www.tsa.gov

Sensitive Security Information

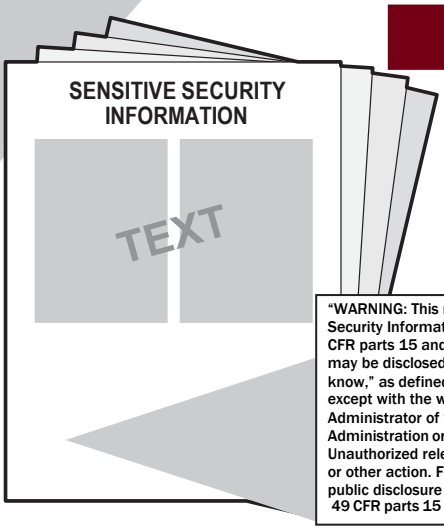
SSI Quick Reference Guide for DHS Employees and Contractors

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 policies and procedures for recognizing, marking, protecting, safely sharing, and destroying SSI. This guidance is required of all DHS and component organization employees and contractors.

Marking SSI



Even when only a small portion of a document contains SSI, every page of the document must be marked with the SSI header and footer.

Don't...

- ★ Don't leave SSI unattended. Leave it in a locked drawer, locked file cabinet, or locked office.
- ★ Don't post SSI on any Internet web site or social media.
- ★ Don't take SSI home without permission from your supervisor.
- ★ Don't share SSI with individuals who do not have a need to know.
- ★ Don't place SSI in the subject line of an email, or in the body of an unencrypted email.
- ★ Don't use personal email or download SSI onto personally-owned electronic devices such as computers, smart phones or other mobile-electronic media.

Recognizing SSI

SSI is information about transportation security activities. The following information constitutes SSI (as defined in 49 C.F.R. part 1520):

1. Security programs, security plans, and contingency plans
2. Security Directives
3. Information Circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspection or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical transportation infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator

Do...

- ★ Make sure all SSI is properly marked.
- ★ Use an SSI cover sheet on all SSI materials.
- ★ Protect SSI according to the SSI regulation and report any unauthorized disclosures or poor security practices to your SSI Coordinator and supervisor.
- ★ When leaving your computer or desk, lock up all SSI and mobile electronic media, and lock or log off your computer.
- ★ Encrypt SSI in transmission, either in a separate encrypted attachment (i.e., password-protected document) or in an encrypted email (if available). Call or send the password in a separate, non-descript email.
- ★ SSI stored in network folders or file-sharing sites should either require a password to open or limit access to the folder or site to only those with a need to know.
- ★ Personally hand-deliver SSI to the intended recipient; never leave SSI unattended in the recipient's work space.
- ★ Be conscious of your surroundings and take measures to prevent eavesdropping or shoulder-surfing.
- ★ Use encrypted mobile electronic media (e.g., USB flash drives, hard drives).
- ★ Mail SSI 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.
- ★ Only use secure video conferencing tools approved by DHS.

Destroying SSI

- ★ Destroy SSI when no longer needed.
- ★ Shred with a cross-cut shredder.
- ★ Where available, place SSI in designated SSI bins.
- ★ Use any method approved for the destruction of classified.
- ★ Destroy electronic SSI using any method that will preclude recognition or reconstruction of the information.