



Sensitive Security Information

Best Practices Guide for Non-DHS Employees and Contractors

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

What is SSI?

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

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

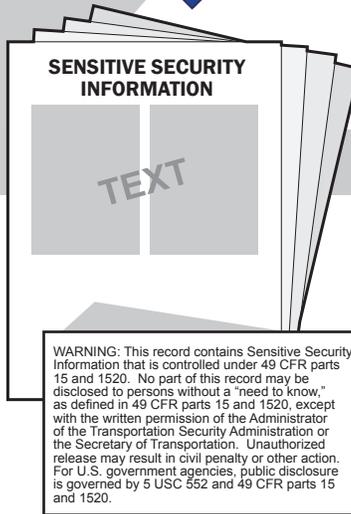
SSI Requirements

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

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

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

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



Best Practices Guide

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

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