www.tsa.gov

Sensitive Security Information

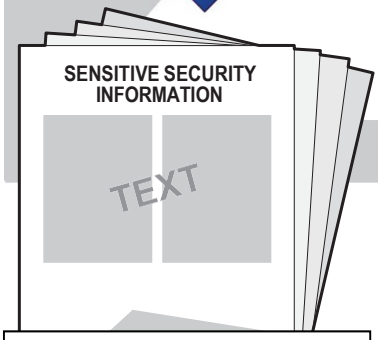
Best Practices Guide for Non-DHS Employees and Contractors

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.



"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."

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 or in a locked room (as defined by Federal regulation 49 C.F.R. part 1520.9 (a)(1)).

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.

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).

Best Practices Guide

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

* Use an SSI cover sheet on all SSI material.
* Electronic presentations (e.g., PowerPoint) should be marked with the SSI header on all slides and with the SSI footer on the first and last slides of the presentation.
* Spreadsheets should be marked with the SSI header and the SSI footer (or an image of the footer) on every page.
* Video and audio should audibly state protection requirements and/or show the header and footer at the beginning and end of the recording.
* CDs/DVDs should be encrypted or password-protected, with the header on the media; the header and footer should be affixed to the outside case, jacket, or sleeve.
* Mobile electronic media, including USB flash drives, do not need to be marked. The drive itself should be encrypted or all SSI documents stored on it should be password protected. All SSI documents should be appropriately marked.
* When leaving your computer or desk you must lock up all SSI, and you should lock or log off your computer.
* Taking SSI home is not recommended. If necessary, get permission from a supervisor and lock up all SSI at home.
* Do not handle SSI on computers that have peer-to-peer software installed on them or on your home computer.
* Properly destroy SSI using a cross-cut shredder.
* Encrypt SSI in transmission, either in a separate encrypted attachment (i.e., password-protected document) or in an encrypted email (if available). SSI should not be placed in the subject line of an email, or in the body of an unencrypted email.
* 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 is discouraged unless a more secure option is not feasible. Before faxing, verify 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 or file-sharing sites should either require a password to open or the network should limit access to the folder or site to only those with a need to know.
* Properly destroy electronic records using any method that will preclude recognition or reconstruction.