49 C.F.R. § 1520.5(b)(1) through (16)).[2] For additional guidance on how to identify SSI, see the SSI Program office Identification Guides.

Purpose

This Handbook contains policies and procedures on how to properly identify, mark, handle, protect, disclose, and destroy SSI. This Handbook covers many media that may contain SSI, including hard copy (paper), soft copy (electronic), magnetic, CDs and DVDs, video, and other types of media (written and spoken). If a topic of interest is not covered in this Handbook, contact the SSI Program office at SSI@tsa.dhs.gov for consideration of inclusion in future SSI P&P Handbook updates or in the SSI Program office Frequently Asked Questions (FAQ).

During periods of national emergency or exigent circumstances, the Transportation Security Administration (TSA) Administrator or SSI Program Chief may determine that certain requirements of this Handbook should be temporarily suspended.[3] Even during national emergency or exigent circumstances, however, all covered persons are still required to take reasonable measures to protect SSI.

Who Should Use This Handbook?

All persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including interns and foreign nationals) must follow the guidance in this Handbook and are hereafter referred to generally as "personnel," unless otherwise specified. While this Handbook was specifically designed for TSA Personnel, it may also serve as a model for use by other DHS components.

This Handbook may also be used as a collection of best practices for non-Department of Homeland Security (DHS) persons who handle SSI. These persons include transportation stakeholders (i.e., regulated entities such as air carriers); other Federal agencies; state, local, and tribal governments; and other covered persons as defined in 49 C.F.R. § 1520.7. For consideration of sharing this Handbook outside of DHS, contact the SSI Program office directly at SSI@tsa.dhs.gov for a determination on a case-by-case basis.

---

[1] Under 49 C.F.R. § 1520.5(a), the SSI Regulation also provides other reasons for protecting information as SSI beyond that the release of the information would be detrimental to the security of transportation. TSA, however, primarily uses the criterion of "detrimental to the security of transportation" when determining whether information is SSI.

[2] All future "§" references refer to sections in the SSI Regulation, 49 C.F.R. Part 1520.

[3] Even if SSI Program office policies or procedures are temporarily suspended, other TSA program offices (e.g., Information Technology's Information Assurance and Cybersecurity Division [IAD]) may have policies that still need to be followed.

2.0 Definitions (In alphabetical order)

Authorized Redactor

TSA employee who has completed the mandatory TSA Redaction Training and, therefore, authorized to redact documents and/or perform quality assurance reviews on documents redacted by another Authorized Redactor at TSA.

Coordinators

SSI Coordinator

A TSA employee who has been appointed by the Deputy Administrator, an Assistant Administrator or equivalent (e.g., Chief of Staff, the Chief Counsel [CC]), a Federal Security Director (FSD), or a Supervisory Air Marshal in Charge (SAC) to be a point of contact for their office and to liaise between their office and the SSI Program office.

Certified SSI Coordinator

An SSI Coordinator who has (1) completed the required modules of Advanced SSI Training, (2) passed the SSI Certification Exam, and (3) properly maintained their certification status by completing Continuing Education in SSI (CESSI) Training on an annual basis.

Covered Persons

As defined in the SSI Regulation at § 1520.7, an individual or entity that has transportation security or transportation security-related responsibilities to include, but not limited to, (1) anyone who is permanently or temporarily assigned, attached, detailed to, employed by, or under contract with DHS, (2) regulated parties, Federal, State, Local and tribal government employees, contractors, and grantees, as well as TSA stakeholders and industry partners; (3) Committees of Congress; (4) other persons with a need to know as defined in § 1520.11; and (5) persons receiving SSI pursuant to other conditional disclosures.

Destroy

The process of making a record (see below) unreadable and unrecoverable.

Disclose

The act of providing access to a record containing SSI to covered person(s) with a need to know or others who are authorized in writing by the TSA Administrator or designee to have access to SSI.

Identifying SSI

Determination

A decision made by the TSA Administrator (also known as the Administrator of the Transportation Security Administration) or designee to identify whether or not information, which has not previously been evaluated for SSI content, is SSI.

Identification Guides

SSI Program office-issued guidance, created in coordination with subject matter experts (SMEs), to help authorized redactors or other personnel identify SSI pursuant to § 1520.5(b).

Loss of SSI Designation
Information loses its SSI designation when the TSA Administrator, or designee, determines in writing pursuant to § 1520.5(c) that the information once protected as SSI under § 1520.5(b) no longer is detrimental to transportation security.

Redaction (R)
To obscure or prevent portions of a record containing SSI from being viewed and accessed. Adobe® Acrobat® Professional is TSA's standard software tool for electronic document redaction. Redaction of hard copy documents must follow the procedures described in Section 7(B) of TSA MD 2800.21, *Document Redaction*.

SSI Advanced Application Guide
Guidance developed by the SSI Program office designed to assist in conducting an SSI Assessment to determine whether a record contains SSI, as well assist SSI Program Analysts conduct SSI Reviews.

SSI Assessment
An evaluation of whether a record contains SSI.

SSI Review
An evaluation of a record by the SSI Program office to identify and mark SSI within the record and cite the specific subsection(s) of 49 C.F.R. § 1520.5(b) that justifies the determination.

Visual Redaction (VR)
The process of visually identifying SSI in a record, usually by means of highlighting or boxing-in the SSI. This process does not actually remove or obscure the data within the record, as with a redaction, but it allows for the accurate application of redactions to a document in the future.

Incidents

Password Incident
When either (1) a password created to encrypt SSI is inappropriately shared with covered persons in a manner not in accordance with this TSA SSI P&P Handbook; or (2) the Standard TSA Password is shared inappropriately with persons not within DHS.

SSI Incident
The verified or suspected loss, breach, or unauthorized disclosure of SSI to non-covered persons; the unauthorized disclosure of SSI to covered persons who do not have a need to know the information; or the non-compliance with the TSA SSI Policies & Procedures Handbook in the handling of a record containing SSI.

Marking
Applying the SSI protective marking (SSI header) and distribution limitation statement (SSI footer) to materials containing SSI in accordance with the SSI Regulation at § 1520.13. Some circumstances may require variations in marking as further detailed in Section 4.0 *Marking SSI* of this Handbook.

Need to Know
Generally, a person or entity has a need to know SSI when access to the SSI is necessary to carry out transportation security activities or to perform official duties as defined in the SSI Regulation at § 1520.11. For specific SSI, the TSA Administrator, or designee, may make a finding that only specific persons or classes of persons have a need to know.

Protect
Taking both required and reasonable steps, as defined in the SSI Regulation at § 1520.9 and this TSA SSI P&P Handbook, to safeguard a record containing SSI and prevent disclosure to non-covered persons or persons without a need to know.

Record
Any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and information stored in any electronic format. The term record, for the purposes of SSI protection, also includes any draft, proposed, or recommended change to any record.

Release
Provide access to a record without expectation of continued protection. ***Note**: This term is often seen used as if it is interchangeable with "disclose." However, the two terms are distinct and the use must be evaluated carefully to ensure proper protection of SSI.*

Sensitive Security Information
As defined in the SSI Regulation at § 1520.5, SSI is information obtained or developed in the conduct of security activities, including research and development, the public disclosure[4] of which DHS/TSA has determined would, among other things, be detrimental to the security of transportation.

Share
See *Disclose*.

SSI Impact Assessment (SSIIA)
A document prepared by a program office or system owner (SO) in conjunction with the SSI Program office and the Information Technology's (IT) Information Assurance and Cyber Security Division (IAD) to assess the security in place to protect SSI and resultant risk associated for an IT system. This document may also be used by other non-TSA systems or other secure sites not requiring Security Authorization (SA) to document alternate acceptable protection in lieu of standard SSI policies and procedures.

SSI System
Any system that processes, stores, or transmits SSI information. A system's SSI status shall be reflected in its SSI Threshold Analysis (SSITA) document and is subject to DHS Directive 4300A, *DHS Sensitive Systems Policy.*

SSI Threshold Analysis (SSITA)
A document prepared by a program office or system owner (SO) in conjunction with the SSI Program office and Information Technology's (IT) Information Assurance and Cybersecurity Division (IAD) to determine if an IT system processes, transmits, or stores SSI. This document is produced as part of the

[4] Authorizing legislation for Sensitive Security Information (SSI) uses the term "disclosure" to describe the unauthorized release of SSI. Use of the term "disclosure" in this definition should not be confused with TSA's use of disclose/disclosure in policy where it is used to describe authorized information sharing.

Security Authorization (SA) process. This document shall also be used for emerging and standing security programs and initiatives to determine whether it may be appropriate to develop an SSI Identification Guide for the program in coordination with the SSI Program office.

SSI Training

SSI Awareness Training

Training on SSI developed or endorsed by the SSI Program office to educate covered persons about the principles of identifying, marking, safeguarding, disclosing, and destroying SSI offered either through mandatory training for TSA Personnel or through customized training provided as needed.

Advanced SSI Training

TSA training on SSI developed and provided by the SSI Program office that provides a higher-level of guidance on SSI identification. Completion of all specified advanced SSI training modules is required before an appointed SSI Coordinator or other federal personnel may take the SSI Certification Exam.

SSI Certification Exam

An exam provided to federal personnel who have completed all required modules of Advanced SSI Training. Federal personnel who pass the exam achieve the status of "SSI Certified."

CESSI

Continuing Education in SSI training. Certified SSI Coordinators and others who have passed the SSI Certification Exam must complete CESSI requirements annually to maintain SSI Certification.

SSI Certified

Any person who has (1) completed the required modules of Advanced SSI Training, (2) passed the SSI Certification Exam, and (3) properly maintained their certification status by completing CESSI training on an annual basis (See also *Certified SSI Coordinator*).

Standard TSA Password

A password generated by the SSI Program office which may be used by TSA personnel to encrypt SSI. This password may be obtained through the designated SSI Coordinator or the SSI Password Finder App on Salesforce.

Subject Matter Expert (SME)

A person who has expert-level knowledge and information about specific transportation security matters who can assist in determining whether specific program-related information is SSI.

TSA Personnel

Persons permanently or temporarily assigned, attached, detailed to, employed by, or under contract with TSA (including interns and foreign nationals).

3.0 Identifying SSI

3.1 Creating SSI Identification Guidance

As the arbiter of what is SSI, the SSI Program office issues SSI Identification (ID) Guides on precisely what information is and is not SSI within a specific subject area and defines which subsections of the SSI Regulation apply. All SSI ID Guides are developed in collaboration with SMEs, updated periodically as information and programs change, and reviewed for accuracy on a 3-year cycle.

An SSI ID Guide is generally created after repeated requests to review or make SSI determinations on a particular subject matter. Certain new programs or agency efforts have SSI implications, that require the development of an SSI ID Guide at the outset of the program. Furthermore, the development or revision of a TSA Security Classification Guide (SCG) often prompts the creation of, or amendments to, a corresponding SSI ID Guide.

After a subject area is identified as appropriate for an SSI ID Guide, the SSI Program office works through the SSI Coordinator network to identify appropriate SMEs for the subject area. SMEs help identify what information about the program or subject matter should be protected as SSI. ***Note:*** *In order to have accurate SSI ID Guides, full participation and prompt communication from the relevant program office SSI Coordinator(s) and designated SMEs are necessary. If offices are not responsive within 30 days of last contact, the SSI Program will continue to publish guidance to the best of its judgment.*

The SSI Program office then determines if the information suggested for protection meets the standard for being "detrimental" to transportation security and falls within the scope of one or more of the 16 categories of the SSI Regulation. Information not covered in §§ 1520.5(b)(1) through (15) or in an existing (16) determination is considered for a new (16) determination.[5]

See Appendix 1: *SSI Program Initial Decision Flow Chart* for additional information about how the SSI Program office conducts initial determinations on what may be protected as SSI under the SSI Regulation.

3.2 Using SSI Identification Guidance

SSI ID Guides are resources for personnel to recognize whether information requires protection as SSI. The SSI ID Guides are designed for use both by persons with great familiarity with the SSI Regulation and SSI ID Guides and by persons with little familiarity with either.

All personnel are responsible for using SSI Program office-issued SSI ID Guides to recognize if the material they are handling may contain SSI. ***Note:*** *To verify the content does not contain SSI before posting to the Internet or releasing to a non-covered person, see Subsections 3.3 Conducting SSI Assessments and 5.2.1 The Internet.*

Personnel with questions about whether information is SSI should first determine whether a relevant SSI ID Guide exists and verify whether the information is or is not SSI. If the information does not appear to be SSI, personnel shall consult with their SSI Coordinator for verification through an SSI Assessment. Personnel shall also refer to the SSI ID Guides to determine whether to mark and protect a record as SSI, when they are reviewing a record for SSI content, or when they have come into possession of a record

[5] "(16) determination" refers to the authority provided by the regulation to designate any information not otherwise described in §§ 1520.5(b)(1) through (15) that TSA determines should be protected as SSI under 49 U.S.C. 114(r). A (16) determination creates a new category of SSI information.

that they believe is not properly marked. Within the SSI Program office, SSI ID Guides assist in conducting SSI Assessments and SSI Reviews and serve as one authority for SSI determinations.

SSI ID Guides are intended for DHS-wide distribution. For consideration of sharing the SSI ID Guides beyond DHS, contact the SSI Program office directly at SSI@tsa.dhs.gov for a determination on a case-by-case basis.

3.3 Conducting SSI Assessments

An SSI Assessment is an evaluation of whether a record contains SSI. All TSA personnel should evaluate a record as it is being created to identify whether it contains SSI and ensure proper SSI markings are applied, if necessary. If there is uncertainty as to whether or not a record contains SSI, or an individual believes SSI markings should be removed, the record must undergo an official SSI Assessment. An official SSI Assessment of a record may only be completed by Certified SSI Coordinators or the SSI Program office. SSI Assessments must be completed using the appropriate SSI ID Guide(s) (see Subsection 3.2 *Using SSI Identification Guidance* for more information). If an SSI Coordinator cannot confidently complete an SSI Assessment or if there is insufficient current guidance available in an SSI ID Guide, the record must be submitted to the SSI Program for its assessment.

In no case should information be assessed as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

If there is not enough information available in the SSI Regulation, the SSI Advanced Application Guide, and the SSI ID Guides to make a confident SSI Assessment, personnel shall contact the SSI Program office at SSI@tsa.dhs.gov for additional assistance and to provide recommendations for possible SSI ID Guide updates.

3.4 Conducting SSI Reviews

An SSI Review is an evaluation of a record to specifically identify and mark the SSI within the record. Only TSA employees assigned to the SSI Program office may conduct final SSI Reviews.[6] A final SSI Review conducted by the SSI Program office is required before redactions of SSI may be applied by an Authorized Redactor.

The SSI Program office conducts a three-level review process to prevent the over-protection or improper release of SSI. If redactions are applied to the record, an independent reviewer conducts a quality assurance check for the security of the electronic redactions after the final review is completed.

Certified SSI Coordinators are authorized to conduct the first-level SSI Review for CESSI credit (See Subsection 8.0, *SSI Training Programs*, for more information on the CESSI Program) and must send their review findings to the SSI Program office for the second- and final-level reviews, and a quality assurance check.

Personnel conducting an SSI Review must abide by the following general principles:

[6] The SSI Regulation, at 49 CFR part 1520.9(a)(3), requires stakeholders to refer requests by other persons for SSI to TSA, or the applicable DHS component or agency. In order for SSI to be redacted from stakeholder records, submit these requests to the SSI Program for review and redaction by following instructions in Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*.

- Protect SSI on the merits of the particular information being reviewed, regardless of the requester of the information or the purpose of release.
- Release as much information publicly as possible without compromising transportation security. The following factors must be considered:
    - **Operational Use to Adversaries:** Would the information help them bypass or defeat transportation security measures or identify specific targets to plan or execute attacks?
    - **Level of Detail:** More detailed information is generally more useful and more likely to be SSI.
    - **Public Availability:** Has the Government released the information publicly in an official statement or document?
      Note: *Some partially-compromised (publicly or unofficially released) open source information may remain SSI because of its operational use to adversaries.*
    - **Obviousness:** Obvious or intuitive information is generally not protected as SSI unless its operational use to adversaries dictates otherwise.
    - **Age of the Record:** This factor may be overridden by the SSI reviewer's assessment of the current security implications (e.g., superseded, inactive screening procedures may still be SSI if they match or reflect current procedures) or potential future use of historical procedures.
- Redact the smallest possible portion of the record (word, phrase, or sentence) necessary to protect SSI, unless the entire document, page, or paragraph is SSI. Do not simply redact entire documents, pages, or paragraphs unless it is necessary (1) to prevent an inference of the redacted information, or (2) to prevent a cumulative SSI effect where the non-redacted portions of a document, when read in total, legitimately constitute SSI.
- Strive for consistency in SSI redactions (e.g., if information was redacted or released in a record previously reviewed for SSI, that information should be similarly or identically redacted or released in a record being currently reviewed, *unless* changes in SSI identification guidance, security measures, technology, or other factors make it necessary to redact the record differently).
- Protect SSI even when it is contained within a record not properly marked as SSI.
- Release in full (RIF) a record marked as SSI if it contains no SSI, unless other information protections (e.g., Privacy Act information) apply. ***Note:*** *The SSI Program does not review a record for any other sensitive information except SSI.*

In no case should information be identified as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

See Appendix 1: *SSI Program Initial Decision Flow Chart* for additional information on how the SSI Program office conducts initial determinations on what may be protected under the SSI Regulation.

3.5 Requesting an SSI Assessment or SSI Review from the SSI Program

Personnel shall use the following guidance to request the SSI Program office conduct an SSI Assessment or an SSI Review of material:

- Submit the SSI Review Request through the SSI App on Salesforce.

  IMPORTANT: Do not include Classified National Security Information (CNSI) in the request (e.g., do not include titles containing classified information)!

- Requests for assessment or review of audio material over 15-minutes in length must be transcribed prior to submission to the SSI Program.

Follow Job Aid: SSI Review Submissions in SSI App to accurately submit a request to include contact information, intended use of the document, and justification for any requests for expedited review, if needed prior to the standard 10-day (i.e., 10 business days) processing time.

3.6 Requesting an SSI Review of Classified Material from the SSI Program

Personnel shall use the following guidance to submit requests for the SSI Program office to review classified material[7] for the presence of SSI (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*). This type of review typically occurs when the classified material is being considered for declassification; it may also occur to ensure appropriate marking within the classified document.

The requester must prepare the material to be reviewed as follows:

- Ensure the classified material is properly marked;
- Provide two (2) paper copies for an assessment or four (4) paper copies for an SSI Review of the material being requested for review; put the copies into a folder; and attach the appropriate classified cover sheet to the folder.
- If more than one document is being requested for review, clearly write at the top of the file the document number (e.g., Document 1) for tracking purposes.
  - For Confidential and Secret material: Hand-deliver the copies to the SSI Program. **WARNING:** Follow all required CNSI handling requirements. Do NOT leave the folder on a desk. You must coordinate a secure hand-off with an SSI Program analyst.
  - For Top Secret material: Contact the SSI Program office for an alternate process;

Alternately, to provide an electronic record for review, contact the SSI Program for assistance.

The SSI Program office begins processing the request once the requestor follows the SSI Review submission process in Salesforce. Follow the SSI Review Submissions in SSI App Job Aid to accurately submit a request to include contact information, intended use of the document, and justification for any requests for expedited review, if needed prior to the standard 10-day (i.e., 10 business days) processing time. ***Note:*** *For classified reviews, include an unclassified name for the review and upload a blank place-holder file indicating the document number for each document. For FOIA requests, include the FOIA request number.*

[7] Requester acknowledges that an SSI review of classified material is not a declassification review and SSI may or may not overlap with classified information. If a declassification occurs after the SSI review, SSI may still remain in the document; therefore, the requester is encouraged to undertake a declassification review of the material *before* submitting it to the SSI Program office for SSI Review.

After review, the SSI Program office analyst provides the Visual Redaction (VR) or Redaction (R) and arranges a time for pick-up with the requester.

3.7 Identifying Maritime SSI

For issues related to maritime SSI, contact the SSI Program office at SSI@tsa.dhs.gov. The SSI Program office consults with the United States Coast Guard (USCG) SSI Program Manager for resolution of the issue and notifies the requester of the result of discussions with the USCG SSI Program Manager. Requests for foreign disclosure of maritime-related SSI must be coordinated through the SSI Program office for ultimate approval by the USCG SSI Program Manager.

3.8 SSI Challenge and Appeals Process

Any authorized recipient of SSI who believes the information has been improperly or erroneously marked as either SSI or not SSI (hereafter referred to as "challenger") is encouraged to challenge the marking. An appeal to the decision made by the recipient of the challenge may be filed with the TSA SSI Program office. Challenges may be made either informally or formally.[8] Any decision to remove an SSI marking must be coordinated with the office which either applied the SSI marking or is programmatically responsible for the information (hereafter referred to as "information holder or owner") and/or the SSI Program office before the information may no longer be protected as SSI. All information under challenge or appeal will be protected as SSI until the process is complete.

3.8.1 SSI Challenge and Informal Appeals Process

Most questions regarding the appropriate marking for the information in question may be resolved through a challenge or informal appeal process. If a requestor has a question seeking clarification that does not rise to a difference of opinion or a need to change a marking on a file, the question may be answered and noted within the comments section of the review.

- Challenges may be made directly by the challenger to the information holder or owner, who must then reevaluate the marking against the criteria in the SSI Regulation, at § 1520.5(b)(1) through (15) and implementing guidance published or approved by the SSI Program Chief available on .[9] Offices are encouraged to include their SSI Coordinator in the discussion, if in need of assistance.
- Challenges may also be resolved by submitting the document in question to the SSI Program office for SSI Assessment or Review using the process documented in Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program.*
- The information holder or owner may request formal resolution, requiring the challenger to submit written justifications for change in marking using the process for formal appeals detailed in Subsection 3.8.2, *Formal SSI Appeals Process*.
- An informal appeal of SSI Program markings must be made directly to the SSI Program office (SSI@tsa.dhs.gov).

[8] DHS MD 11056.1, Sensitive Security Information, VI.F Challenging SSI.
[9] When uncertain whether information constitutes SSI, handle it as if it does and password-protect the attachment.

- Individuals submitting a challenge or appeal must not be subject to retribution for bringing such actions. Anonymity may be requested from any of the reviewers, and the reviewers must honor a challenger's request for anonymity and fully consider and appropriately process the challenge.

3.8.2 Formal SSI Appeals Process

Formal SSI Appeals to an SSI determination may be made to the SSI Program. The following process outlines the steps an individual must take to initiate a formal appeal:

- Individuals shall submit formal SSI Appeals through the SSI App on Salesforce following the instructions found in the *Submitting SSI Appeals Job Aid*. For personnel submitting appeals from outside of TSA, they may submit the appeal in writing to the SSI Program office (SSI@tsa.dhs.gov). Formal appeal submissions should contain the word "Appeal" and the official review number in the subject line. For personnel submitting through Salesforce, these steps will be completed automatically as the individual follows the appeal instructions.
- Attached to the appeal submission, the challenger must include a *Formal Appeal Justification* as a reference file, identifying the specific information at issue and the justification or rationale for the protection or release of that information. Rationales must be based upon the criteria in the SSI Regulation, at § 1520.5(b) implementing guidance published or approved by the SSI Program Chief available on SharePoint. The challenger may include documentation that speak to issues relevant to challenged information (i.e., reports indicating the sensitivity of the matter or level of public availability of the information).
- A senior SSI Program analyst (i.e. with final review authority) will review the appeal documentation and solicit any necessary clarification or supporting documentation from the challenger within five (5) business days of initial receipt. The SSI Program will then provide the information holder or owner with a copy of the appeal documents.
- The information holder or owner must provide the SSI Program with a response denoting the justification or rationale for the protection or release of that information. Rationales must be based upon the criteria in the SSI Regulation, at § 1520.5(b)(1) through (15) or in the (16) determination, implementing guidance published or approved by the SSI Program Chief available on SharePoint. The challenger may include documentation that speaks to issues relevant to challenged information (i.e., reports indicating the sensitivity of the matter or level of public availability of the information). The response must be sent to the SSI Program within five (5) business days of receipt of the appeal documents.
- After receipt of the information holder or owner's response the SSI Program may solicit additional responses or comment from the parties. The SSI Program may provide preliminary opinions and attempt to obtain concurrence from all parties before issuing a final determination.
- The SSI Program Chief will evaluate the information gathered through the formal appeals process, including the rationale and justification provided, and will provide the final decision to both parties within five (5) business days after receipt of the information holder or owner's appeal response.
- Formal appeals originating outside of TSA should be submitted to the respective DHS component SSI Program Manager (hereafter referred to as "component manager"). Formal appeals of component managers' decisions, including intra-component challenges, are made to the TSA SSI Program as detailed herein.

- Formal appeal of the SSI Program Chief decisions may be appealed to the TSA Administrator.
- The final decision of the TSA Administrator is exclusively reviewable by a United States Court of Appeals pursuant to 49 U.S.C. § 46110. (The D.C. Circuit or the Circuit in which a person resides).

3.8.3 Formal SSI Appeals Schedule

The following table provides a target schedule for handling appeals in order to address formal appeals in a timely manner. Challengers, information owners and the SSI Program shall strive to meet the following schedule when responding to SSI formal appeals.

FORMAL APPEALS PROCESS AND SCHEDULE	
Day	**Action**
Zero	**SSI Office Receives Appeal Document**
1 - 5	*SSI Program may solicit additional information or clarifications from requestor.*
5	**Appeal Documents Provided To Information Holder Or Owner**
6-10	*SSI Program may solicit additional information or clarification from information holder or owner.*
10	**Holder or Owner Delivers Appeal Response to the SSI Program**
11-15	SSI Program will consolidate commentary, provide initial determination to both parties, attempt to obtain concurrence on initial determination, and/or solicit additional input from both parties.
15	**SSI Program Provides Formal Appeal Decision To Both Parties**

3.8.4 Final SSI Appeals

A further appeal of the decision made by the SSI Program Chief may be made to the TSA Administrator through the Executive Secretariat process. The SSI Program Chief will submit to the Administrator the documentation developed during the Formal Appeal and any additional documentation developed by the SSI Program or submitted by the requestor. The decision of the TSA Administrator constitutes final agency action and is exclusively reviewable by a United States Court of Appeals[10] pursuant to 49 U.S.C. § 46110.

[10] The D.C. Circuit or the Circuit in which the appellant resides.

4.0 Marking SSI

The creator of the record as well as any authorized holder of the information is responsible for appropriately marking SSI. Personnel who receive a record containing SSI that is not properly marked must apply the SSI header and footer, and inform the creator and/or sender that the header and footer were missing. If unable to determine the creator/sender, personnel should contact their SSI Coordinator for assistance. Personnel disclosing SSI to covered persons who have a need to know must verify that the records containing SSI have the appropriate header and footer.

If a document is marked as SSI and has been assessed by a certified SSI Coordinator or the SSI Program to have been incorrectly marked as SSI, the header and footer may be removed or struck through. Struck-through SSI markings indicates the document does not contain SSI.

TSA encourages personnel handling SSI, both in paper and electronic form, to use the SSI Cover Sheet (DHS Form 11054) in addition to the header and footer required by the SSI Regulation as detailed below (See also Subsection 4.1, *Marking Records & Media Containing SSI*).[11] This language is mandated by the SSI Regulation and may not be changed.

> **Header**: SENSITIVE SECURITY INFORMATION
>
> **Footer**: *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.

Subjects, titles, paragraphs, charts, and similar portions need not be portion marked unless (1) the record contains other types of information that requires portion marking, e.g., classified information or other sensitive information; or (2) the information is to be transmitted outside of DHS to Congress.

All SSI records submitted by TSA/DHS to Congress must be portion-marked. Portion markings must be reviewed by the SSI Program prior to dissemination. The parenthetical abbreviation (SSI) shall be used.

Personnel shall abide by the following when marking SSI contained in classified records:

- The SSI marking is conveyed in the portion mark.
- The SSI information must be identified in the source reference citations as endnotes keyed to the relevant SSI information in the document.
- If the document does not include source reference citations, the SSI portions must be segregated from all non-SSI portions.
- Apply SSI portion markings as (U//SSI) next to each paragraph/picture/area pertaining to SSI;
- Instead of the SSI header, add "SSI" to the end of the classification banner at the top and bottom of the page; and
- Apply the SSI footer to the bottom of the front page above the overall classification marking.

In no case should information be marked as SSI to:

- Conceal a violation of law, inefficiency, or administrative error; or
- Prevent embarrassment to any person, organization, or agency.

[11] See also DHS MD 11056.1 for instruction on marking SSI for delivery to Congress.

4.1 Marking Records & Media Containing SSI

SSI markings shall be applied to different types of records and media as defined below. Personnel are also encouraged to use the SSI Cover Sheet (DHS Form 11054) on all documents and binders or folders containing SSI records. See also Marking Templates and Appendix 3: *Instructions for Watermarking Files*.

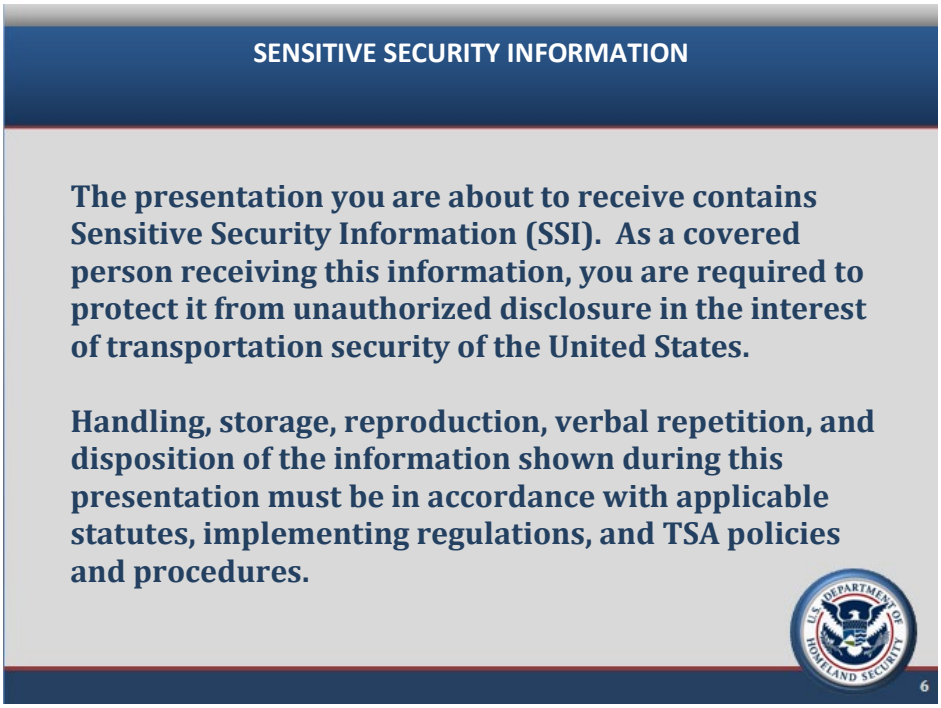
Table 1: SSI Marking Guidance for Records & Media

Type of Record	Marking
Emails	Encrypted emails containing SSI in the body of the email must be marked with the SSI header and footer; alternately, an email may begin with the marking (SSI) at the top or use tagging options, if available. Attachments containing SSI must comply with SSI marking guidance and encryption requirements (See also Subsection 5.3.4, *Methods for Applying Encryption to SSI* for encryption requirements in email).
Documents (e.g., Word, PDF)	Use header and footer on every page and on any covers.
Forms	Forms which are SSI must comply with the SSI marking guidance for "Documents." As appropriate, a disclaimer may also be added during form creation underneath the header that states "When filled out, this record contains SSI" or "When filled out, this record may contain SSI."
Presentations (e.g., PowerPoint)	Use both header and footer on first and last slides; use header only on all other slides (See Subsection 4.2, *SSI in Presentations and Briefings*).
Spreadsheets (e.g., Excel)	Use header and footer (or image of footer) on every page.
Databases (e.g., Access)	Output reports for databases producing SSI material must comply with the SSI marking guidance for "Documents."
Messaging Systems (e.g., Teams)	Portion mark SSI sent in messaging systems with (SSI) at the start of the SSI text; attachments containing SSI sent through chat must comply with the SSI marking guidance for that record type.
Charts, Maps, and Images	Place the header and footer wherever they can be readily seen.
Video and Audio Recordings	If practical, record protection requirements audibly (See Subsection 4.2, *SSI in Presentations and Briefings*) and/or show header and footer visually at the beginning and end of the recording.
CDs, DVDs, and Other Media	Apply header on media using labels or a permanent marker; apply header and footer on outside case, jacket, or sleeve.
Mobile Electronic Media (e.g., USB Flash Drives)	No external marking, *but personnel must use a TSA-approved/provided encrypted media;* mark all records containing SSI as annotated in this table for the appropriate type of record.
Other System/Application Outputs (e.g., dashboards, web page reports)	Output records generated from TSA applications/systems (e.g., Power Platform, custom apps) leveraging SSI must include SSI markings relevant to the record type (e.g., email, webpage).
Binders and Folders	Documents collected in a binder or folder are a single record and must be marked as *Documents*. Alternately, separate the SSI information and maintain those portions separately as an SSI annex to the record. SSI and non-SSI portions may also be separated by tabs/section dividers.

4.2 SSI in Presentations and Briefings

In addition to following the presentation marking requirements (See Subsection 4.1, *Marking Records & Media Containing SSI*), if a presentation or briefing contains SSI, the following language must either (1) appear on the first slide under the cover slide or (2) be read to the audience at the start of the briefing. ***Note:*** *For training programs or events where multiple presentations are delivered during the same day, the presentation statement only needs to be read once at the start of the day unless new attendees join during the course of the day. Each SSI presentation should still be marked independently.*

> "The presentation you are about to receive contains Sensitive Security Information (SSI). As a covered person receiving this information, you are required to protect it from unauthorized disclosure in the interest of transportation security of the United States.
>
> Handling, storage, reproduction, verbal repetition, and disposition of the information shown during this presentation must be in accordance with applicable statutes, implementing regulations, and TSA policies and procedures."[12]



[12] **Note:** When providing the presentation or briefing to non-DHS employees, remove the reference to "TSA policies and procedures" as other covered persons outside of the DHS network are not required to follow TSA policies and procedures for safeguarding SSI.

5.0 Safeguarding SSI

SSI may be disclosed to covered persons who have a need to know the information (See also Subsection 6.1, *Determining Covered Persons with a Need to Know*). Covered persons must protect SSI by ensuring it is disclosed only in a secure manner, achieving an effective balance between information sharing and information protection. This section of the Handbook provides ways to safely share, yet reasonably protect, SSI. Any technology not explicitly covered below must receive Chief Information Security Officer (CISO) and SSI Program office approval prior to security implementation.[13]

5.1 General Protection of SSI

Personnel who possess records containing SSI are responsible for ensuring those records are protected at all times to prevent disclosure to non-covered persons or to covered persons who do not have a need to know. See TSA MD 1400.3, *Information Technology Security* and Attachment 1, *TSA Information Assurance Handbook* for specific information-security policies and guidelines for TSA computer networks, systems, and equipment. The TSA IT Security Policy applies to all TSA personnel and all TSA information systems that collect, generate, process, store, display, transmit, or receive TSA data, including pilot (i.e., prototype) and telecommunications systems.

- When not under direct physical control, lock up the record containing SSI, including records stored on TSA-owned portable devices such as USB flash drives, CDs, or other portable devices, in a desk drawer, cabinet, or office. The *TSA Information Assurance Handbook* requires logging off or locking unattended computers. This can be done by simultaneously hitting the Ctrl + Alt + Delete keys and then "Enter" or simultaneously pressing the Windows® key and "L" key.
- Destroy SSI when it is no longer needed. (See also Subsection 7.0, *Destruction of SSI*).
- To transport or transmit SSI, use of the SSI Cover Sheet (DHS Form 11054) is encouraged.

5.2 Protecting SSI in Transmission & Storage

Personnel must ensure proper protection of information created, stored, or transmitted to limit access to covered persons with a need to know. The following subsections serve as guidance for the protection of information through a variety of media, including storage of data on authorized network drives, collaborative applications, and local hard drives.

5.2.1 The Internet

Personnel shall not under any circumstances post records containing SSI to a publicly accessible Internet site that is not a TSA-approved secure system, even if the record is password-protected or encrypted (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*).[14] Before posting anything on any publicly-accessible Internet website—including on TSA Internet website www.tsa.gov—personnel must evaluate whether the content could *possibly* constitute SSI. Content is not limited to documents but could also be in the form of photos, video, audio recordings, social media

[13] Designation as an SSI System and completion of required system security authorization in accordance with *DHS Sensitive Security Systems Policy Documents (4300A)* and *TSA Information Assurance Handbook* satisfies this need for explicit approval.

[14] Secure Internet sites approved for handling SSI are addressed in Section 12.0, *Protection Requirements for SSI Systems & Other Secure Sites.*

posts, etc. All personnel are obligated to protect SSI from posting to the Internet, whether the posting is made at work or off-duty. ***Note:*** *Internet posts can take many forms including posts on social networking and job-hunting sites.*

Before TSA personnel post any information to the Internet, they must certify that the information is not SSI by following the steps below. ***Note:*** *Following this process does not remove the employee's responsibility to obtain supervisory approval prior to posting content related to work to a publicly accessible website.*

- If the information *could possibly* be SSI, personnel must send a record (e.g., document, video) containing the information in question to the SSI Program office for an SSI Assessment (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*).
- If the SSI Program office determines the record contains **no SSI**, the information may be posted on the Internet.
    - Each office posting to the Internet must retain records, subject to their office's records retention schedule, of the SSI Assessment conducted and the finding that the information was **not SSI.**
- If the record *does* contain SSI, the requesting TSA personnel submit the record to the SSI Program office for an SSI Review to identify the specific SSI and must have the record edited to remove the SSI or have an Authorized Redactor redact the SSI before posting the information (See also TSA MD 2800.21, *Document Redaction*).
    - **Best Practice:** Sometimes, after an electronic record is edited to remove SSI, SSI content remains in the metadata of the record. [15] If SSI is removed from a record, a simple way of ensuring the metadata does not remain is by ensuring all track changes are resolved and removed, copying all the non-SSI content, and pasting the non-SSI content into a blank (new) record.

5.2.2 TSA Shared Network Resources: Shared Drives, Systems, & TSA Intranet

SSI protection requirements for TSA shared drives, systems, and Intranet are the same. These shared network resources are on a restricted (i.e., closed) computer network. Often, a large community of people can access shared networks resources if they are granted permission.

SSI may be stored without passwords on TSA shared network resources, including on classified networks, and within the various TSA sites as long as access is limited to covered persons with a determined need to know, and the records are properly marked. Owners[16], Information System Security Officers (ISSOs), and administrators must periodically review the security settings and user permissions for locations that contain SSI, verify access is limited to only those covered persons with a need to know, and promptly remove access for those individuals who no longer have a need to know the SSI.

5.2.2.1 Shared Drives and OneDrive

Shared drives enable TSA offices to store, search, and access files from any TSA-issued device and between team members. Although SSI is permitted within these drives, each office is responsible for

[15] Electronically-stored data that provides information about other data (e.g., track changes, author, creation, etc.).
[16] i.e., system owners, content owners, and/or team/site owners, depending on the platform in question.

periodically (i.e., quarterly) reviewing the permissions for the folder to ensure any stored SSI is only available to those who have a need to know the information (See also Subsection 5.2.2, *TSA Shared Network Resources: Shared Drives, Systems & TSA Intranet*) and employee access is removed when they no longer have a need to know (e.g., upon leaving the current assignment).

OneDrive is used by each individual on the TSA domain. Each user is permitted to store sensitive information within their OneDrive and is responsible for ensuring any records stored there are shared only with those who have a need to know the information.

5.2.2.2 TSA Systems and Applications

Some systems, databases, and applications within the TSA domain or within the TSA Intranet may contain SSI. ISSOs for IT systems must complete an SSITA and, if the system contains SSI, may be required to complete an SSIIA (See also Section 11.0, Determining *SSI Systems*). Each system or application should have clear user guidance regarding the sensitivity of the information and any system-unique instructions for marking, handling, and sharing SSI within the system (See also Job Aid: *SSI Marking Considerations in Systems*) and when exporting (i.e., removing) from the system.

For information on how to protect SSI through other SSI Systems and other secure sites, see Section 12.0, *Protection Requirements for SSI Systems & Other Secure Sites.*

5.2.2.3 TSA Intranet (e.g., Teams, SharePoint)

Sharing SSI through TSA collaborative applications such as TSA SharePoint is permitted as long as access is limited to covered persons with a need to know, and the information is appropriately marked (See also Subsection 4.1, *Marking Records & Media Containing SSI*). On TSA SharePoint, this is accomplished by clearly identifying sites on which SSI may be posted (e.g, banner, label). Posting of SSI must follow the procedures as defined in Table 2 below. Personnel must also check and adhere to sensitivity requirements set by the site administrator for each site.

Offices must examine the SharePoint site's permissions periodically (i.e., quarterly) to ensure everyone with access to the site has a need to know the information contained therein. In addition to these requirements, site administrators must label the site to clearly indicate which type of sensitive information is permitted on the site. In the event there is external (non-TSA) sharing from the site, consult with the SSI Program at SSI@tsa.dhs.gov for tailored guidance for marking and SSI awareness materials for the site.

Offices may create custom connections (e.g., form lists) with SharePoint to access and store data within the TSA domain. However, site owners are responsible for ensuring appropriate site permissions are established and transfer of data to and from other TSA systems is conducted securely (See also Subsection 5.2.3, *Encrypting SSI in Transmission and Storage*). Search engines for SharePoint must not provide visibility to approved SSI locations to individuals without explicit access.

Table 2: SSI Posting Guidance for SharePoint		
Location	**Who Has Access?**	**Okay to Post SSI?**
TSA SharePoint	Most TSA Personnel. Some parts of TSA SharePoint are open to all DHS personnel through DHS Connect.	**NO** SSI on high-level TSA SharePoint sites (i.e., ustsa.sharepoint.com/sites). Note: TSA may occasionally choose to publish a video containing SSI. In these instances, the videos are clearly marked and intended for distribution to TSA.
Office Sites	Persons granted permission by the site administrator; some office sites deliberately have open access to large audiences.	Yes, with *restricted permission to the people with a determined need to know.*
OneDrive	Only the individual and other personnel to whom the individual has specifically granted access.	Yes, as long as only those with a need to know the information have access and the record is properly marked.

Similar to SharePoint, TSA Teams has the ability to store and share information. Within TSA Teams, SSI may be shared in the body of a chat session, through the call features, and in the Teams collaborative spaces. Each TSA office, organization, and team may create, store, and/or share SSI via any SharePoint and TSA Teams medium as long as access is limited to covered persons with a need to know and the information is appropriately marked (see also Subsections 4.1, *Marking Records & Media Containing SSI* and 5.2.2.4, *Teleconferencing and Information-Sharing Applications*).

TSA Teams and SharePoint contain sensitivity label options "*Sensitive Information Allowed -*" and "*No Sensitive Information Allowed*" for "TSA Only" or "TSA and DHS Only."[17] Some SharePoint sites still maintain a classic view with banners indicating if sensitive information is permitted on the site. The team or site owner must determine the appropriate sensitivity label or banner when standing up the site and is responsible for monitoring that site users adhere to the sensitivity marking. In addition to these requirements, team and site owners must clearly indicate on the site which types of sensitive information are permitted. TSA personnel must check and adhere to sensitivity requirements for each page/team site (See also Job Aid: *Marking Considerations in SSI Systems*).

5.2.2.4 Teleconferencing and Webinar Applications

TSA and DHS-hosted secure[18] applications are authorized to transmit SSI. TSA and DHS Teams, Cisco WebEx, Jabber (i.e., soft phone), TSA's video teleconferencing technology (VTC) system, and Homeland Security Information Network (HSIN)-hosted Adobe Connect are the only applications approved for use for SSI at this time. All other teleconferencing and webinar applications (e.g., Zoom), including external systems[19], are not permitted for handling, storing, or transmitting SSI.

[17] Sensitivity labels will be persistent and carry through to the subordinate Teams sites by default.
[18] Systems managing sensitive information must comply with DHS Directive 4300A, DHS Sensitive Systems Policy.
[19] Should a meeting be held through externally-hosted virtual meeting software; discussions which will contain SSI may only be held through a separate unmonitored teleconferencing line.

Personnel may discuss and/or display SSI using video, conferencing, and chat features in approved applications as long as all participants are covered persons and have a need to know the information. If an individual's identify cannot be verified or need to know cannot be established, SSI must not be shared. Organizers of virtual meetings should restrict access to intended invitees who have a need to know the information, and shall verify attendance during the conference to ensure that only covered persons with a need to know are present during the meeting.

TSA virtual meetings may be recorded only when the recording is stored on a user-restricted TSA internal system (***Note:*** *This is default for TSA VTC systems*), such that the information cannot be accessed by a person who does not have a need to know. SSI data from a virtual meeting may not be stored on a non-federal system.

Personnel shall not have calls monitored by any non-covered personnel servicing the call and must suspend discussion and/or display of SSI during any period when a non-covered person is present (e.g., while a person is present providing technical support for the call).

5.2.3 Encrypting SSI in Transmission and Storage

Records containing SSI must be encrypted within all email, even within DHS, as well as during other types of electronic transmission traveling outside the DHS domain. SSI must never be placed in the body or subject line of an email and must be encrypted separately, *unless an email encryption method is available*. When M365 Exchange (i.e., TSA email) is protected with encryption, SSI is not required to be separately password-protected by the user *within* TSA email (i.e., from and to recipients with TSA email addresses) on TSA-authorized devices.[20] SSI sent without email encryption or sent *outside* of TSA must still be separately encrypted (See also Subsection 5.3.3, *Methods for Applying Encryption to SSI*.) SSI must be encrypted in other forms of electronic transmission and storage as detailed in the *TSA Information Assurance Handbook*.

Images or video which may contain SSI may be transmitted within the mobile device security sandbox (e.g., BlackBerry software) on TSA-authorized devices for operational needs. For example, an image of a suspect item taken within the BlackBerry software and transmitted to a TSS-E for evaluation is authorized. TSA personnel must apply SSI markings on images or video which may contain SSI as soon as operationally viable. SSI markings may be removed and other protection requirements cease only once the image or video has been assessed to not contain SSI. For more information, see Subsection 3.3, *Conducting SSI Assessments*.

Note: *Other methods of encrypting a record for transmission may be established by the SO in coordination with the TSA IT and the SSI Program and consistent with* Technical Standard (TS) 002, *Encryption*. For guidance on password use, see Subsection 5.3, *Passwords*.

5.2.4 Electronic Devices

SSI may be stored on TSA-issued government furnished equipment (GFE) (i.e., laptops, mobile electronic media [MEM] such as USB flash drives) without user-level encryption as long as the device itself meets TSA IT security requirements.[21] All sensitive TSA data must also be encrypted when stored on removable media (e.g., disks or CDs) and, therefore, requires additional user-level protection (See also Subsection

[20] Exchange Online encryption is FIPS 140-2 compliant for transmission of sensitive information.
[21] All TSA data must be encrypted when stored on GFE such as laptops or portable drives (e.g., USB flash drives). TSA GFE, by default, is encrypted.

5.3, *Passwords*). SSI may not be stored outside of the mobile device security sandbox (i.e., BlackBerry software) on TSA-approved iOS/iPhone devices.

Personnel must not open, view, process, download, or store SSI on non-GFE, including computers, cell phones, USB flash drives, portable hard drives, or other MEM that are not approved by TSA IT. Non-TSA devices may not be connected to TSA equipment. See also TSA MD 1400.3, *Information Technology Security*, its associated Attachment 1, *TSA Information Assurance Handbook*, and the DHS Sensitive Security Systems Policy Documents (4300A).

Per the DHS 4300A, version 11.0, 5.4.6.i, "*Auto-forwarding or redirecting of DHS email to any address outside of the .gov or .mil domain is prohibited. Users may manually forward individual messages after determining that the risks or consequences are minimal.*" SSI may not be sent to contractor emails unless the contract company specifically completes the SA process with TSA IT. ***Note:*** *See the contracting officer's representative (COR) for assistance.*[22] Additionally, personnel must not forward emails containing SSI to personal email addresses (e.g., Gmail, Yahoo).

SSI must be sanitized from all electronic media before resale, disposal, or reuse outside of the agency. For more information, see Section 7.0, *Destruction of SSI*.

Note: *For information on traveling with TSA-owned equipment that contains SSI, see Subsection 5.2.10, Removing SSI from the Workplace (Traveling with SSI). See also Section 7.0, Destruction of SSI for more information on handling information on electronic devices.*

5.2.5 Scanners, Copiers, & Printers

When scanning, copying, or printing records containing SSI, personnel must employ safeguards to protect the SSI and ensure it cannot be accessed or stolen by non-covered persons or covered persons who do not have a need to know.[23] Reproducing SSI using these methods often places the data in shared locations that can be accessed by multiple individuals over a network or through direct, physical access if proper security measures are not implemented.

Personnel shall only process records containing SSI using TSA-owned GFE in TSA facilities by covered persons with a need to know. However, 3rd party equipment, facilities, and services (e.g., Kinko's, FedEx, or Staples) may be used if purchased through the acquisition process in accordance with the Government Printing Office (GPO) Simplified Purchase Agreement (SPA) program requirements.[24] TSA contractors scanning or reproducing SSI material in the performance of their contract shall use TSA-owned GFE or their respective contractor-owned equipment for processing SSI. Use of other 3rd party equipment shall require prior approval of the COR. Processing SSI on non-GFE not approved for use by TSA IT is prohibited.

Personnel should use caution to print to the correct location. For scanners, copiers, and printers, password-protection and data encryption are considered minimum requirements for SSI data at rest and in transit. The CISO shall provide procedures and instructions in cases where this functionality is not

[22] See also TSA IT IAD's Security Authorization SOP. Contact IAD's Governance, Risk, and Compliance Branch for assistance initiating a risk assessment and approval.

[23] Many scanners, copiers, and printers have the ability to password-protect so that the document is only retrievable by the intended audience. When available, these features should be employed to properly protect SSI. See Job Aid: *Protected Printing and Scanning* for more information.

[24] Through the SPA program, GPO issues agreements with third party document reproduction facilities on behalf of the requiring agency. The GPO also has their own printing facilities which may be used for sensitive material reproduction. Requests for processing SSI through GPO must be submitted to Contracting & Procurement.

available. Passwords created to encrypt information and the encryption itself shall be compliant with TS-001, *Passwords* and TS-002, *Encryption* respectively. See also Section 7.0, *Destruction of SSI* for more information.

Personnel must conduct proper sanitization and disposition of media used to process SSI as it is critical to ensuring confidentiality before being decommissioned or reallocated. Printing, scanning, and copying devices typically contain persistent memory such as hard drives or internal flash memory to store data. TSA and DHS disposition requirements[25] prohibit this media from leaving the facility and require that it be destroyed on-site. All associated sanitization and disposition of media used to process SSI shall be consistent with the *TSA Information Assurance Handbook,* including Section 3.10, *Media Sanitization*. See also TS-046, *IT Media Sanitization and Disposition*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, for guidance on destruction of SSI on electronic media by using any of the designated methods, and DHS Sensitive Security Systems Policy Documents (4300A) for more information.

Note: *Exceptions to this policy may be approved by the SSI Program Chief on a case-by-case basis. Field requests for exceptions must be routed though the respective operational chain-of-command and TSA headquarters office to the SSI Program Chief as the approving authority.* TSA Form 1408, IT Waiver/Exception Request *with AO approval may be required if the policy exception is related to an Information Assurance policy requirement*.

5.2.6 Faxes

Use of facsimile (fax) is discouraged unless using a more-secure option, such as sending a protected scan of the record via email, is not feasible. Personnel may send records containing SSI via fax[26] as long as the recipient is a covered person with a need to know. Before sending the fax, personnel must (1) complete the SSI Fax Cover Sheet; (2) verify that the fax number of the covered person is correct and current; and (3) verify that either the recipient is standing by to receive the faxed record or that the fax machine is in a secure area accessible by only those with a need to know the SSI. See also Subsection 5.2.5, *Scanners, Copiers, & Printers* for information on configuring, maintenance, or disposal of fax machines.

5.2.7 Telephone

Personnel may discuss SSI over the phone, to include FaceTime on iOS (e.g., iPhone) devices, as long as all persons present are covered persons with a need to know. Personnel must not discuss SSI if their conversation can be overheard by someone who is not a covered person or who does not have a need to know. Personnel must be aware of their surroundings when using a speakerphone. Text messaging SSI, even on government furnished cell phones, is prohibited outside of the mobile device security sandbox (e.g., BlackBerry, Teams) (see also 5.2.3, *Encrypting SSI in Transmission and Storage*).

Use of landline phones or the TSA-approved Voice Over Internet Protocol (VOIP) system (e.g., TSA Headquarters phone system) when discussing SSI is preferred. When using TSA-encrypted radios, walkie-talkies, or other mobile computing devices to discuss SSI, take precautions to discuss SSI sparingly and privately.

[25] Refer to DHS Sensitive Security Systems Policy Documents (4300A), Attachment DD, Section 11.7 and 11.8 for further detail.

[26] TSA use of fax machine must be from a TSA-approved fax from the authorized products list. Any use of fax besides from the authorized products list must be approved by the Authorizing Official (i.e., TSA CIO).

5.2.8 Packaging & Delivering SSI

When personnel need to hand-deliver SSI, send it through the mail, or carry it from one location to another, they must follow the procedures below in order to minimize the risk of loss or improper disclosure. While packaging records containing SSI, personnel must ensure that the records are properly marked. See also Subsection 4.1, *Marking Records & Media Containing SSI*.

Table 3: Guidance on Packaging SSI

U.S. Mail (including U.S. authorized commercial delivery services such as FedEx, UPS, etc.) Interoffice Mail	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required). 2. Use an opaque (non-see through) envelope, wrapping, or carton. 3. Do not mark the envelope or outside wrapping with the SSI header or footer or any other indication of the contents' sensitivity. 4. Address with an attention line containing the name and office of the intended recipient. 5. For U.S. Mail, send by USPS First Class certified mail or another traceable delivery service requiring signature upon delivery. 6. Validate that the shipment arrived to the appropriate location.
Hand-carrying (on-site)	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required). 2. Do not leave SSI unattended or unlocked in the recipient's workspace.
Hand-carrying (off-site)	1. Attach the SSI Cover Sheet, DHS Form 11054, to the records (encouraged but not required). 2. Place material in an opaque (non-see through) envelope or case. 3. Do not leave SSI unattended or unlocked in the recipient's workspace.

When personnel must transfer large quantities of data, such as thousands of scanned images, mobile electronic media (e.g., hard drive, USB flash drives) may need to be sent to the intended recipient[27]. In the case of sending mobile electronic media containing SSI, personnel shall use the following procedures:

- Use only media that are TSA-approved and encrypted; send the password separately;
- Double-wrap the media using tamper-resistant wrapping;
- Ship the media using FedEx, UPS, or U.S. Mail (Certified) with a tracking number; and
- Validate that the shipment arrived to the appropriate location.

Shipping of SSI to overseas offices is permitted only when approved by International Operations (IO) or the office is serviced by a U.S. Embassy, Consulate, or military postal facility (i.e., APO/FPO). When the overseas office is not serviced by a U.S. Embassy, Consulate, or military postal facility, the materials will be sent through IO, the Department of State, Diplomatic Courier or TSA employee traveling on official business. See also Subsection 5.2.10, *Removing SSI from the Workplace (Traveling with SSI).*

[27] In the event that a drive is being transferred from a non-TSA partner, personnel must work with their IT POC to have the drive scanned prior to use on a TSA system.

When moving SSI to a new office or location, the SSI only needs to be locked up so that it cannot be accessed or tampered with by those who do not have a need to know. This includes any method which secures the SSI and/or reveals any attempts of tampering with the containers, such as a box sealed with security tape, a moving crate with a zip-tie, or an actual lock on a case. The moving/storage company must provide a level of security in transport and storage so that the information is not susceptible to theft.

5.2.9 SSI Handling during Telework and Remote Work

SSI should be protected at the telework or remote work location in the same manner as when in the office including (but not limited to):

- Do not discuss SSI if non-covered persons may overhear the discussion.
- Limit visibility of the computer screen when conducting TSA business and lock the screen when not in use or whenever the computer may be unattended.
- Maintain positive physical control over the SSI (such as keeping paper copies of SSI locked in a secure container when not in use) so it is not accessible by non-covered persons or those who do not have a need to know the information.

Personnel shall only process electronic files containing SSI using TSA-approved devices (e.g., VPN-enabled TSA laptops). Permission to process SSI on GFE (i.e., TSA-issued computers and devices) is implied by a signed telework or remote work agreement. Personnel shall not use non-GFE (e.g., computers or other electronic devices) to process SSI (See also Section 13.0, *SSI Policy Exceptions* for information regarding times of national emergency or exigent circumstances). Storing SSI on non-GFE devices is prohibited. Use only TSA-approved conferencing platforms for work involving SSI as detailed in Subsections 5.2.7, *Telephone* and 5.2.8, *Virtual Meetings*.

Personnel must obtain permission from their supervisor before handling hard-copy (i.e., paper, disks) SSI in a telework or remote work location. Contract employees must obtain permission from the contracting officer representative (COR) before removing SSI from the workplace.

5.2.10 Removing SSI from the Workplace (Traveling with SSI)

Personnel must obtain permission from their supervisor (for contractors, their COR) before removing SSI from the work place. While traveling, personnel shall maintain positive physical control over any hard-copy (i.e., paper) SSI and electronic devices[28] containing SSI whenever possible. If circumstances require SSI to be left unattended in a vehicle, the vehicle must be locked and the SSI material, or any container holding the material, must not be left in plain view. If circumstances require SSI to be left unattended at any time during travel (e.g., in a hotel room), secure the SSI in a locked container (e.g., hotel room safe[29], locked bag) to prevent unauthorized access to the SSI by others, including co-habitants, intruders, or hotel staff. Per TSA's *Computer and Wireless Mobile Device Access Agreement* (TSA Form 1403), TSA personnel are responsible for providing physical security for the TSA-issued computer, laptop, or wireless mobile device and keeping such equipment under exclusive and strict control.

The guiding principle for securing SSI during travel is to take all reasonable steps necessary to protect SSI from access by non-covered persons or those without a need to know the information. For more information, see resource *Protecting SSI and Sensitive PII Away from the Workplace*

[28] See also TSA MD 1400.3, *Information Technology Security*, its associated Attachment 1, *TSA Information Technology Security Handbook* for additional IT security requirements on removable media.

[29] If there is no hotel room safe, SSI may be stored in a hotel safe in a sealed, tamper-evident envelope.

5.3 Passwords

Personnel must ensure proper protection of SSI created, stored, processed, or transmitted to limit access to covered persons with a need to know. See below for guidance on how to encrypt information.

5.3.1 Standard TSA Password

Personnel may use the Standard TSA Password when sharing SSI[30] with other TSA, DHS, and component personnel who have a need to know and are within the DHS network.[31] TSA's SSI Program office creates a new Standard TSA Password[32] on a 90-day cycle or in response to a password breach (See also Subsection 5.3.6, *Password Incidents*) and posts the updated password to the SSI Password Finder application on Salesforce. SSI Coordinators may then distribute this password to personnel within their area of responsibility who have a need to know the Standard TSA Password. For the current Standard TSA Password, personnel should contact their designated SSI Coordinator.

Individuals who routinely require access to historic passwords may request access to the SSI Password Finder application from their SSI Coordinators using the SSI Password Finder Job Aid. SSI Coordinators must periodically review the list of those who have access and contact the SSI Program to remove an individual's access as needed. Personnel must protect all historic password lists and applications as SSI. Personnel must not maintain a personal or office list of historic Standard TSA Passwords nor print or further distribute such lists. Personnel must not use the password application to build a historic password list.

To disclose SSI to covered persons outside of DHS, personnel must not use the Standard TSA Password and must instead use the External TSA Password, or create a personal password instead of the Standard TSA Password to protect the SSI in transmission (See also Subsections 5.3.2, *External TSA Password*, and 5.3.3, *Creating Passwords to Encrypt SSI*). A password incident occurs when the Standard TSA Password is shared outside of DHS (See Subsection 5.3.5, *Password Incidents*).

5.3.2 External TSA Password

Personnel may use the External TSA Password when sharing SSI with covered persons who have a need to know and are outside of the DHS network[33]. TSA's SSI Program office creates a new External TSA Password on a 90-day cycle or in response to a password breach (See also Subsection 5.3.5, *Password Incidents*) and posts the updated password to the SSI Password Finder application on Salesforce. SSI Coordinators may then distribute this password to personnel within their area of responsibility who have a need to know the External TSA Password. For the current External TSA Password, personnel should contact their designated SSI Coordinator.

[30] To lessen the administrative burden created by maintaining multiple standard passwords across TSA, the Standard TSA Password may also be used to protect other sensitive information within TSA, as necessary.
[31] Access is not limited to federal employees. Contractors, including at Screening Partnership Program (SPP) airports, may receive the password as determined by local SSI Coordinators. DHS network is determined by whether they have a DHS email address ending in "dhs.gov".
[32] The Standard TSA Password is also known as the TSA National Password or the TSA SSI Password. For consistency and to reduce confusion, please use the term "Standard TSA Password."
[33] DHS network is determined by whether they have a DHS email address ending in "dhs.gov". TSA, DHS, and component personnel may also have access to the External TSA Password, as needed.

Individuals who routinely require access to historic passwords may request access to the SSI Password Finder application from their SSI Coordinators using the SSI Password Finder Job Aid. Personnel must protect all historic passwords and applications as SSI. Personnel must not maintain a personal or office list of historic Standard or External TSA Passwords nor print or further distribute such lists. Personnel must not use the password application to build a historic password list. A password incident occurs when the External TSA Password is shared with individuals without a need to know. (See Subsection 5.3.6, *Password Incidents*).

5.3.3 Creating Passwords to Encrypt SSI

Passwords must be consistent with TS-001, *Passwords*. The TSA standard for encryption of sensitive information is AES-256 bit or higher encryption (See TS-002, *Encryption*). When creating passwords to encrypt records containing SSI, personnel must follow the below criteria:

- All passwords must:
  a. Be at least eight characters in length;
  b. Have at least one upper-case and one lower-case letter;
  c. Contain at least one number; base 10 digits (e.g., 0 through 9);
  d. Contain at least one symbol (e.g., *&^%$#!); and
  e. Not be a word in the dictionary, a portion of the file name, or identifying information of an individual.
- Personnel may use the same password for multiple documents shared between the same sender and recipient.
- Passwords created to protect SSI must be changed every 90 days.

5.3.4 Methods for Applying Encryption to SSI

The following table provides guidance on which types of electronic systems and devices require encryption when storing SSI:

Table 4: Encryption Standards for Various Media*

Type of Media	Encryption Required?
Email (Within TSA network)	Yes. When sending within an encrypted email, individuals must mark the email as containing sensitive information (See also Subsection 4.1, *Marking Records & Media Containing SSI*). SSI is not authorized in the subject line of emails.
Email (Outside TSA network)	Yes. Encrypt SSI in an attachment to the email. SSI is not authorized in the body or subject line of emails. Send the External TSA Password or personally-created password in a separate email or communication channel (e.g., phone).
Shared Network Folders	No. User-level encryption (i.e., password) is not required as long as the folder is restricted to those with a need to know.
Internet Sites	Posting SSI to the Internet (i.e., publicly-accessible sites) is strictly prohibited, even if it is password-protected or encrypted.

Individuals who routinely require access to historic passwords may request access to the SSI Password Finder application from their SSI Coordinators using the SSI Password Finder Job Aid. Personnel must protect all historic passwords and applications as SSI. Personnel must not maintain a personal or office list of historic Standard or External TSA Passwords nor print or further distribute such lists. Personnel must not use the password application to build a historic password list. A password incident occurs when the External TSA Password is shared with individuals without a need to know. (See Subsection 5.3.6, *Password Incidents*).

5.3.3 Creating Passwords to Encrypt SSI

Passwords must be consistent with TS-001, *Passwords*. The TSA standard for encryption of sensitive information is AES-256 bit or higher encryption (See TS-002, *Encryption*). When creating passwords to encrypt records containing SSI, personnel must follow the below criteria:

- All passwords must:
  a. Be at least eight characters in length;
  b. Have at least one upper-case and one lower-case letter;
  c. Contain at least one number; base 10 digits (e.g., 0 through 9);
  d. Contain at least one symbol (e.g., *&^%$#!); and
  e. Not be a word in the dictionary, a portion of the file name, or identifying information of an individual.
- Personnel may use the same password for multiple documents shared between the same sender and recipient.
- Passwords created to protect SSI must be changed every 90 days.

5.3.4 Methods for Applying Encryption to SSI

The following table provides guidance on which types of electronic systems and devices require encryption when storing SSI:

Table 4: Encryption Standards for Various Media

Type of Media	Encryption Required?
Email (Within TSA network)	Yes. When sending within an encrypted email, individuals must mark the email as containing sensitive information (See also Subsection 4.1, *Marking Records & Media Containing SSI*). SSI is not authorized in the subject line of emails.
Email (Outside TSA network)	Yes. Encrypt SSI in an attachment to the email. SSI is not authorized in the body or subject line of emails. Send the External TSA Password or personally-created password in a separate email or communication channel (e.g., phone).
Shared Network Folders	No. User-level encryption (i.e., password) is not required as long as the folder is restricted to those with a need to know.
Internet Sites	Posting SSI to the Internet (i.e., publicly-accessible sites) is strictly prohibited, even if it is password-protected or encrypted.

Intranet (including SharePoint) and other secure sites	No. User-level encryption is not required as long as access to the site is restricted to those with a need to know and the site/system is not searchable by individuals without access (See also Table 2*: SSI Posting Guidance for SharePoint*).
Messaging	No. Additional encryption is not required for SSI sent in TSA-approved/provided messaging platforms (e.g., Teams). Individuals must mark messaging as containing sensitive information (See also Subsection 4.1, *Marking Records & Media Containing SSI*).
Scanners	Yes. Use encryption when possible. When not possible, immediately delete any files in queue.
Fax	No. However, TSA use of fax must be on a TSA-approved device (See also Subsection 5.2.6, *Faxes*).
Databases	No. Additional user-level encryption is not required as long as the database has access restricted to covered persons with a need to know.
CDs and DVDs	Yes. Whenever possible, encrypt all records that contain SSI.
Mobile Electronic Media (e.g., Removable Hard Drives, USB Flash Drives)	No. The device must be a TSA-approved encrypted media; the files do not need to be individually encrypted.

See Job Aid: *Applying and Removing Encryption to Transmit SSI* for instruction using the most common methods used to encrypt records. Other encryption methods shall adhere to the requirements of *TSA Information Assurance Handbook*, Subsection 3.1, *Access Control* and *TS-002, Encryption.* Individuals must mark the email as containing sensitive information. See also Subsection 4.1, *Marking Records & Media Containing SSI*.)

5.3.5 Transmitting SSI Passwords

The Standard TSA Password or other password may be shared (See also Subsection 5.3.2, *Creating Passwords to Encrypt SSI*) in person, over the telephone, in a voicemail message, or in an email with no subject line or with a non-descript subject line. Do not reply to the original email with the password. This email *must not* contain the record the employee is trying to protect.

Personnel must not forward the Standard TSA Password outside of DHS (See also Subsection 5.3.1, *Standard TSA Password*). ***Best Practice:*** *If the document will likely get forwarded beyond DHS to other covered persons with a need to know the information, create a separate password to help reduce the number of SSI Password incidents.*

5.3.6 SSI Password Incidents

An SSI password incident occurs when either (1) a password created to encrypt SSI is inappropriately shared with covered persons in a manner not in accordance with this Handbook (See also Subsection 5.3.5, *Transmitting SSI Passwords*); or (2) the Standard TSA Password is shared with persons outside of DHS. See also Subsection 10.3, *Password Incident Response & Resolution*.

6.0 Disclosure of SSI

According to the SSI Regulation, records containing SSI are not available for public inspection or copying. As such, TSA does not release records containing SSI to non-covered persons or covered persons who do not have a need to know. The SSI Regulation does, however, provide for authorized disclosure of SSI to the groups and persons described below.

6.1 Determining Covered Persons with a Need to Know

Generally, a covered person is an individual or entity who has transportation security or transportation security-related responsibilities to include, but not limited to, (1) anyone who is permanently or temporarily assigned, attached, detailed to, employed by, or under contract with DHS; (2) regulated parties, Federal, State, Local and tribal government employees, contractors, and grantees, as well as TSA stakeholders and industry partners; (3) Committees of Congress; (4) other persons with a need to know as defined in § 1520.11; and (5) persons receiving SSI pursuant to other conditional disclosures. ***Note:*** *Just because an individual is a covered person does not mean they also have a need to know. Need to know determinations must be made on a case-by-case basis.* For a complete listing of covered persons or persons with a need to know, see the SSI Regulation at §§ 1520.7 and 1520.11 and Appendix 2: *Determining Need to Know Flow Chart*. For further guidance, consult the SSI Program office at SSI@tsa.dhs.gov.

Although an individual might be a covered person, TSA may also determine whether to make an individual's access to SSI contingent upon the satisfactory completion of a security background check (See also 6.9, *Vetting for Access to SSI*).

The SSI Program office provides additional guidance as to who is a covered person with a need to know:

- **Contractors/Subcontractors:** A DHS or TSA contract/subcontract employee automatically becomes a covered person for the purposes of performing the contract starting on the effective date of the contract. A subcontractor becomes a covered person for the purposes of performing the contract by virtue of the prime contractor's relationship with DHS or TSA. Although contractors and subcontractors become covered parties at the start of the contract, they are also subject to security vetting before receiving SSI. For vetting and approval to disclose SSI to contractors/subcontractors who are foreign nationals, see TSA MD 2810.3, *Management of Foreign Access to Sensitive Information*. ***Note:*** *For instances of subject-matter experts working for the contract company but not in performance of a contract or other nuances of a contract, work with the COR for appropriate handling.*

  The COR is responsible for ensuring all contractors/subcontractors complete required SSI training. A contractor/subcontractor will always be a covered person responsible for protecting SSI in accordance with the SSI Regulation, even after the termination or expiration of the contract. After the performance period of the contract, a contractor/subcontractor no longer has a need to know SSI unless they fit into another category of covered person.

- **Potential Offerors (i.e., Pre-Award Acquisition):** In some instances, potential offerors are not able to provide sufficient response to a TSA solicitation without receiving access to SSI. In these instances, there is a process for approving and documenting the authorization to disclose SSI in pre-award acquisition actions as well as the plan to safeguard SSI during disclosure; the written authorization serves as a conditional disclosure. See also TSA MD 2810.2, *Disclosure of SSI in the Pre-Award Acquisition Process*.

- **Other Contract-Like Agreements (e.g., Memorandum of Agreement (MOA), Bailment) and Other Transaction Agreements (OTAs):** Individuals involved in a contract-like agreement or OTA are acting in the interest of transportation security and are, therefore, authorized to receive SSI pertinent to the written agreement.
- **Research and development partners:** Occasionally TSA collaborates with research labs (e.g., Sandia, Transportation Security Laboratory [TSL]) or universities on joint projects. Research and development partners may be considered covered persons to the extent that they are working on behalf of the federal government. Any research projects involving the disclosure of SSI must have a written information protection agreement with SSI requirements in place, including the requirement to review and remove SSI before publication, through the appropriate contract or other contract-like agreement (e.g., MOA, Cooperative Research and Development Agreements [CRADA]). ***Note:*** *SSI may not be disclosed to individuals or groups soliciting information from TSA under the auspices of private research purposes or to be "helpful" to TSA. Information requests for private research must be submitted through the FOIA process.*
- **Aircraft manufacturers:** Aircraft manufacturers are covered persons whom may receive and produce SSI related to the vulnerabilities, research and development, and security of the aircraft.
- **Foreign nationals:** A foreign national becomes a covered person if they fit into one of the categories of covered persons or persons with a need to know. Permission to disclose SSI to foreign nationals who are transportation stakeholders (i.e., regulated entities such as air carriers[34]) need not be coordinated through the SSI Program office or IO. Additionally, foreign nationals who are contractors/subcontractors, potential offerors, and engaged in other contract-like agreements may, on a case-by-case basis, be granted access to SSI in support of the TSA mission. Such access is dependent upon: 1) TSA documenting how the disclosure is in the best interest of the government and 2) successful completion of vetting. See TSA MD 2810.3, *Management of Foreign Access to Sensitive Information.*
- **Foreign and domestic intelligence partners:** Foreign and domestic intelligence partners who are already authorized recipients of CNSI may receive access to SSI contained within intelligence products inherent to the nature of the partnership in the interest of transportation security.
- **Foreign governments:** There is an official process for determining whether information may be disclosed to foreign governments. Per TSA MD 2810.1, *Sensitive Security Information (SSI) Program*, IO has the delegated authority to determine appropriate sharing of SSI. Any disclosure of SSI to foreign governments must be coordinated through IO, as it maintains delegated authority to authorize the disclosure of SSI to select foreign governments and select foreign entities (e.g., foreign airports and regional/multilateral aviation security organizations) determined to have a need to know the information. Contact the SSI Coordinator for IO for assistance.
- **Personal representatives:** A TSA employee may designate an advisor to serve as their personal representative consistent with TSA policy.[35] Under the SSI Regulation, personal representatives are covered persons for purposes of access to SSI and may receive SSI when they have the requisite need to know (See also 49 C.F.R. §§ 1520.7(k), 1520.11(a)(4), and 1520.11(a)(5)). Therefore, the personal representative must abide by the TSA and SSI requirements for personal

[34] Foreign air carriers regulated by 49 C.F.R. Part 1546 are covered persons even when owned by a foreign government and may access SSI for which they have a need to know.

[35] Employees document designation using TSA Form 1163-1, *Personal Representative Designation*.

representatives, including signing a non-disclosure agreement (NDA) (See also Subsection 6.3, *Disclosure of SSI to AFGE and Personal Representatives*).

Suspicious requests for SSI should be reported immediately to your supervisor, SSI Coordinator, and the Insider Threat Unit at insiderthreat@tsa.dhs.gov.

6.2 Non-Disclosure Agreements

The SSI Program office does not make a practice of determining *when* an NDA should be administered to covered persons, appropriately leaving that responsibility to the program office/covered person disclosing the SSI. The following guidance on NDAs is provided to aid personnel in determining whether an NDA is appropriate for each individual situation. Personnel who have determined that use of an NDA is appropriate must use DHS Form 11000-6, *Non-Disclosure Agreements*, TSA Form 2815, *Terms and Conditions for Access to Sensitive Security Information Non-Disclosure Agreement*, or another equivalent document approved by CC. Typically, DHS Form 11000-6 is used for TSA personnel while TSA Form 2815 is recommended for individuals not familiar with SSI and/or not subject to TSA SSI Policies and Procedures. There is no prohibition on issuing both NDAs if the situation warrants additional guidance on SSI.

While the SSI Regulation does not speak to requirements for signing NDAs, they are a tool used by DHS and TSA to ensure that covered persons receiving sensitive information understand the responsibilities to protect that information.[36] NDAs should be executed prior to the disclosure of SSI and shall only be used to disclose information with covered persons who have a need to know the information. The signing of an NDA does not allow disclosing of SSI with non-covered persons.

It is good practice when addressing a group of covered persons who do not routinely handle SSI to provide them with the SSI Program office's *SSI Best Practices Guide for Non-DHS Employees*. The NDA is an additional measure the covered person disclosing the information may want to consider. Responsibility for ensuring a covered person receiving SSI understands the responsibilities entailed rests with the party disclosing the information. The SSI Program office generally advises those inquiring about NDAs to err on the side of caution by executing an NDA if the need is not clear. The program offices are responsible for maintaining NDAs by their program in accordance with TSA Records Retention Schedules. In the case of contractors, the COR maintains the NDAs within the contract files.

6.3 Disclosure of SSI to AFGE and Personal Representatives

On June 29, 2011, the Federal Labor Relations Authority (FLRA) certified the American Federation of Government Employees (AFGE) as the exclusive representative of bargaining unit employees at the TSA.[37] Consistent with this certification, made under the TSA Administrator's February 4, 2011,

[36] As examples, CC may require NDAs be signed in certain litigation access procedures and other offices have developed internal policies requiring NDAs be signed when providing SSI to stakeholders and contractors; Acquisition, when providing some contractors with SSI, requires NDAs be signed and maintained by the COR; and some TSA systems designed for stakeholder use contain NDA language in the terms of use.

[37] Bargaining unit employees are full and part-time non-supervisory personnel carrying out screening functions under 49 U.S.C. § 44901, as that term is used in ATSA, § 111(d); specifically, Transportation Security Officers, Lead Transportation Security Officers, Master Transportation Security Officers (which include Security Training Instructors, and Equipment Maintenance Technicians), and Expert Transportation Security Officers (which include Security Training Instructors, and Equipment Maintenance Technicians).

Determination on Transportation Security Officers and Collective Bargaining[38] and AFGE's status as the union representative under the 2020 Collective Bargaining Agreement (Rev. November 9, 2021), and as explained herein, AFGE holds a status as a covered person under 49 C.F.R. Part 1520.

- AFGE as a Covered Person: The SSI Regulation does not explicitly address a union's status as a covered person, for the purposes of collective bargaining or a union's need to know SSI. However, section 1520.7(k) is applicable to "[e]ach person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position." Therefore, TSA determines that AFGE, as the certified exclusive representative of bargaining unit employees and acting in the collective interests of bargaining unit employees under the Determination, is a covered person under section 1520.7(k). TSA authorizes the disclosure of SSI to AFGE contingent upon the specific conditions of access and terms for protection of SSI detailed below.
- AFGE Representatives Serving as Personal Representatives: A TSA employee may designate an AFGE representative to serve as their personal representative consistent with TSA policy and § IV.A.4 of the Determination. When serving as a personal representative, the AFGE representative is serving in their personal capacity and not in their capacity as an AFGE representative. Under the SSI Regulation, personal representatives are covered persons for purposes of access to SSI and may receive SSI when they have the requisite need to know. *See* 49 C.F.R. §§ 1520.7(k), 1520.11(a)(4), and 1520.11(a)(5). Therefore, the AFGE representative serving as a personal representative must abide by the TSA and SSI requirements for personal representatives, including signing an NDA.

TSA has the regulatory authority, at 49 C.F.R. § 1520.11(c), to "*make an individual's access to the SSI contingent upon satisfactory completion of …other procedures and requirements for safeguarding SSI that are satisfactory to TSA….*" Pursuant to its authority under 49 C.F.R. § 1520.11(c), TSA has determined that, under the conditions stated below, AFGE may receive SSI when AFGE has the requisite "need to know" to perform its responsibilities under § IV.C.1.c of the Determination.

To receive such information, AFGE must abide by the following conditions:

(1) AFGE agrees not to disclose SSI to any other person or entity outside of AFGE or TSA without the expressed written permission of TSA, irrespective of whether that person or entity is a covered person under the SSI Regulation;

(2) AFGE recognizes and understands that every AFGE employee, AFGE contractor, and AFGE representative does not have the need to know required to receive SSI by virtue of their employment or affiliation with AFGE. AFGE employees, AFGE contractors, and AFGE representatives will only share SSI with other AFGE employees, AFGE contractors, and AFGE representatives who have the requisite need to know in that specific matter in order to receive the relevant SSI;

(3) AFGE understands that it is a covered person as defined in 49 C.F.R. § 1520.7 and is required to comply with the safeguarding and handling provisions of 49 C.F.R. Part 1520;

(4) AFGE will adhere to TSA's *SSI Quick Reference Guide for DHS Employees and Contractors*, which contains instructions for the proper handling and storing of SSI;

[38] The Determination, among other things, provides the purposes for which the exclusive representative of bargaining unit employees, AFGE, may receive SSI.

(5) AFGE, in consultation with TSA, will train all of its employees, representatives and contractors who are or may be working with TSA employees on the requirements of this Contingent Disclosure and the obligations regarding SSI; and

(6) AFGE will submit requests for access to SSI for the purposes defined in § IV.C.1.c of the Determination to Labor Management Relations to TSAPartnership@tsa.dhs.gov. Labor Management Relations, in conjunction with relevant TSA program offices, will determine whether AFGE has the requisite need to know to receive the requested SSI on a case-by-case basis.

The identified conditions are intended to safeguard SSI shared with AFGE against unauthorized disclosure, and failure to meet the conditions may result in civil penalty or other enforcement or corrective by DHS, as authorized by 49 C.F.R. § 1520.17.

6.4 Congress and Government Oversight (e.g., GAO, OIG)

Disclosures to Congress and Government Accountability Office (GAO) are covered in the SSI Regulation at § 1520.15, *SSI disclosed by TSA or the Coast Guard*. Per § 1520.15(c), records containing SSI may be disclosed to:

- Committees of Congress; and
- Comptroller General of the GAO or to any authorized representative of the Comptroller General.

Similarly, the Inspector General Act authorizes Inspector Generals (IGs) to initiate, conduct, supervise and coordinate audits, investigations, inspections and other reviews relating to the programs and operations of the Federal government. The Inspector General Empowerment Act of 2016 confirms that IGs have timely access to all records, reports, audits, reviews, documents, papers, recommendations, or other materials available related to the Federal programs and operations the IGs oversee.

DHS MD 0810.1, *The Office of Inspector General*, authorizes OIG to promptly access TSA officials and files, records, reports, or other information that may be requested either orally or in writing pursuant to its audit objectives.

- The directive indicates that DHS/TSA employees will provide "prompt access for auditors, inspectors, investigators, and other personnel authorized by the OIG to any files, records, reports, or other information that may be requested either orally or in writing" pursuant to its audit objectives.
- DHS/TSA employees are directed to cooperate fully by disclosing complete and accurate information pertaining to matters under investigation or review and informing OIG of any other areas or activities they believe require special attention.

6.4.1 SSI Disclosure to Congress

Any disclosure of SSI to Congress must be coordinated through Legislative Affairs (LA). To satisfy SSI statutory and regulatory provisions on disclosure to Committees of Congress, disclosure must be made to the Chairperson of a committee or subcommittee of Congress with jurisdiction[39] over TSA matters

[39] The following are committees/subcommittees with jurisdiction over TSA: House Committee on Appropriations; House Committee on Homeland Security; House Committee on Oversight and Reform; Senate Committee on Appropriations; Senate Committee on Commerce, Science, and Transportation; and Senate Committee on Homeland Security and Governmental Affairs.

relevant to their committee's authority, and committee staff members upon written request. Disclosure to Chairs and the committee staff members requires no additional regulatory documentation or approval.

Per TSA MD 2810.1, *SSI Program*, the Assistant Administrator (AA) of LA has the authority to disclose SSI to a Ranking Member of a committee or subcommittee of Congress with jurisdiction over TSA matters relevant to the committee's authority and committee staff members. The AA for LA may determine the need for and authorize the disclosure of SSI upon a determination that the disclosure is not detrimental to transportation security in accordance with 49 C.F.R. § 1520.15(e). Furthermore, the AA for LA shall take steps to ensure that any recipients of SSI fully comply with restrictions, procedural safeguards, and limitations on further dissemination in accordance with 49 C.F.R. Part 1520. This determination authority may not be further delegated beyond the AA for LA.

The determination and authorization process shall include:

- Documenting the specific SSI sought and how the SSI is relevant to the oversight jurisdiction of the committee.
- Coordinating with the program office/owner of the records being considered for release to a Ranking Member of a congressional committee or subcommittee and maintaining an auditable record of this coordination.
- Maintaining an auditable record, in accordance with the approved file plan, of the AA authorization for disclosure, the SSI that was disclosed and to whom it was disclosed, and any delivery instructions for protection.
- Limiting SSI disclosed under this section to the minimum amount necessary for congressional committees or subcommittees to effectively conduct their congressional oversight functions.

Finally, other Members of Congress, in their individual capacity, are not considered employees of the Federal Government[40] and the SSI regulation does not explicitly authorize the sharing of SSI with these Members. Other Majority and Minority members of committees with jurisdiction must request access through the Committee Chair or Ranking Member where approval is coordinated by Legislative Affairs and documented through a 15e signed by the Chief of the SSI Program, as needed. Requests for sharing with other Members of Congress or to Committees or Subcommittees without jurisdiction must be submitted to the SSI Program at SSI@tsa.dhs.gov for review.

6.4.2 SSI Disclosure to GAO

Any disclosure of SSI to GAO must be coordinated through Audit Liaison Division (ALD). Offices providing SSI to GAO must ensure that GAO has purview over the matter (i.e., matches congressional request for GAO's work as to subject, scope and objectives) for which they are seeking information that contains SSI. If the requested materials may likely or do contain SSI, immediately consult with the GAO audit liaison to raise/resolve SSI issues with the GAO audit team.

When transmitting, ensure the records are properly marked and protected as SSI with a password other than the Standard TSA Password (see also Subsection 5.3.2, *Creating Passwords to Encrypt SSI*). Ensure that all recipients of SSI are notified of the prohibition on further disclosure. TSA officials should make ALD aware of information provided to auditors so that a centralized record can be maintained. Procedurally, GAO coordinates a review of draft reports with the SSI Program through ALD to ensure SSI

[40] For the purposes of receiving SSI pursuant to 49 C.F.R. § 1520.11(b)(1).

is properly marked and protected in final reports. Any TSA response to audit recommendations should be coordinated through the SSI Program for SSI Review (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*).

6.4.3 SSI Disclosure to OIG

Any disclosure of SSI to OIG must be coordinated through Audit Liaison Division (ALD). Offices providing SSI to OIG must ensure that OIG has purview over the matter (i.e., request matches subject, scope, and objectives of audit). If the requested materials may likely or do contain SSI, immediately consult with the audit liaison to raise/resolve SSI issues with the OIG audit team.

When transmitting, ensure the records are properly marked and protected as SSI with a password, either a unique password or the Standard TSA Password (see also Subsection 5.3.2, *Creating Passwords to Encrypt SSI*). Ensure that all recipients of SSI are notified of the prohibition on further disclosure. TSA officials should make ALD aware of information provided to auditors so that a centralized record can be maintained. Procedurally, OIG coordinates a review of draft reports with the SSI Program through ALD to ensure SSI is properly marked and protected in final reports. Any TSA response to audit recommendations should be coordinated through the SSI Program for SSI Review (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*).

6.5 Freedom of Information Act (FOIA) Requests

When the public wants to view government-held information about transportation security, they may request the information under FOIA. Records containing SSI may be released only *after* all SSI has been properly redacted from the record. FOIA requests that may involve SSI are handled as follows:

- FOIA requests are routed to the TSA FOIA Office for processing;
- The FOIA Office gathers responsive records and determines if the records *may* contain SSI;
- The FOIA Office forwards records that may contain SSI to the SSI Program office for review;
- The SSI Program office identifies SSI in the records received from the FOIA Office and prepares a visually redacted version of the record; and
- The visually redacted version is sent to the FOIA Office for further processing and, before the responsive records are sent to the requester, the FOIA Office redacts the SSI identified by the SSI Program office in accordance with TSA MD 2800.21, *Document Redaction*.

6.6 State Open Records Requests

Similar to FOIA requests, many state laws (e.g., "Sunshine" laws) provide citizens the right to access government records. Certain exemptions may apply to these requests such as information that is confidential by law, either constitutional, statutory, or by judicial decision. While laws 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, or tribal public information and related laws. SSI falls under the SSI Federal Regulation, which preempts conflicting State, local, and tribal law. Processing requests within TSA should be handled as follows:

- 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 belonging to the state or transportation authority should be submitted for full SSI Review to the SSI Program.
- Requests may be submitted by the state agency directly to the SSI Program at SSI@tsa.dhs.gov or through TSA Field Counsel or a local SSI Coordinator using the SSI App on Salesforce. (See also Subsection 3.5, *Requesting an SSI Assessment or SSI Review from the SSI Program*.)
- Requests for SSI Assessments of video may be completed by Certified SSI Coordinators. SSI Coordinators shall document their determinations using the *SSI Assessment Findings Memo* template. ***Note:*** *SSI Assessment requests of video for a contentious incident should be sent directly to the SSI Program at Headquarters.*

6.7 Enforcement Proceedings

As defined in § 1520.11(a)(5), records containing SSI may be disclosed to persons in judicial or administrative enforcement proceeding when access to the SSI is necessary for the persons to prepare a response to allegations in a legal enforcement and/or personnel action proceeding.

Before granting access to SSI in an enforcement proceeding, TSA may require persons to undergo a background check with favorable results. Such disclosures must be handled by CC and the SSI Program office as defined in TSA MD 2810.1, *SSI Program*, (See also Subsections 6.2, *Non-Disclosure Agreements* and 6.9, *Vetting for Access to SSI*).

6.8 Other Conditional Disclosures

Specific records containing SSI may be conditionally disclosed to a non-covered person upon a written determination signed by the TSA Administrator or designee that disclosure would not be detrimental to transportation security. TSA may place limitations or restrictions on the disclosure and describe those limitations in the written determination, known as a 15(e) memo.[41] The requester of a 15(e) memo must supply the SSI Program office with the following information to develop the 15(e):

- The specific SSI proposed for disclosure;
- The background and purpose of the disclosure;
- Any proposed restrictions or limitations regarding the disclosure; and
- The benefit disclosure will have to transportation security.

One condition of disclosure may be the completion of a security threat assessment (STA) using TSA Form 2817B, *SSI Access Threat Assessment Questionnaire - Standard* (See also Subsection 6.9, *Vetting for Access to SSI).* Persons granted conditional disclosure by virtue of a 15(e) memo become covered persons under § 1520.7 of the SSI Regulation and have a duty to protect SSI under § 1520.9.

6.9 Vetting for Access to SSI

TSA may determine whether to make an individual's access to SSI contingent upon the satisfactory completion of a security background check or other procedures or requirements, in accordance with 49 CFR § 1520.11(c) and § 1520.15(d)(2).

[41] Section 1520.15(e) of the SSI Regulation grants the TSA Administrator the authority to make these written determinations. The Administrator's authority to make these 15(e) determinations is primarily delegated to the SSI Program Chief in TSA MD 2810.1, *SSI Program*.

6.9.1 Vetting Requirements by Role

The standards for vetting vary based upon the nature of the role of the individual with TSA.

- **TSA Personnel (Federal Employees and TSA Contractors):** Prior to being granted access to TSA facilities, sensitive information, or information technology resources, TSA Personnel (including TSA Contractors) must have a favorably adjudicated, fingerprint-based, criminal history record check and credit check.[42] These record checks may be conducted prior to or concurrently with a Tier 1 investigation. See also TSA MD 2800.71, *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors*.
- **Other Federal Employees and Other Federal Agencies' Contractors:** For the purposes of sharing SSI, TSA does not require additional vetting for other federal agencies and their contractors as the vetting standard is the same. By virtue of the other federal employees' and other federal agencies' contractors' .gov email, it may be inferred that they have completed required vetting. SSI may not be sent to contractor email addresses.
  Note: *Since other federal employees and other federal agencies' contractors may not be familiar with SSI, TSA employees should consider issuing an NDA and providing SSI awareness training or materials (See also Subsection 6.2, Non-Disclosure Agreements).*
- **Foreign Nationals:** The Tier 1 used for federal employees and contractors may not be used for vetting due to an individual's status as a foreign national. An alternate process, as detailed within *TSA MD 2810.3, Management of Foreign Access to Sensitive Information*, must be used to determine whether the foreign national represents a low-risk to the agency. Requests for vetting must be submitted through the Salesforce Concourse app, Security icon, *Foreign National SSI Access* service request.
- **Potential Offerors (i.e., Pre-Award Acquisition):** Potential offerors seeking access to SSI to submit a response to a request for proposal (RFP) are subject to a risk assessment coordinated by Contracting and Procurement. Disclosure during this process is for transparency and to maintain a fair and level playing field. As part of this risk assessment, individual recipients of SSI are vetted using the SSI STA process.[43]
- **Other Contract-Like Agreements (e.g., MOA, Bailment) and OTAs:** TSA may also require vetting for other contractual agreement and other transaction agreement participants, or those who receive other conditional SSI disclosures on a case-by-case basis.
  - **MOAs and OTAs** - For MOA and OTA recipients who have not been previously vetted through other means (e.g., Security Identification Display Area [SIDA] Badge, though airport-specific vetting, or other means documented in Subsection 6.9.2, *Processing SSI*

[42] The Office of Personnel Management (OPM) Federal Investigative Standards Tier 1 is the minimum investigative standard for TSA personnel requiring staff-like access to TSA facilities on a recurring basis (i.e., more than 14 days per year) for positions designated as low-risk, non-sensitive. It is also the minimum level of investigation for a final credentialing determination for physical and logical access.

[43] In addition to the information required for security background checks, TSA requires potential offerors to provide 1) a certification from each company/entity that its employees/personnel who are provided access to SSI are properly trained; 2) an NDA for each individual who is granted access to SSI; and 3) an affirmation that each company/entity will designate a Senior Official who can certify that all appropriate protections will be followed, only authorized individuals will have access to the sensitive information, and that those individuals adequately understand their responsibilities to protect the information.

Security Threat Assessment [SSI STA] Requests), the COR submits each individual for an SSI STA.

- **Bailments** - Bailments are vetted to the same standard as TSA employees and TSA contractors. The COR submits vetting requests to Personnel Security (PERSEC). See also TSA MD 2800.71, *Pre-Employment Investigative Standards for TSA Non-Screener Employees and Contractors*.

- **Research and development partners:** Vetting for research and development partners depends on the nature of the relationship with TSA. The terms of the written agreement specify the vetting requirements for each particular instance and will typically either include standard Tier 1 vetting used for Federal employees and contractors (such as for CRADAs) but may also include use of an SSI STA when Tier 1 vetting is not possible.

- **Litigants:** A party in civil proceedings in the U.S. District Courts, as required by section 525(d) of the DHS Appropriations Act, may seek access to SSI where the party demonstrates 1) a substantial need for relevant SSI in preparation of the party's case and 2) an undue hardship to obtain equivalent information by other means. The party or party's counsel is designated as a covered person under 49 CFR part 1520.7, provided that certain requirements are met.[44] A separate request is required for party-retained experts or consultants, or court reporters who record or transcribe testimony containing SSI. Unless they are covered persons with a need to know, individuals seeking access to SSI in court proceedings are generally required to complete an SSI STA by coordinating with TSA's CC's office.

- **Other conditional disclosures** – When SSI is provided during other conditional disclosures (as addressed in Subsection 6.8, *Other Conditional Disclosures*), TSA may require recipients to complete an SSI STA.

6.9.2 Processing SSI Security Threat Assessment (SSI STA) Requests

To determine whether an individual may be granted access to SSI, TSA may conduct an SSI STA, including adjudication of a criminal history records check (CHRC), a name-based check against Federal law enforcement, terrorism, and immigration databases, and/or implement other procedures and requirements for safeguarding SSI that are satisfactory to TSA.

- Individuals seeking access to SSI in court proceedings are required to complete a TSA Form 2817A *SSI Access Threat Assessment Questionnaire - Litigation*.

- Any non-litigant applicants are required to complete TSA Form 2817B, *SSI Access Threat Assessment Questionnaire – Standard.*

  - Companies for potential offerors submit the required data in a spreadsheet as required in the solicitation. Submit requests for vetting pre-award to RFP.Access@tsa.dhs.gov (See also TSA MD 2810.2, Disclosure of SSI in the Pre-Award Acquisition Process).

A recipient who 1) is a member of the TSA PreCheck® Application Program with an active known traveler number (KTN); 2) has recently (i.e., typically within two years) successfully undergone a federal background investigation (i.e., Tier 1); 3) has recently completed a comparable STA conducted by TSA; or

[44] The requirements are that 1) the overseeing judge enters an order protecting the SSI from unauthorized disclosure; 2) the individual undergoes an SSI STA, including adjudication of a fingerprint-based CHRC and assessment check of terrorism and related databases; and 3) the provision of access to the specific SSI in question in a particular proceeding does not present a risk of harm to the nation.

4) holds an active security clearance (as defined by Executive Order 12958) is not required to complete the full Pre-Enrollment process for an SSI STA.

The program office seeking the disclosure of SSI facilitates and tracks the vetting process. Depending on the information provided by the recipient, the program office routes the request to these offices:

- For KTN validations, submit the request directly to the SSI Program at SSI@tsa.dhs.gov.
- For Federal Background Investigation or security clearance validation, submit the request to PERSEC at PERSEC-CTRIntake@tsa.dhs.gov.

  Note: *If the individual has a KTN, current Federal Background Investigation (i.e., Tier 1), or active security clearance and TSA validates the information, further vetting is not required.*

- For a name-based check against Federal law enforcement, terrorism, and immigration databases, submit the form to Transportation Vetting System (TVS) at OIA.TVS-OPS@tsa.dhs.gov and operations@tvs.tsa.dhs.gov.
- For requests requiring a CHRC, individuals must complete SSI Access Pre-Enrollment online at https://universalenroll.dhs.gov/, schedule an appointment for in-person SSI Access enrollment, and complete the in-person electronic fingerprinting at a designated Universal Enrollment Services (UES) Center. The program office then submits the form to TVS after confirming appointment completed. See also *TSA SSI Access Enrollment Instruction Sheet*.

7.0 Destruction of SSI

Subject to applicable records retention laws, schedules, and directives (See TSA MD 200.7, *Records Management Program*), records containing SSI must be destroyed to prevent recognition or reconstruction using the following procedures:

Destruction of Paper SSI

- Dispose in an SSI Bin, if available;
- Shred in a cross-cut shredder so particles do not exceed 1 ½" by ¼";[45] or
- Any method approved for the destruction of CNSI.

Destruction of Optical Media (CDs, DVDs, Disks, etc.)

- Use one of the following authorized methods of destruction: shredding, incinerating, or disintegrating, in accordance with *TSA Information Assurance Handbook*, Subsection 3.11, *Media Protection* and TS-046, *IT Media Sanitization and Disposition*. At TSA Headquarters, SSI Bins contain a media drop.

If destruction of SSI (paper or optical media) is completed by a document destruction vendor, either 1) the vendor employees must be vetted by TSA in accordance with § 1520.11(c) or 2) the SSI must be collected and destroyed under the direct supervision of a TSA employee using one of the methods authorized for the destruction of SSI as outlined above. Upon destruction completion, even when observed by TSA, the vendor must also provide TSA with a document signed by the vendor, or authorized representative, and witnessed by the TSA employee who supervised the destruction, as applicable, outlining how the SSI was destroyed.

Destruction of Electronic Media (USB Flash Drives, Hard Drives, Copy Machines, Scanners, etc.)

- Printing, scanning, and copying devices typically contain persistent memory such as hard drives or internal flash memory to store data. SSI must be properly sanitized from all electronic media before resale, disposal, or reuse outside of the agency; proper disposition of media is critical to ensuring confidentiality.
- TSA and DHS disposition requirements[46] prohibit this media from leaving the facility and require that it be destroyed on-site. In order to arrange removal of SSI from electronic media, contact the Authorized Property Officer (APO)[47] to excess the property. Excess property is sent to the TSA Warehouse for sanitization and/or destruction.[48]

[45] If destruction of SSI is completed by a vendor in bulk, the maximum acceptable size particles that vendors must conform to is 1 ½" by 5/8".
[46] Refer to DHS Sensitive Security Systems Policy Documents (4300A), Section 4.13 for further detail.
[47] To identify the appropriate APO, contact the TSA Property Management Office at Property.Mgmt@tsa.dhs.gov.
[48] A determination of whether a copier drive, hard drive, USB flash drive, or scanner is cleared (wiped), purged, or destroyed is based on the security categorization level of information it contains and the security categorization of the system it falls within (*See also TSA Information Assurance Handbook*, Subsection 3.11, *Media Protection* and TS-046, *IT Media Sanitization and Disposition*, to determine if the information warrants clearing, purging, or physical destruction; *see also* Table 5: *NIST Specific Guidance on Destruction of Electronic Media* below for instructions on media destruction).

8.0 SSI Training Programs

The SSI Program office currently offers the following SSI training:

SSI Training for New Employees (HQ): Instructor–led SSI Awareness Training delivered to new employees outlining where to find information on SSI, the SSI Regulation, and the principles of identifying, marking, safeguarding, disclosing, and destroying SSI.

Initial and Recurrent SSI Awareness Training: TSA Organizational Security Fundamentals (TSA-ALL-ORGSECFUND-TO[49]) is an online, self-paced (i.e., asynchronous) training required for all TSA employees and contractors. This training addresses how to keep sensitive and protected information, including SSI, out of the hands of those who should not have access and may wish to do harm to our systems or the public. Specific topics include identifying the elements of operational security, recognizing the different types of protected information, marking and safeguarding protected information, defining consequences of unauthorized disclosure, and outlining foreign visitor best practices.

Initial SSI training is automatically assigned and is required for all personnel within the first 60 days of employment with TSA. This training is also required annually for all personnel with an Online Learning Center (OLC) account and is automatically assigned by job title within the Learning Management System (LMS). CORs for TSA contractors and subcontractors without an OLC account are responsible for ensuring assigned contractors adhere to the requirements for initial and annual recurrent SSI training. CORs are also responsible for maintaining an auditable system to track training completion.

Customized SSI Awareness Training: The SSI Program provides customized training designed to supplement initial and recurrent SSI Awareness Training. This training includes topical training such as *SSI and Mobile Devices*; training designed to address stakeholder needs such including air carriers, airport operators, surface transportation operators, law enforcement, and fusion centers; and job aids designed to assist with SSI-related functions. Customized SSI Awareness Training can also be provided upon request to support the unique needs of TSA program offices and their stakeholders.

Initial SSI Coordinator Training: This self-paced SSI Training is required for all newly-appointed SSI Coordinators within 30 days of appointment and is a prerequisite for Advanced SSI Training and Certification. This training covers introductory topics such SSI Coordinator roles and responsibilities to include review of TSA MD 2810.1; identifying available resources to answer common SSI questions; submitting an SSI Assessment or SSI Review to the SSI Program via Salesforce; creating and updating SSI Coordinator records; and completing common tasks for SSI Coordinators such as annual self-inspection checklist, incident reporting, and SSI Password management.

Advanced SSI Training and Certification: This blended training is delivered by the SSI Program office and provides a more extensive training on in-depth SSI topics. The Advanced SSI Training modules may be taken individually or as a complete training program prior to taking the SSI Certification Examination. Appointed SSI Coordinators or other course attendees must complete all required webinars and Advanced SSI Training modules on OLC before taking the two-part SSI Certification Examination. In order to receive SSI Certification, individuals must score at least 80% on each portion of the exam.

All appointed SSI Coordinators must complete Advanced SSI Training and pass the SSI Certification examination within six months of appointment. If an appointed SSI Coordinator does not pass the SSI Certification examination within one year of appointment or does not pass the SSI Certification examination after two attempts, the appointing official must appoint another TSA employee to serve as

[49] Federal Air Marshal Service uses TSA-ALL-ORGSECFUND-TO-FAM.

an SSI Coordinator. Once an SSI Coordinator becomes SSI Certified, the individual must complete annual CESSI Training, as outlined below, to maintain status as a Certified SSI Coordinator.

Federal employees and contractors other than SSI Coordinators may opt to take the Advanced SSI Training for individual professional development but will not be tracked and maintained as SSI Coordinators.

CESSI Training: In order to maintain SSI Certified status, individuals are required to attend continued education training issued by the SSI Program office. Individuals earn CESSI credits by attending CESSI Training Webinars or by performing SSI-related activities throughout the year. Activities include, but are not limited to, participation in bimonthly conference calls, conducting SSI training or exercises at their office or airport, and conducting awareness activities. Fifty (50) CESSI credits must be earned annually (i.e., calendar year) in order to maintain certification.

9.0 SSI Awareness Programs

As part of TSA's SSI Awareness efforts, the SSI Program office leverages its SSI Coordinator network to establish and maintain direct contact with all TSA personnel. The SSI Program office uses a number of communication methods—to include Be On the Lookout (BOLO) notifications, bimonthly SSI Coordinator conference calls, SSI Q&A calls, and SSI Awareness Week activities—to conduct this outreach. The SSI Program office also maintains the SSI SharePoint page to make its most critical documents and resources easily accessible by all TSA personnel.

9.1 SSI Coordinators

SSI Coordinators, whose responsibilities are defined within TSA MD 2810.1, *SSI Program*, are a critical part of the SSI Program Awareness initiatives. SSI Coordinators are appointed by Assistant Administrators or the equivalent, Supervisory Air Marshals in Charge, and Federal Security Directors. The appointing official (i.e., FSD, FAM SAC, or AA) should document appointments to SSI Coordinator positions using the template SSI Appointment Letter, which includes a full listing of SSI Coordinator responsibilities. The SSI Program recommends filing a copy of the appointment letter in the SSI Coordinator's personnel file.

Newly-appointed SSI Coordinators must follow the *Instructions for New SSI Coordinators* for notification to the SSI Program regarding appointment and completion of the required SSI Coordinator Training. For more information on SSI Coordinator responsibilities, see TSA MD 2810.1, *SSI Program* and *Initial SSI Coordinator Training.*

9.2 SSI BOLOs and Stakeholder Alerts

The SSI Program office uses SSI BOLOs to draw attention to policies targeted for additional awareness throughout TSA. SSI BOLOs are published on an ad hoc basis as changes occur at offices and airports nationwide. SSI BOLOs are also written in response to SSI incidents and from ideas or observations submitted by SSI Coordinators. SSI BOLOs do not contain SSI and can be posted publically.

The SSI Program occasionally publishes Stakeholder Alerts specifically designed for regulated entities who are not obligated to follow the same policies and procedures as TSA personnel. Stakeholder Alerts are often coordinated through Compliance as part of outreach efforts.

The SSI Program office recommends all SSI Coordinators post SSI BOLOs and Stakeholder Alerts in common areas (e.g., break rooms, work spaces) and in local newsletters to be seen by as many personnel as possible. Current and past SSI BOLOs and Stakeholder Alerts can be accessed by SSI Coordinators in the SSI Coordinators' Corner of the SSI Program office SharePoint page.

9.3 SSI Conference Calls

The SSI Program office schedules bimonthly conference calls with SSI Coordinators to discuss SSI updates and issues. Conference calls are also an opportunity for SSI Coordinators to submit ideas and recommendations for future SSI policies. SSI Coordinators can access bimonthly recordings by visiting the SSI Coordinators' Corner of the SSI Program office SharePoint page.

Additionally, the SSI Program hosts monthly Question and Answer (Q&A) calls as an agenda-free time for SSI Coordinators to ask any questions which may arise. Q&A call invites may be shared with others in the office/airport who have questions or simply wish to learn more about the SSI Program.

9.4 SSI Awareness Week

SSI Awareness Week, held annually during the first week of November, is used to remind personnel of the importance of SSI and the responsibility to properly recognize, mark, protect, disclose, and destroy SSI. The SSI Program office engages personnel with activities such as crossword puzzles, word searches, quiz questions, training exercises, awards for exceptional SSI protection, and other creative ideas. The various activities provided by the SSI Program office for SSI Awareness Week are available to SSI Coordinators in the SSI Coordinators' Corner of the SSI Program office SharePoint page.

9.5 SSI SharePoint Page & Internet Page

The SSI Program office relies on the SSI SharePoint Page to provide critical information to SSI Coordinators and other TSA personnel. Applicable documents pertaining to the SSI Program and other guidance in recognizing, protecting, and handling SSI are available at this site.

The SSI Program office also maintains a public site available on the TSA homepage. This site contains information related to stakeholder and non-DHS training and policies.

9.6 Self-Inspection Program

Annually, each SSI Coordinator is required to complete the SSI Self-Inspection Checklist for every airport (hub/spoke) and program office and submit the findings to the SSI Program in accordance with DHS MD 11056.1, *Sensitive Security Information*. SSI Coordinators are also encouraged to conduct additional informal self-inspections throughout the year. The Self-Inspection Checklist includes TSA-wide SSI programmatic requirements. For more information, contact the SSI Program at SSI@tsa.dhs.gov or your local Primary SSI Coordinator.

10.0 SSI Incidents

SSI Incident identification, response, and resolution are critical to TSA's ability to mitigate potential damage that may occur as a result of loss, compromise, unauthorized disclosure or mishandling of SSI. All incidents must be reported no matter how small to the SSI inbox at SSI@tsa.dhs.gov. It is important to not send emails directly to a staff member within the SSI Program.

10.1 Identifying SSI Incidents

SSI incidents fall into three categories: major SSI incident, policy infraction, and password incident.

Major SSI Incident

The verified or suspected breach, loss, or unauthorized disclosure of SSI to non-covered persons. The unauthorized disclosure of SSI to covered persons who do not have a need to know the information also shall be reported as a major SSI Incident. ***Note:*** *Depending on the circumstances, the SSI Program office may reduce incident to policy infraction. The standard to be used in evaluating an SSI Incident as major or policy infraction is whether there is a "reasonable suspicion" as to the loss or compromise of SSI.*

- **Breach of SSI:** SSI was accessible to or has been accessed by a non-covered person (e.g., the public).
- **Lost SSI:** SSI which, after reasonable attempts were made to find the material, cannot be located. ***Note:*** *Typically, SSI misplaced or discovered within a public area is categorized as a breach.*
- **Unauthorized Disclosure of SSI:** SSI was accessible to or has been accessed by a covered person who does not have a need to know the information.

Policy Infraction

The non-compliance with the TSA SSI Policies & Procedures Handbook in the handling of a record containing SSI that does not rise to the level of a major SSI incident.

SSI Password incidents occur when:

- Any password created to encrypt SSI was not created or handled in accordance with the SSI Policies & Procedures Handbook; or
- The Standard TSA Password was sent to persons outside of DHS.

10.2 SSI Incident Response & Resolution

SSI incident response and resolution is a TSA-wide effort requiring the support and participation of many program offices. The SSI incident response and resolution process is composed of discovery and initial notification, immediate evaluation and follow-up notification, early mitigation, incident closure, long-term risk mitigation, and incident investigation (See Appendix 4: *SSI Incident Response Flow Chart*).

10.2.1 Discovery & Initial Notification

All personnel are responsible for identifying and reporting SSI incidents to the immediate supervisor and also to the designated SSI Coordinator. Personnel must also report routine mismarking of SSI to their SSI Coordinators. The SSI Coordinator is responsible for reporting major SSI incidents to the SSI Program office using the SSI incident reporting instructions (See Appendix 5: *SSI Incident Reporting Instructions*) as soon as possible, but no later than 8 hours after discovery. If, during the initial incident assessment, the SSI Coordinator determines the SSI Incident may be major, the SSI Coordinator must also notify the Transportation Security Operations Center (TSOC). ***Note:*** *Security Operations Field SSI Coordinators must report major SSI incidents to the TSOC through their Coordination Center.*

10.2.2 Immediate Evaluation & Follow-Up Notification

Once the SSI Program office receives the SSI incident report, SSI Program office personnel review the information and verify the SSI Coordinator's assessment as to whether the subject record is SSI. After processing the initial incident report, the SSI Program office will forward information on major incidents to the program owner of the information, CC, and other TSA headquarters offices, as appropriate:

- **Investigations and the Chief Security Officer:** When a *TSA employee or contractor* is responsible for an SSI Incident.
- **Compliance:** When a *TSA stakeholder* is responsible for an SSI Incident.
- **IT Computer Security Incident Response Team (CSIRT):** When an SSI Incident is *electronic*.
- **Policy, Plans, and Engagement:** When subject SSI pertains to stakeholder assets.
- **Strategic Communications and Public Affairs:** When an incident may generate media interest
- **Other Programs:** In addition to the program office that owns the subject SSI, the SSI Program office will notify other program offices whose functions or interests may be affected by the incident; when a *TSA contractor* is responsible for an SSI Incident, the affected program office's COR may take appropriate action.

If the SSI Program office, in consultation with the relevant program office, determines the records *do not contain SSI*, the SSI Program office relays this finding to the reporting SSI Coordinator and the incident is closed.

If the SSI Program office determines the records do contain SSI and the SSI Incident is major, the SSI Program may recommend a team composed of members of affected program offices perform a damage assessment and affiliated risk mitigation (See also Subsection 10.2.5, *Long-Term Risk Mitigation*).

10.2.3 Early Mitigation

The program office responsible for the incident and their SSI Coordinator must take reasonable steps to mitigate the effects of the SSI Incident. In incidents where no program office is clearly responsible, the SSI Program office coordinates early mitigation efforts.

Major SSI Incidents

- **Breach of SSI:** Reasonable attempts must be made to retrieve the content or limit further access by additional non-covered persons, unless such actions would draw more attention to the loss (consult with the SSI Program office, as necessary, to make this determination). Where appropriate, consider the use of NDAs for non-covered parties inadvertently receiving SSI to reduce the likelihood of further SSI incidents and breaches.

- **Lost SSI:** Reasonable attempts to recover the materials (e.g., back-track through last known location, survey of other personnel with access to the area, review of CCTV footage covering the suspected location of the loss, etc.) must be undertaken. ***Note:*** *The major factor on whether lost SSI is a major or minor incident is the "reasonable suspicion" that the SSI was accessed by non-covered persons.*
- **Unauthorized Disclosure of SSI:** Further access to the SSI must be restricted. Certain cases of unauthorized disclosure may not rise to the level of a major incident. Consult with the SSI Program office at SSI@tsa.dhs.gov to determine whether the improper disclosure is a major SSI incident.

Policy Infractions

- **Mishandling of SSI:** Appropriately lock up or destroy SSI (See also Subsection 5.0, *Safeguarding SSI*). Training and evaluation of safeguarding measures are appropriate to prevent further mishandling of SSI.

Note: *CSIRT assists in limiting access to the SSI on TSA SharePoint and network folders and may also assist in having SSI content removed from Internet pages when proper approvals are provided.*

10.2.4 Incident Closure

The SSI Program office considers SSI Incidents closed when the following have been met:

Major SSI Incidents

- **Breach of SSI:** When all reasonable remedial and mitigating measures have been exhausted, though the SSI may remain beyond TSA's control.
- **Lost SSI:** When all reasonable remedial and mitigating measures have been exhausted, though the SSI may remain beyond TSA's control.
- **Unauthorized Disclosure of SSI:** When only covered persons with a need to know the information may access it and, as practical, when all persons inappropriately receiving the information are notified not to further disseminate the SSI.

Policy Infractions

- **Mishandling of SSI:** Closed by the SSI Coordinator upon receiving assurance from the appropriate office that procedures are in place to prevent recurrence.

Non-SSI Incident

- Incidents initially reported as SSI incidents are closed if the SSI Program office determines the information is not SSI, or for any other reason the SSI Program office determines the reported event does not constitute an SSI incident.

10.2.5 Long-Term Risk Mitigation

In some major incidents, it is appropriate for the program office that owns the SSI to lead an effort to perform a damage assessment, associated risk assessment, and complete a risk mitigation plan. If changes are made to processes or procedures in order to mitigate the effects of the incident or to prevent future incidents, the SSI Program office must be informed of the changes. If the affected program office creates an evaluation of the effect of the breach on its operations, the SSI Program office must be provided with the same. Feedback to the SSI Program office is key to ensuring these changes are incorporated into future SSI assessments and reviews.

The information owner is responsible for long-term risk mitigation. The SSI Program office may assist affected program offices, such as providing additional education and awareness regarding the proper handling and protection of SSI to prevent similar incidents from occurring.

10.2.6 Incident Investigation

In some instances, Investigations may open a misconduct investigation into the incident. In all investigations pertaining to SSI, the SSI Program office provides support to the office conducting the investigation, as appropriate, by providing a finding that SSI was or was not compromised in the incident. The SSI Program office may also supply the investigating authority with the data and information collected as part of the evaluation phase of the incident.

The investigating authority, if appointed, is responsible for final communication and reporting. SSI Incidents not warranting further investigation need not have detailed investigative closeout reports.

10.3 SSI Password Incident Response & Resolution

Personnel must immediately report password incidents to the SSI Program office at SSI@tsa.dhs.gov through the designated SSI Coordinator. The SSI Program office evaluates whether the password incident requires the issuance of a new Standard TSA Password. If a password incident *does* require the creation of a new Standard TSA password, the SSI Program office develops and distributes it through the SSI Password Application on Salesforce.

The SSI Program office, in coordination with the SSI Coordinator, advises on other appropriate mitigation strategies for each unique password incident.

10.4 Penalties for Mishandling or Unauthorized Disclosure of SSI

Any TSA employee who violates TSA SSI policies and procedures may be subject to administrative and/or disciplinary action in accordance with TSA MD 1100.75-3, *Addressing Unacceptable Performance and Conduct*. TSA contractors who violate TSA SSI policies and procedures may be subject to administrative and/or disciplinary action as levied by the Contracting Officer (CO).

Additionally, pursuant to 49 C.F.R. § 1520.17 and 49 U.S.C. § 46301(a)(4), civil penalties[50] for unauthorized SSI disclosure may include the following:

a. Aircraft Operators: Up to $34,777 per violation
b. Airport Operators: Up to $13,910 per violation
c. Individuals: Up to $13,910 per violation
d. Small Business: Up to $13,910 per violation
e. Surface and Other Non-Aviation: Up to $11,904 per violation

If there are multiple violations, there is no "maximum" limit for the civil penalties for the case. The total penalty dictates what court hears the case in the event of a formal proceeding. If the amount in controversy exceeds $50,000 for individuals and small businesses or $400,000 for all other violators, and the matter cannot be resolved informally, the proceedings are addressed in a United States district court, pursuant to the authority in 49 U.S.C. 114 or 46305 to prosecute and collect the civil penalty (See 49 CFR §§ 1503.701 and 1503.703). If the amount is under $50,000 for individuals and small businesses or $400,000 for all other violators, the matter may be heard before an Administrative Law Judge (ALJ).

[50] Current adjusted numbers can be found in Enforcement Sanction Guidance. Numbers have been adjusted for inflation effective February 8, 2021.

11.0 Determining SSI Systems

In accordance with the *TSA Information Assurance Handbook*, all ISSOs are required to complete an SSI Threshold Analysis (SSITA) for assigned systems as part of the required documentation for the SA package. The SSITA is required for the SO to determine whether the systems process, store, or transmit SSI and generally how that SSI is protected within these systems. Systems which have not identified themselves as processing, storing, or transmitting SSI and have completed the security requirements for sensitive systems may not process, store, or transmit SSI. See also Subsection 5.2.2, *TSA Shared Network Resources: Shared Drives, Systems & TSA Intranet* and Appendix 6, *SSI Threshold Analysis*.

12.0 Protection Requirements for SSI Systems & Other Secure Sites

SSI may be shared with covered persons with a need to know through SSI Systems, including restricted networks and other secure sites approved by TSA through the SA process. SSI Systems are required to have protections in place to ensure only covered persons with a need to know can access the information and have a minimum Federal Information Processing Standard (FIPS) 199 impact level of "Moderate" or higher for confidentiality and integrity.

During the SA process, each ISSO is required to complete an SSITA as part of the system documentation (See also Section 11.0, *Determining SSI Systems*) and submit it to SSI@tsa.dhs.gov. Upon review of the SSITA, the SSI Program office may determine that additional documentation in the form of an SSI Impact Assessment (SSIIA) will be required for an SSI system and other secure sites. While completing an SSIIA for the systems, ISSOs should consider what SSI will be posted, how it will be posted, and any applicable restrictions to its access. ISSOs should also consider plans for training or verifying the training of SSI recipients, how the content will be reviewed periodically for usefulness, and how they will conduct audits of users to determine if they still have a need to know.

Per the FIPS 199 and NIST 800-53, additional security controls may be required in addition to the minimum protection requirements. After reviewing a completed SSIIA, the SSI Program office, in coordination with IT, determines whether any additional protection requirements are appropriate for the system.

Users of SSI Systems and other secure sites must be familiar with the terms of use for each particular system where they post SSI. If a user is concerned with how the information is being handled on any particular site, contact the site administrator or the SSI Program office directly at SSI@tsa.dhs.gov. See also Appendix 7, *SSI Impact Assessment*.

13.0 SSI Policy Exceptions

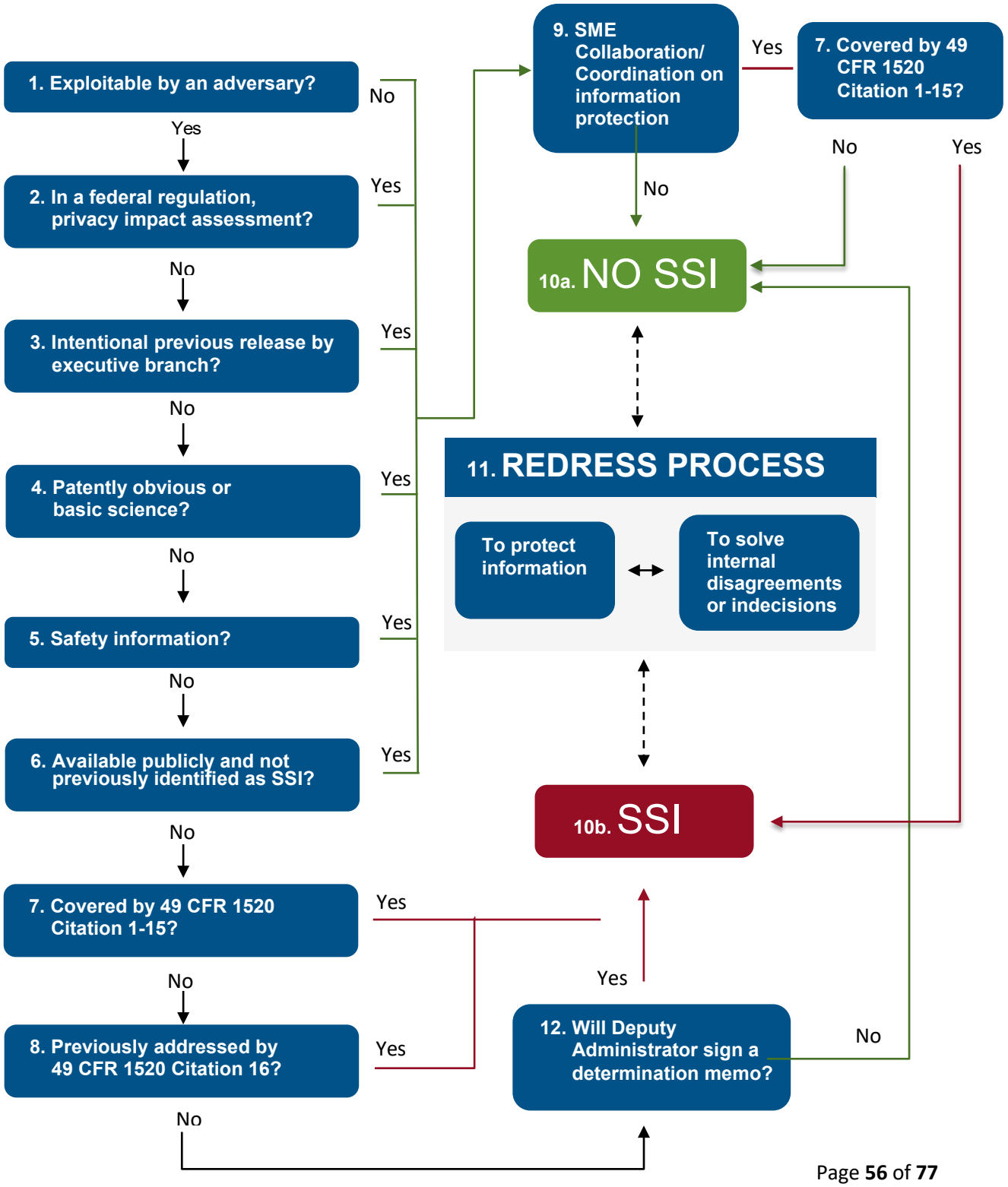
This Handbook is designed to meet the needs of personnel during the course of routine business. If an office or program must address a unique challenge with SSI, use the SSIIA template (at Appendix 7) to document this challenge, and submit the SSIIA to the SSI Program office at SSI@tsa.dhs.gov.

During periods of national emergency or exigent circumstances, the TSA Administrator or SSI Program Chief may determine that certain requirements of this Handbook should be temporarily suspended.[51] Even during national emergency or exigent circumstances, however, all covered persons are still required to take reasonable measures to protect SSI.

[51] Even if SSI Program office policies or procedures are temporarily suspended, other TSA program offices (e.g., IT's IAD) may have policies that still need to be followed.

Appendix 1: SSI Program Initial Decision Flow Chart

This product is designed to explain how the SSI Program office conducts its evaluations of information to determine if information warrants protection as SSI and whether that information protection is consistent with the SSI Regulation.



Flow Chart Notes

1. Exploitable by an Adversary?

- Can the information be used to:
  - Bring prohibited items into sterile areas?
  - Defeat vetting processes?
  - Avoid attention of Law Enforcement Officers/Intelligence?
  - Target or avoid one screening method over another?

2. In a Federal Regulation or Privacy Impact Assessment?

- Is the information being reviewed publicly available in the Code of Federal Regulations?
- Is the information contained in a Privacy Impact Statement as required by the E-Government Act of 2002 or the Homeland Security Act?

3. Intentional Previous Release by Executive Branch?

- Has an executive agency voluntarily released the information for public consumption?
  - TSA/DHS press releases; information available on www.tsa.gov?
  - Testimony in open session of Congress or unprotected court filings?
  - Previous determinations by Administrator or SSI Program Chief?

4. Patently Obvious or Basic Science?

- Would an average person, with some knowledge of the topic, be able to reasonably answer the question with confidence?
  - Ex. “Do Federal Flight Deck Officers (FFDOs) carry their firearms in ordinary, non-descript bags?”
  - Note: “Obvious” is admittedly subjective.

5. Safety Information?

- Does the information need to be widely known to the traveling public to ensure safe and efficient operation?
- Do first responders need to openly share this information for their own safety and the safety of others?

6. Available Publicly and Not Previously Identified as SSI?

- Is the information available:
  - Using a standard web search engine?
  - On a Federal public web site?
  - ***Note:*** *In some circumstances, information will continue to be protected as SSI despite its presence on public websites.*

7. Covered by SSI Regulation 49 C.F.R. § 1520.5(b)(1)-(15)?

- Do one of the 15 applicable categories of 49 C.F.R. § 1520.5(b)(1)-(15) apply?
- Is it contained in an SSI Identification Guide?
- Could a (16) determination be executed and legally sufficient to protect this information?

8. Covered by 49 C.F.R. § 1520.5(b)(16)?

- Previous (16) determinations include:
  - Aggregate Incident Data
  - Railroad Automated Equipment Identification reader locations
  - Names and identifying information for Inspections' Covert Testers

9. SME Collaboration/Coordination on Information Protection

- SME Collaboration
  - Engage program area SMEs to further explain rationale for release or protection.
  - Include other TSA offices which may have equities.
- SME Coordination
  - Based on past practice, written guidance or confirmed specific concurrence, do the SMEs concur that the information should be protected?

10. Appeals Process

Appeals of previous SSI findings undergo a re-review with emphasis on additional SME input and cost/burden input from appellant.

11. Will Deputy Administrator Sign a Determination Memo?

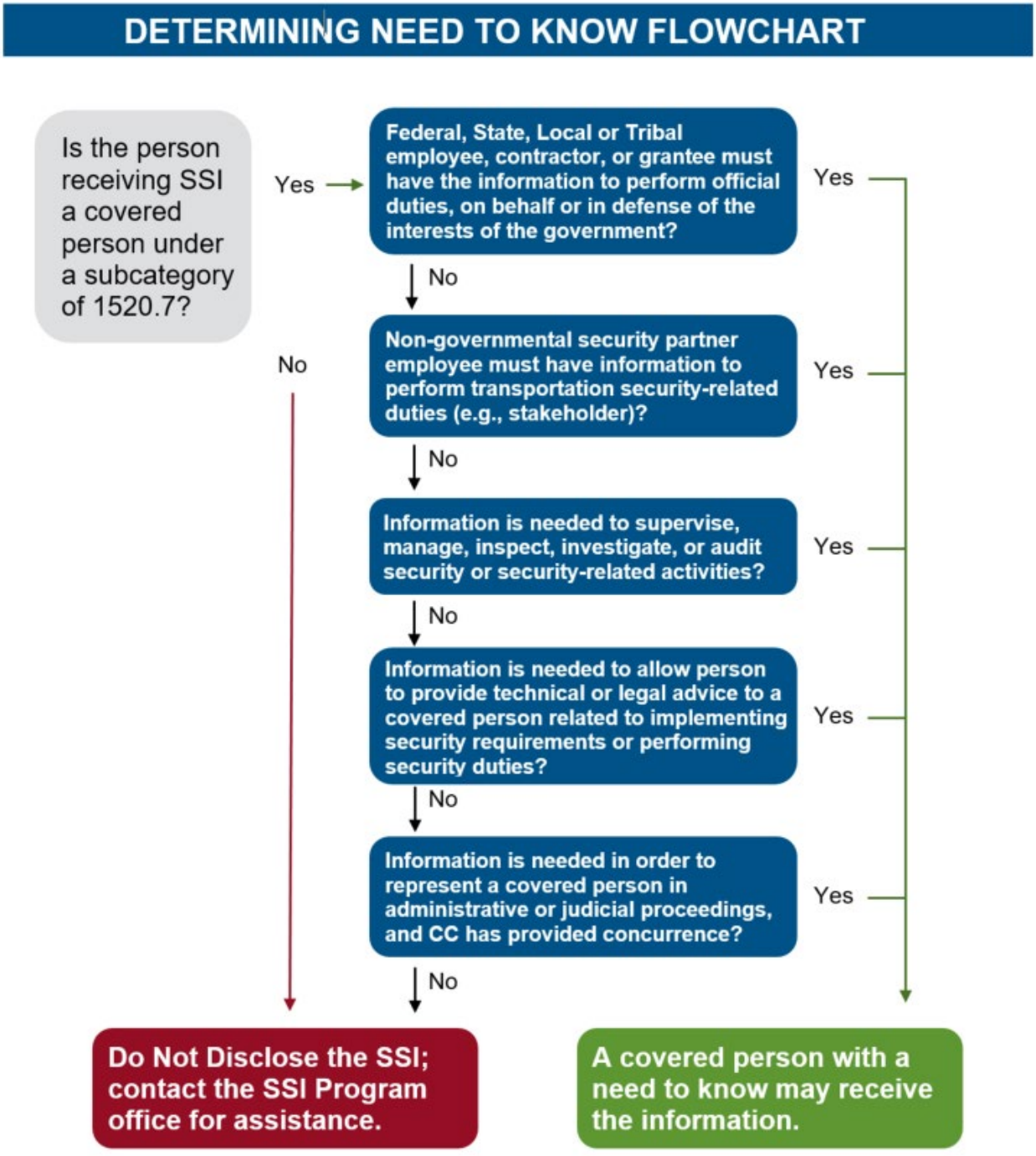
The recommended (16) determination is socialized with the SSI Program and then processed through ExecSec for concurrence and Deputy Administrator signature.

12. SSI? Yes/No

- Will the information be protected as SSI?
- Do we have concurrence within the SSI Program office?
- Does the SSI Program office require additional support from an AA or the Administrator to protect or release this information?

Appendix 2: Determining Need to Know Flow Chart

This product is intended for general use outside of the SSI Program office. It was designed to assist personnel in determining whether an individual or group has a need to know SSI and if that information sharing is consistent the SSI Regulation 49 C.F.R. §§ 1520.7 and 1520.11. If further guidance is needed, contact the SSI Program office at SSI@tsa.dhs.gov.

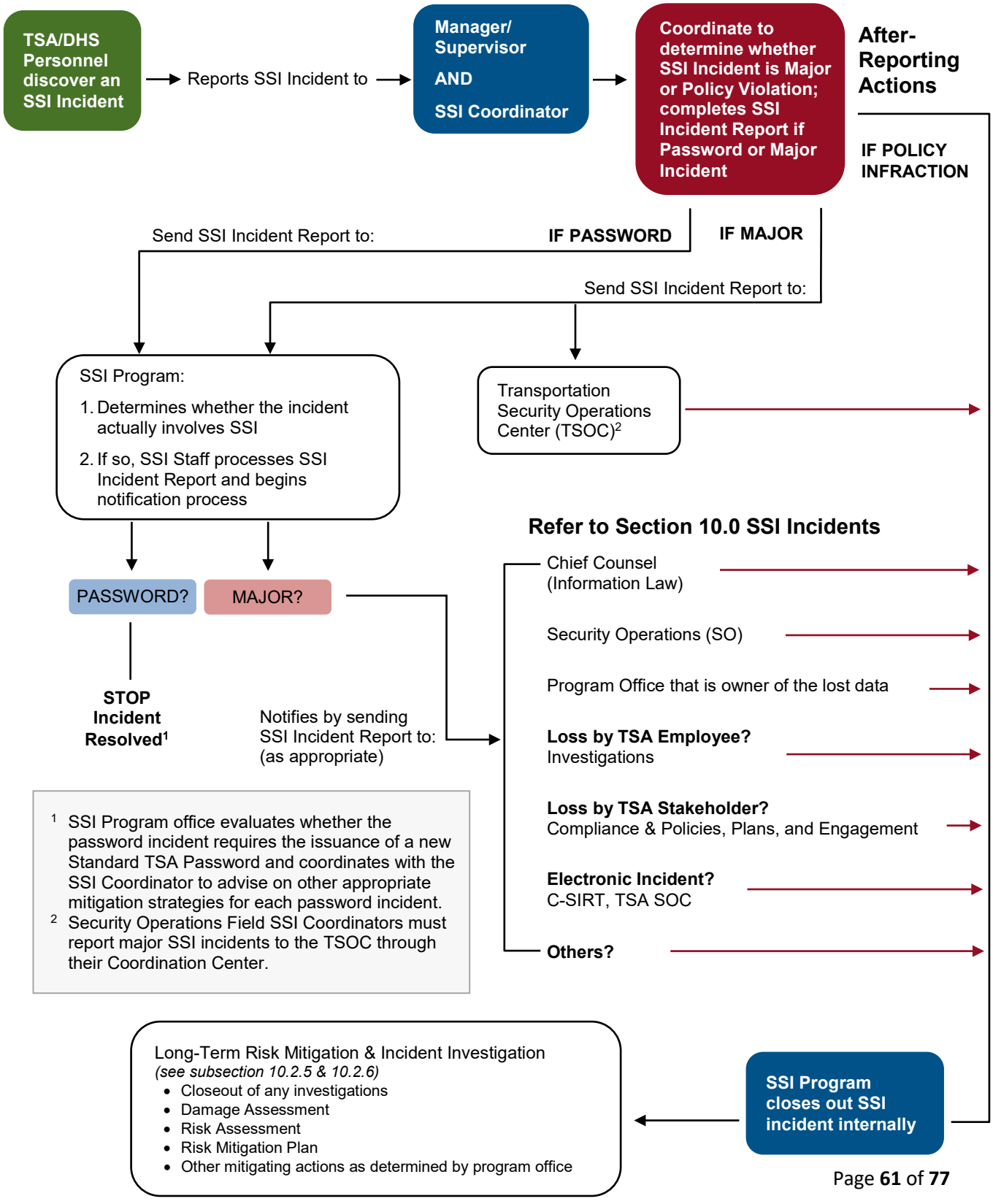


Appendix 3: Instructions for Watermarking Files

Watermarking may be used as a tool with regard to SSI documents' identification, protection and tracking. In accordance with requirements under TSA MD 2810.1, *SSI Program* and TSA MD 2810.2, *Disclosure of SSI in the Pre-Award Acquisition Process*, the IT's IAD/Compliance and Policy Branch has developed the following instruction for watermarking files as needed to protect SSI.

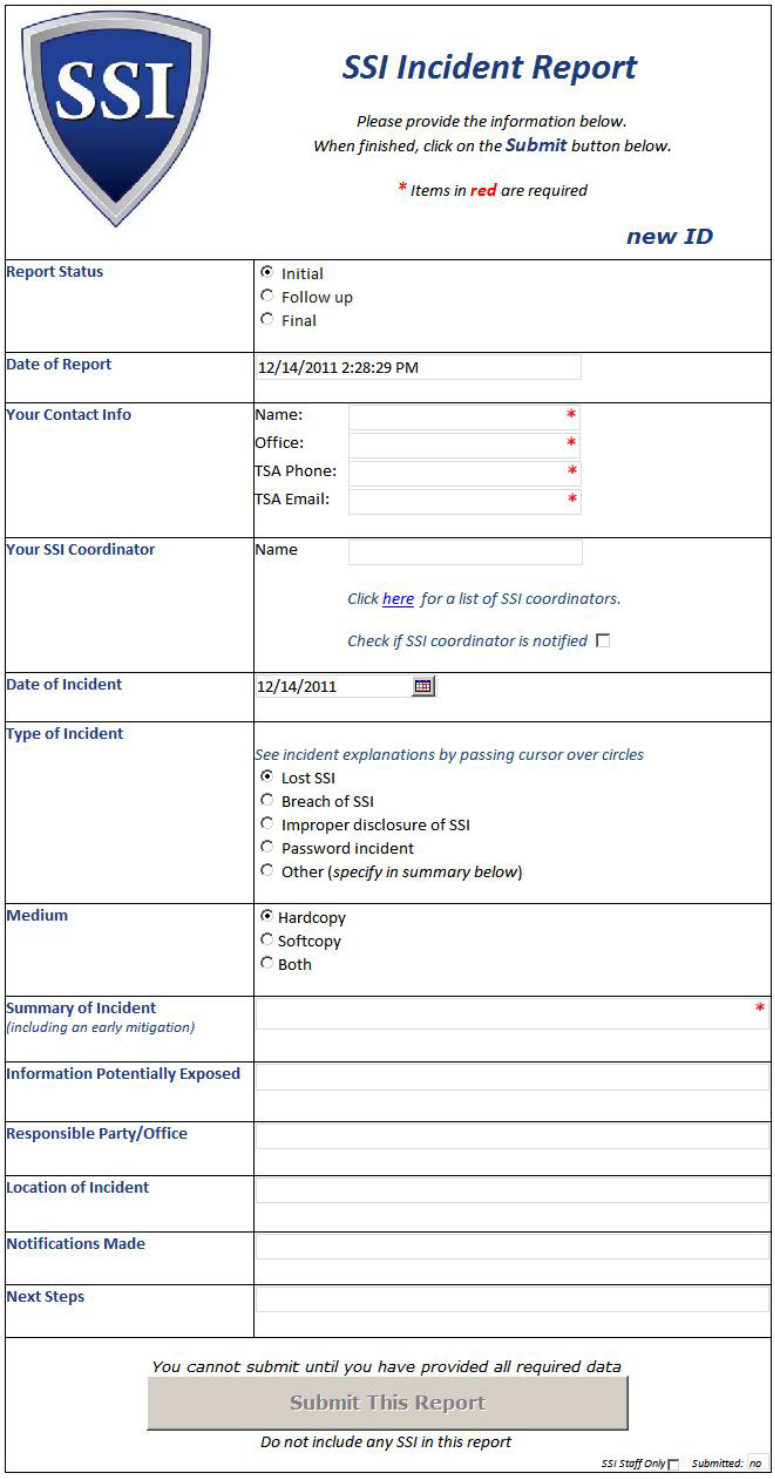
- In MS Word, the official submitter/owner of the SSI document shall open the SSI file using the initial password and ensure that appropriate SSI headers and footers are incorporated into the SSI document, if not done so already.
- As part of the document lockdown process, the submitter shall incorporate and track *restrictions to editing* password, and add a Watermarking Code containing the following key information:
    a. In MS Word, open SSI document and click on the *Design tab*, select *Watermark*, select *Custom Watermark,* select *Text watermark* box and place cursor inside the *Text* box and type-in the following (example): **BT**IBM**JD**014**07282022**
    b. Select Color preference: Medium gray (preferable)
    c. Semitransparent Box: Leave *checked*
    d. Size: 60
    e. Characters 1-2: Submitter initials (**B**rian **T**homas) – this is the person sending the password-protected SSI document to the vendor.
    f. Characters 3-5: Receiving company name (**IBM**) - this space is for each and every unique vendor receiving the SSI document from the submitter.
    g. Characters 6-7: Receiving POC name (**J**ohn **D**oe) – this is the contractor/person receiving the SSI document from the submitter.
    h. Characters 8-10: Internal document sequence number (**014**) – the sender keeps track of all sequence numbers and submissions.
    i. Characters 11-12: Submission month (**07**) – month of document submission.
    j. Characters 13-14: Submission day (**28**) – day of document submission.
    k. Characters 15-18: Submission year (**2022**) - year of document submission.
    l. NOTE: This Watermark Code shall be placed at angle.
    m. *Save* document
    n. Lockdown of SSI document:
        i. In MS Word, go to the very top of the document tool bar and click on the right-most arrow (i.e. Customize Quick Access Toolbar).
        ii. Unclick or disable: Save, Quick Print, Print Review and Print and Email.
        iii. Save document
    o. Restrict Editing Password:
        i. Go to *Review* tab
        ii. Click on *Restrict Editing* (upper far right-hand side)
        iii. Item 2. Click box to "*Allow only this type of editing in the document*".
        iv. Select "*No Changes (Read Only)"*
        v. Item 3. Start Enforcement: Click on "Yes, Start Enforcing Protection".
        vi. Select AND TRACK the selected password. (See Subsection 5.3.2, *Creating Passwords to Encrypt SSI*).
    p. Save MS Word SSI document. Closely track all passwords and place document in a secure place.

Appendix 4: SSI Incident Response Flow Chart



Appendix 5: SSI Incident Reporting Instructions

When reporting SSI Incidents to the SSI Program office, refer to Section 10.0, *SSI Incidents* and Appendix 4: *SSI Incident Response Flow Chart* and ensure to include the following details:



SSI Incident Report

Please provide the information below.
When finished, click on the ***Submit*** *button below.*

* *Items in* ***red*** *are required*

new ID

Report Status	◉ Initial ○ Follow up ○ Final
Date of Report	12/14/2011 2:28:29 PM
Your Contact Info	Name: * Office: * TSA Phone: * TSA Email: *
Your SSI Coordinator	Name *Click here for a list of SSI coordinators.* *Check if SSI coordinator is notified* ☐
Date of Incident	12/14/2011
Type of Incident	*See incident explanations by passing cursor over circles* ◉ Lost SSI ○ Breach of SSI ○ Improper disclosure of SSI ○ Password incident ○ Other (*specify in summary below*)
Medium	◉ Hardcopy ○ Softcopy ○ Both
Summary of Incident *(including an early mitigation)*	*
Information Potentially Exposed	
Responsible Party/Office	
Location of Incident	
Notifications Made	
Next Steps	

You cannot submit until you have provided all required data

Submit This Report

Do not include any SSI in this report

SSI Staff Only ☐ *Submitted: no*

An PDF version of this template is available on the TSA SSI Program office SharePoint homepage.

Appendix 6: SSI Threshold Analysis

SSI Threshold Analysis

Appendix 6 to SSI Policies & Procedures Handbook

Version 2

SSI Program
Current as of 15 July 2022

Sensitive Security Information (SSI)
Threshold Analysis

The purpose of this SSI Threshold Analysis (SSITA) is to determine where SSI (as defined in 49 C.F.R. Part 1520) resides in electronic form within DHS IT systems. An SSITA must be completed (1) during each review of Authorization to Operate (ATO); (2) during any significant modification or update to the system impacting information available on the system; or (3) every three years, whichever event occurs first.

Additionally, this SSITA must be included as part of the TSA certification and accreditation document suite. IT systems containing SSI must also complete an SSI Impact Assessment (SSIIA) to determine what supplemental protections, if any, are necessary for development within the IT system.

Definitions of the terms used within this document may be found in the *TSA SSI Information Assurance Handbook*, Section 5, *Definitions*.

Email the completed document to the SSI Program office for review and concurrence at SSI@tsa.dhs.gov.

Sensitive Security Information (SSI)
Threshold Analysis

PART A: Does Your Information System/Program Store, Transmit or Process Any Category of Information Listed Below?

(Check all that apply)

1. ☐ **Security programs, security plans, or contingency plans**. Any transportation security program, security plan, or security contingency plan.

   Examples: Corporate Security Plans, Aircraft Operator Standard Security Programs, Airport Security Programs, other security programs for certain modes of transportation.

2. ☐ **Security Directives/Emergency Amendments**. Any Security Directive/Emergency Amendment.

   Examples: TSA Office of Security Operations Security Directives (SDs), Airport and Indirect Air Carrier (IAC) SDs and Emergency Amendments.

3. ☐ **Information Circulars**. Any notice issued by DHS/DOT components regarding a threat to aviation or maritime transportation.

4. ☐ **Performance specifications**. Any performance specification and any description of a test object or test procedure, for 1) devices used for the detection of any person, and any threat item (e.g., weapon, incendiary device, explosive); and 2) communications equipment.

   Examples: Performance specifications in pre-award acquisition actions; performance and test data; descriptions of test objects used for covert testing.

5. ☐ **Vulnerability assessments**. Any vulnerability assessment regarding transportation security.

   Examples: Pre-planned security audits, tests, and vulnerability assessments (not incident-related).

6. ☐ **Security inspection or investigative information**. Details of any transportation security inspection or investigation of an alleged violation of aviation, maritime, or surface transportation security requirements of Federal law that could reveal a security vulnerability.

   Examples: Unplanned (incident- or violation-related) inspection or investigative information.

7. ☐ **Threat information**. Any information held by the Federal Government concerning threats against transportation or transportation systems, sources or methods used to gather or develop threat information, including threats against cyber infrastructure.

   Examples: Threat analysis; suspicious incident reporting; trend analysis; details of bomb threat.

8. ☐ **Security measures**. Specific details of transportation security measures or protocols, information concerning the deployments, numbers, and operations of Coast Guard personnel

engaged in maritime security duties, Federal Air Marshals (FAMs)and Federal Flight Deck Officers (FFDOs), and any armed security officer procedures issued by TSA under 49 C.F.R. Part 1562. *Examples:* Non-screening security measures; FAM/FFDO deployments and operations; FAM numbers.

9. ☐ **Security screening information.** Security screening under aviation or maritime transportation security requirements of Federal law: 1) procedures for screening of persons, property, and cargo; 2) information and sources of information used by a passenger or property screening program or system; 3) security screener tests and scores; 4) performance or testing data from security equipment or screening systems; 5) screening images or threat image projection systems (TIPS) images.

   Examples: Checkpoint Screening Standard Operating Procedures (SOP); Checked Baggage SOP; security screening procedures; electronic images from screening monitors.

10. ☐ **Security training materials**. Records created or obtained for the purpose of training persons to carry out transportation security measures.

    Examples: Transportation Security Officer training manuals; training materials related to security.

11. ☐ **Identifying information of certain transportation security personnel.** Lists of names or other identifying information that identify persons as 1) having unescorted access to a secure area of a transportation facility, 2) holding a position as a security screener (e.g., TSOs) employed by or under contract with the Federal Government (e.g., SPP airports), or 3) holding a position as a Federal Air Marshal or Federal Flight Deck Officer.

    Examples: Lists of Transportation Security Inspectors (TSIs), lists of most or all Transportation Security Officers (TSOs) at an airport.

12. ☐ **Critical transportation infrastructure asset information**. Any list identifying systems or assets, whether physical or virtual, so vital to the transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security.

    Examples: Lists of critical pipeline entities; used infrequently.

13. ☐ **Systems security information**. Any information involving the security of operational or administrative data systems operated by the Federal Government and are critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

    Examples: Security information on IT systems that are mission essential systems (MES) or high-value assets (HVAs), including screening technology.

14. ☐ **Confidential business information**. Information contained in 1) solicited or unsolicited proposals received by DHS or DOT to perform work pursuant to a grant, contract, cooperative agreement, or other transaction; 2) trade secret information, including information required or requested by regulation or Security Directive; or 3) commercial or financial information.

    Examples: Rarely used; consult SSI Program office.

15. ☐ **Research and development**. Information obtained or developed in the conduct of research related to transportation security activities including research results.

    Examples: Next generation of screening equipment test results.

16. ☐ **Other information**. Any information not otherwise described in 49 C.F.R. § 1520.5(b) that TSA determines is SSI. Upon the request of another Federal agency, TSA may designate as SSI information not otherwise described in this section.

    Examples: Aggregate incident data; railroad automated equipment identification reader locations; names and identifying information on Inspections Covert Testers; consult SSI Program office at ssi@tsa.dhs.gov for a current list.

Sensitive Security Information (SSI)
Threshold Analysis

PART B: Summary of the System

DATE submitted for review:
NAME of System: <Please enter the name.>
Department Component Owner: <Please enter the component name.>
Name of System Owner: <Please enter the name.>
Email for System Owner: <Please enter the email address.>

Name of ISSO: <Please enter the name.>
Email for ISSO: <Please enter the email address.>

TYPE of System:

☐ General Support System ☐ Major Application
☐ Minor Application ☐ Non-DHS System

Status of System:

☐ This is a new development effort undergoing **initial Security Authorization**.

☐ This is an operational system going through **reauthorization**.

☐ This is a non-DHS system which does not require **Security Authorization**.

Purpose of System: <One Sentence Description>

Collection and Use of SSI: Describe how the system collects and uses SSI, including a typical transaction that gives the life cycle from collection/creation to destruction of SSI.
<One to Two Sentence Description>

Information Sharing: Describe any information sharing conducted by the system.
<One to Two Sentence Description>

Sensitive Security Information (SSI)
Threshold Analysis

PART C: SSI Use Determination and Endorsement

Note: Endorsement on this SSI Threshold Analysis does not remove the applicant's requirement to complete other documentation which may be required by other program offices.

SSI Use Determination

☐ This system DOES collect, process, maintain, use, share, disseminate, or dispose of SSI.

☐ This system DOES NOT collect, process, maintain, use, share, disseminate, or dispose of SSI.

ISSO	**Date**
System or Program Owner (as appropriate)	**Date**
TSA SSI Program Office Reviewer	**Date**

SSI Impact Assessment

Appendix 7 to SSI Policies & Procedures Handbook

Version 2

SSI Program
Current as of 15 July 2022

Sensitive Security Information (SSI)
Impact Assessment

The purpose of this SSIIA is to determine how SSI (as defined in 49 C.F.R. Part 1520) is being protected within TSA IT systems; to verify compliance with SSI policies and procedures; and, if necessary, to propose alternate acceptable protection in lieu of standard SSI policies and procedures.

The TSA SSI Program office will review this SSIIA and advise if additional protections will be required for the system seeking Security Authorization through Information Technology (IT). This SSIIA may also be used by other non-TSA systems or other secure sites not requiring Security Authorization to document alternate acceptable protection in lieu of standard SSI policies and procedures.

SSIIA must be completed (1) during each review of Authorization to Operate (ATO); (2) during any significant modification or update to the system impacting users or information available on the system; or (3) every three years, whichever event occurs first.

Use the attached template to complete the SSIIA as required by TSA MD 2810.1, *SSI Program*, TSA SSI Policies & Procedures Handbook, or SSI Threshold Analysis (SSITA). Definitions of the terms used within this document may be found in the *TSA SSI Information Assurance Handbook*, Section 5, *Definitions*.

Submit the completed SSIIA to the TSA SSI Program office at SSI@tsa.dhs.gov for review. Upon receipt, the SSI Program office may contact the sender for further information and/or documentation.

A copy of this template is available on the TSA SSI Program office SharePointSharePoint homepage.

Abstract[52]

<<ADD Abstract here>>

Overview[53]

<<ADD Introduction Here>>

Section 1.0 - Authorities

1.1 Has the system been approved for the management of sensitive information by TSA Information Technology?[54]

<<ADD Answer Here>>

Section 2.0 - Characterization and Uses of SSI

The following questions are intended to define the scope of the information created and/or collected, as well as reasons for its creation or collection.

2.1 Identify the SSI that the system collects, stores, or disseminates.

<<ADD Answer Here>>

2.2 Describe how and why the system creates, collects, and uses SSI.

<<ADD Answer Here>>

---

[52] The abstract is a single paragraph that describes the program and the SSIIA which should conform to the following format: first sentence should include the name of the component or program office and the system; second sentence should be a brief description of the system and its function; third sentence should provide an analysis of the role of SSI in the program.

[53] Include the following: 1) Describe the system's purpose and how it relates to the Agency's mission. 2) Describe generally how the system collects and uses SSI, including a typical transaction that gives the life cycle from collection/creation to destruction of SSI. 3) Describe any information sharing conducted by the system. 4) Describe the major potential risks of unauthorized disclosure or mishandling within the program, how the program plans to protect SSI, and steps taken to mitigate the risks of unauthorized disclosure of SSI. 5) Identify the technology used and provide a brief description of how it maintains SSI for the system. Include descriptions of any encryption mechanisms in place. If applying for alternate acceptable protections in lieu of or as an exception to current SSI Policies & Procedures, list the SSI Program policies for which the applicant seeks a waiver.

[54] An operational system managing sensitive information, including SSI, must comply with DHS Policy Directive 4300A, DHS Sensitive Systems Policy. Provide the date that the most recent ATO was granted or, if a new system, the date ATO is expected to be awarded. If this SSIIA is being completed as part of a Security Authorization package, please state that here.

2.3 Describe how the SSI is conveyed (e.g., multimedia formats such as audio or video files).

<<ADD Answer Here>>

2.4 Explain how the data and records are properly identified and labeled as SSI.

<< ADD Answer Here>>

Section 3.0 - Data maintenance and information sharing by the system

3.1 Describe how the SSI is maintained by the system.

<<ADD Answer Here>>

3.2 Describe the mechanism used to share and distribute the SSI to other offices.

<<ADD Answer Here>>

3.3 If the system receives SSI from another office or system, describe the information exchange, how the SSI is then used, and who has access to the SSI.

<< ADD Answer Here>>

3.4 If applicable, describe how SSI is shared outside of TSA as part of normal system operations. Identify the entities with which the SSI is shared, how the information is accessed by those entities, and how they use the SSI.

<<ADD Answer Here>>

3.5 Discuss the review process and documentation (e.g., Interconnection Security Agreements (ISAs), Memorandums of Understanding (MOUs)) for any new requests for access to SSI data within TSA and by outside entities.

<<ADD Answer Here>>

3.6 Describe any limitation that may be placed on external agencies or entities from further sharing the SSI provided by the system.

<<ADD Answer Here>>

Section 4.0 - Risk Management

4.1 Discuss the risks and mitigation measures (e.g., encryption) associated with maintenance of the SSI created, collected or maintained by the system.

<<ADD Answer Here>>

4.2 Discuss any risks of unauthorized disclosure and risk mitigation measures (e.g., access controls, policies) that guard against the SSI being disclosed to non-covered persons or covered persons without a need to know the information.

<<ADD Answer Here>>

4.3 Describe the security controls that ensure confidentiality of the information is maintained to individuals with a need to know throughout the lifecycle (i.e., the creation, collection, maintenance, dissemination, and destruction) of the SSI.

<<ADD Answer Here>>

4.4 Describe any measures and frequency of measures used to notify site or system users of data sensitivities, required SSI protections, and limitations on distribution such as Terms of Use Agreements, system notices, or pre-use guidance (e.g., training, SOPs).

<<ADD Answer Here>>

<<ADD Sample Terms of Use Agreement and System Notices Here>>

Section 5.0 - Auditing and Accountability

The following questions are intended to describe technical, regulatory, and policy based safeguards and security measures.

5.1 Describe any technical and policy safeguards and controls used to adhere to this SSIIA.

<<ADD Answer Here>>

5.2 Describe any system-specific training efforts to ensure system users appropriately handle SSI within the system and as it is exported from the system.

<<ADD Answer Here>>

5.3 Explain any SSI education and awareness efforts for system staff and administrators.[55]

<<ADD Answer Here>>

5.4 Describe protocols that are designed to report an unauthorized disclosure of SSI.

[55] SSI Program office provides Advanced SSI Training to data managers or others responsible for monitoring site content, as needed. For more information, contact the SSI Program office at SSI@tsa.dhs.gov.

<<ADD Answer Here>>

Section 6.0 - Additional Protections Required

The following section must be filled out by the SSI Program office reviewer, in conjunction with the System Owner and IT's Information Assurance and Cybersecurity Division.

6.1 Based upon the sensitivity of the information and vulnerability to access as noted within this document, describe any additional protections which would mitigate the risk of information compromise.

<<ADD Specific FIPS impact level high requirements here>>

Endorsements[56]

Signatures below signify concurrence with proposed protections as annotated in this SSI Impact Assessment. Any failure by the System Owner to apply protections as annotated in this document nullifies below approvals.

Information Owner[57]	**Date**
ISSO	**Date**
System or Program Owner (as appropriate)	**Date**
TSA SSI Program Office Reviewer	**Date**
Risk Assessment Lead	**Date**

CC: Chief Data Officer

[56] **Note:** Endorsement by the SSI Program office on this SSI Impact Assessment does not remove the applicant's requirement to complete other documentation which may be required by other program offices. ISSO and CISO signatures are only required when the SSIIA will be used as part of a Security Authorization Package.

[57] This is typically a representative in the program office which generates the need for the system.

Addendum to Appendix: 4 SSI Incident Response Flow Chart

1. When TSA or DHS Personnel discover an SSI Incident, they are required to report that incident to their manager/supervisor and their SSI Coordinator. Proceed to step 2.
2. The manager/supervisor must either report the incident to the SSI Coordinator or, in the event of the unavailability of the SSI Coordinator, report the incident to the SSI Program directly. Proceed to step 3.
3. The SSI Program and the incident contact then coordinate to determine whether the SSI Incident is Major or a Policy Violation. SSI Incident Reports must be completed for Password or Major Incidents. Proceed to step 4.
4. The following after-reporting actions are taken:
    a. If policy violation, proceed to step 7.
    b. If password incident, proceed to step 5.
    c. If, during the initial incident assessment, the SSI Coordinator determines the SSI Incident may be major, the SSI Coordinator must also notify the Transportation Security Operations Center (TSOC). Note: Security Operations Field SSI Coordinators must report major SSI incidents to the TSOC through their Coordination Center. Proceed to step 5.
5. Send the SSI Incident Report to the SSI Program. The SSI Program determines whether the incident actually involves SSI. If so, SSI Staff processes the SSI Incident Report and begins the notification process.
    a. If password, the SSI Program office evaluates whether the password incident requires the issuance of a new Standard TSA Password and coordinates with the SSI Coordinator to advise on other appropriate mitigation strategies for each password incident. Stop.
    b. If major, proceed to step 6.
6. At this step, refer to Handbook Section 10.0, SSI Incidents. If this is a Major Incident, the SSI Program makes appropriate notifications by sending to the following groups, as appropriate: Chief Counsel (Information Law), Security Operations (SO), and the program office that is the owner of the lost/breached data. If it is a loss/breach by a TSA Employee, the SSI Program may notify Investigations. If it is a loss/breach by a TSA Stakeholder, the SSI Program may notify Compliance and Policies, Plans and Procedures. If it is an electronic incident, the SSI Program notifies C-SIRT and TSA SOC. The SSI Program may notify others, as appropriate. Proceed to step 7.
7. The SSI Program works with the incident contact to mitigate the incident and then the SSI Program closes out the SSI incident internally. As necessary, the incident is reviewed for long-term risk mitigation and incident investigation. Stop.