ORAL ARGUMENT SCHEDULED FOR MARCH 10, 2011

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER, ET AL.,	)	
Petitioners,	)	
v.	)	No. 10-1157
JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security, ET AL.,	)	
Respondents.	)	

MOTION FOR LEAVE TO FILE SEALED *EX PARTE* SUPPLEMENTAL APPENDIX

Respondents Janet Napolitano, in her official capacity as Secretary of the U.S. Department of Homeland Security, et al., hereby move for leave to file a sealed *ex parte* supplemental appendix in the case.[1] Respondents' reasons are as follows:

1. This case arises out of a petition for review of agency action, challenging the use of Automated Imaging Technology (AIT) by the Transportation Security

[1] An original and seven copies of the document in question are being lodged with the Court on the date of filing of this motion.

Administration (TSA). The parties are using the "deferred appendix" method, and all of the initial briefs have been filed. Pursuant to the Court's order of December 9, 2010, the parties' final briefs are due on January 27, 2011.

2. On January 19, 2011, petitioners filed in this Court the public Joint Appendix containing material identified in the Amended Certified Index of Record (filed by respondents on October 29, 2010) and cited by the parties in their briefs.

3. As the Amended Certified Index of Record itself makes clear, however, some of the material in the administrative record cannot be publicly disclosed. Congress has mandated that TSA "shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security . . . if [TSA] decides that disclosing the information would . . . be detrimental to the security of transportation." 49 U.S.C. § 114(s)(1)(C). Pursuant to that authority, TSA has defined a set of information known as "sensitive security information" or "SSI" (*see* 49 C.F.R. § 1520.3), which includes "[a]ny Security Directive . . . [i]ssued by TSA," 49 C.F.R. § 1520.5(b)(2)(i). Such information shall not be disclosed except in certain limited circumstances. 49 C.F.R. § 1520.9(a)(2). SSI is different from classified information, but pursuant to federal statute and implementing regulations, it may not be publicly disclosed.

TSA has reviewed the material that constitutes the administrative record in this case. As the Amended Certified Index of Record indicates, TSA has determined that certain portions of the administrative record constitute SSI and must therefore be redacted from the public record. TSA has served a redacted version of administrative record on petitioners, and redacted excerpts from the SSI documents therefore appear in the Joint Appendix.[2] However, the agency wishes to make available to the Court in unredacted form all of the redacted portions of the SSI documents cited in its brief (Amended Certified Index of Record items 38, 49, 50, 51, 53, 54, 57, 61, 88, and 122).[3] For the convenience of the Court, the nonpublic SSI material in the supplemental appendix is clearly identified on the appendix pages by boxes around the redacted information.

---

[2] TSA further informed petitioners' counsel that it may be possible to release some or all of the sensitive security information to them, under an appropriate protective order issued by this Court, pursuant to the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 § 525(d), 120 Stat. 1355, 1382 (Oct. 4, 2006) ("Section 525(d)") (reenacted by Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, § 522, 121 Stat. 1844, 2074 (Dec. 26, 2007); Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, Pub. L. No. 110-329, Div. D, § 510, 122 Stat. 3574, 3682 (Sept. 30, 2008)). By letter, TSA informed petitioners' counsel of the steps required for them to secure clearance to view SSI material. To date, however, they have not initiated that process.

[3] For the Court's guidance and use, we are attaching two one-page documents (TSA's "Best Practice Guide" and its "Quick Reference Guide") that explain the proper handling of SSI material.

4. In addition, as the Amended Certified Index of Record further indicates, the administrative record contains several copyrighted items that were provided to TSA through a single-user license. TSA also wishes to make available to the Court these copyrighted documents (Amended Certified Index of Record items 1, 4, 46, and 67), which were cited in its brief.

5. In order to make all of the SSI and copyrighted documents available to the Court, pursuant to D.C. Cir. R. 47.1(e)(1), respondents seek permission to file a sealed *ex parte* supplemental appendix consisting of both sets of documents specified in ¶¶ 3 and 4, *supra*. Because petitioners have already supplied redacted excerpts from the documents in the public Joint Appendix, respondents respectfully suggest that the Court should dispense with the Rule's otherwise applicable requirement to file a "second appendix segment" that would also be made public.

6. John Verdi, Esquire, counsel for petitioners, has authorized us to state that petitioners oppose this motion.

CONCLUSION

For the foregoing reasons, the Court should grant respondents leave to file a sealed *ex parte* supplemental appendix consisting of the above-described SSI and copyrighted material.

Respectfully submitted,

/s/ Douglas Letter
DOUGLAS LETTER
(202) 514-3602
Douglas.Letter@usdoj.gov

/s/ John S. Koppel
JOHN S. KOPPEL
(202) 514-2495
John.Koppel@usdoj.gov
Attorneys, Appellate Staff
Civil Division, Rm. 7264
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

CERTIFICATE OF SERVICE

I hereby certify that on the 28th day of January, 2011, I caused the foregoing Motion to be filed electronically with the Court via the Court's CM/ECF system, and also caused four copies to be delivered to the Clerk of the Court by hand delivery on that same date. On the same date, service will also be made automatically upon the following CM/ECF participants, and by first-class mail upon the *pro se* petitioner identified below:

Marc Rotenberg, Esquire (CM/ECF participant)
John Verdi, Esquire (CM/ECF participant)
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington , DC 20009

Nadhira Al-Khalili, Esquire (*pro se* petitioner)
453 New Jersey Avenue, SE
Washington, D.C. 20003

/s/ John S. Koppel
JOHN S. KOPPEL
Attorney

www.tsa.gov

Sensitive Security Information

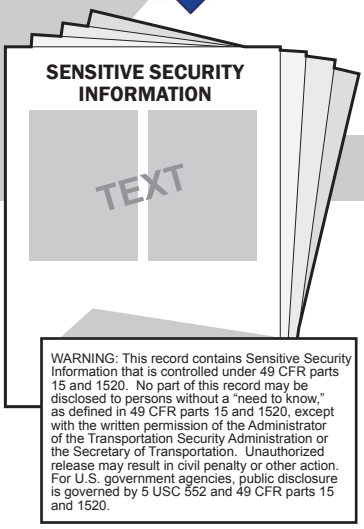
Best Practices Guide for Non-DHS Employees

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 recontruction.

Transportation Security Administration

Phone: (571) 227-3513 • Fax: (571) 227-2945

Safely Sharing Information
SSI@dhs.gov

www.tsa.gov

Sensitive Security Information

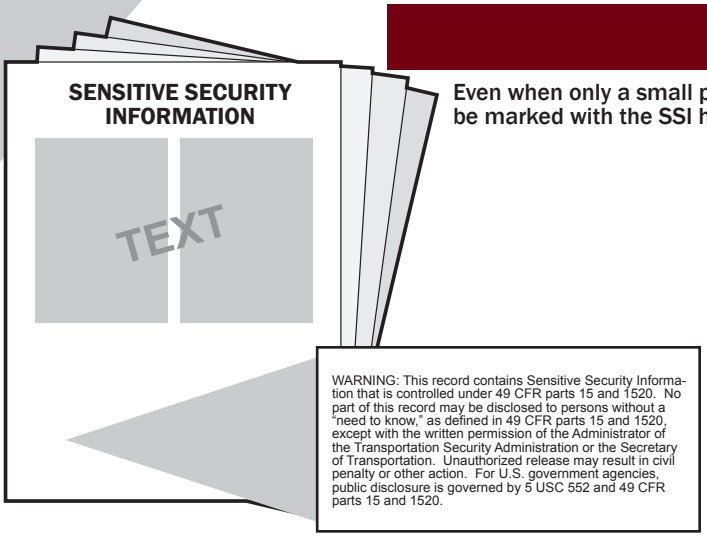
SSI Quick Reference Guide for DHS Employees and Contractors

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.