www.tsa.gov

Sensitive Security Information

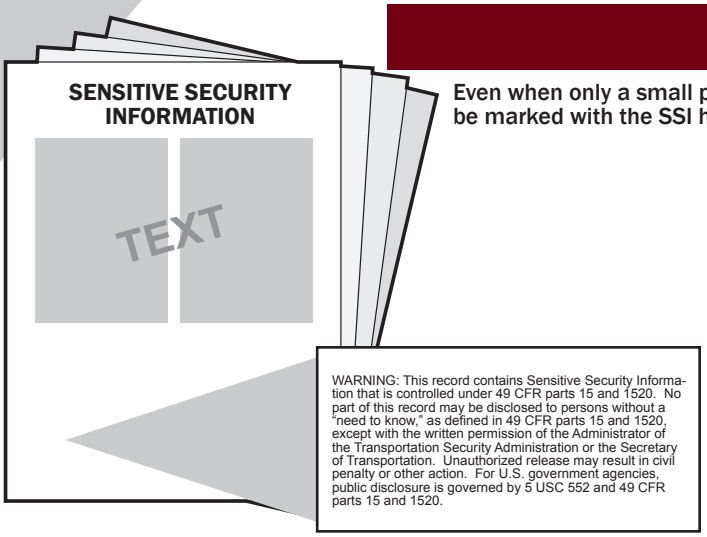
SSI Quick Reference Guide for DHS Employees and Contractors

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 or locked file cabinet.
- ★ Don't post SSI on any Internet web site. Only post SSI on Intranet web sites with prior approval.
- ★ Don't take SSI home without permission from your supervisor(s).
- ★ Don't share SSI with individuals who do not have a need to know.
- ★ Don't put SSI in the body of an email—send it as a password-protected attachment.
- ★ Don't download SSI onto personal computers or other personal data storage devices.

Recognizing SSI

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

1. Security programs and contingency plans
2. Security Directives
3. Information Circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspections 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 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.
- ★ Lock up all notes, draft documents, electronic media, and other material containing SSI.
- ★ Turn off or lock your computer whenever you leave your desk to ensure that no SSI is compromised.
- ★ 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.
- ★ Personally hand-deliver SSI to the intended recipient; never leave SSI unattended in the recipient's work space.
- ★ Destroy all SSI in your possession when no longer needed.
- ★ Be conscious of your surroundings when discussing SSI. Protect verbal communications with the same heightened awareness that you would apply to SSI on paper or email.
- ★ Use encrypted portable devices (i.e. thumb drives) or password-protect SSI on electronic media.
- ★ 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.

Destroying SSI

- ★ Shred with a cross-cut shredder.
- ★ Cut manually into squares smaller than ½-inch.
- ★ Where available, place SSI in designated and clearly marked SSI bins.
- ★ Destroy electronic SSI using any method that will preclude recognition or reconstruction of the information.

Phone: (571) 227-3513 • Fax: (571) 227-2945
SSI@dhs.gov