

NON-DISCLOSURE AGREEMENT

I, _____, an individual official, employee, consultant, or subcontractor of or to

_____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of Pierce Transit.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	Protected Critical Infrastructure Information (PCII)
-----------	---

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 USC 101 et seq.), as amended, the implementing regulations thereto (6 CFR Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	Sensitive Security Information (SSI)
-----------	---

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 CFR Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of Pierce Transit.

Initials:	Other Sensitive but Unclassified (SBU)
-----------	---

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified. I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.
2. By being granted conditional access to the information indicated above, Pierce Transit has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.
3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that Pierce Transit may conduct

inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII –

(1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a Pierce Transit contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same manner as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations. I agree that I shall properly dispose of all SSI, PCII, or SBU materials or data received from Pierce Transit in a manner consistent with the requirements articulated in the attached SSI Reference Guide, at such time those materials are no longer needed for investigative purposes or legally required to be kept.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the Pierce Transit all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII, I hereby assign to the entity owning the PCII and Pierce Transit, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

10. This Agreement is made and intended for the benefit of and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

12. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

I understand and agree to the following terms and conditions of my access to the information indicated above. I make this Agreement in good faith, without mental reservation or purpose of evasion.

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address:	Telephone Number:
Signature:		

Witness

Typed/Printed Name:	Government/Department/Agency/Business Address:	Telephone Number:
Signature:		



Sensitive Security Information

SSI Quick Reference Guide for DHS Employees and Contractors

What is SSI?

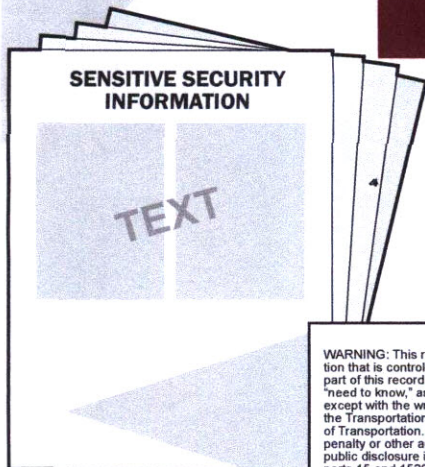


Sensitive Security Information (SSI) is information that, if publicly released, would be *detrimental to transportation security*, as defined by Federal regulation 49 C.F.R. part 1520.

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.



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 USC 552 and 49 CFR parts 15 and 1520.

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



Destroying SSI

- ★ Shred with a cross-cut shredder.
- ★ Cut manually into squares smaller than 1/2-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.



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.

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.