NON-DISCLOSURE AGREEMENT WITH
CAPITAL AREA TRANSPORTATION AUTHORITY
4615 Tranter St., Lansing, MI 48910

SENSITIVE SECURITY INFORMATION

N O T I C E T O V E N D O R S:

In the course of preparing and submitting proposals or bids for Capital Area Transportation Authority ("CATA") project CTC-CCTV Camera Project ("CATA Project") , or if awarded a contract, performing the required work, you may be provided access to Sensitive Security Information, or other confidential or proprietary information that is restricted from dissemination or disclosure by Federal law and regulations, including the Critical Infrastructure Information Act of 2002 (CAA 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, 49 CFR Part 1520, "Protection of Sensitive Security Information", "Policies and Procedures for Safeguarding and Control of SSI", as amended, 49 CFR Part 15 Protection of Sensitive Security Information, and any supplementary guidance issued by an authorized official of CATA.

Sensitive Security Information is an over-arching term that covers any information, that the loss of, misuse of, or unauthorized access to or modification of could adversely affect transportation security, the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled. Sensitive Security Information may be in printed or electronic form and may include oral communications. CATA will make every effort to clearly mark written Sensitive Security Information as such, and will communicate the sensitive nature of other forms of information when provided to vendors. IF THERE IS ANY QUESTION regarding whether information which has come to your attention is Sensitive Security Information, you should ask Mr. Doug Heins, who is CATA's Safety Manager with respect to such information.

Attached to this Agreement is a Sensitive Security Information Quick Reference Guide, which sets forth the manner in which Sensitive Security Information should be treated. IF YOU HAVE ANY QUESTIONS regarding procedures to follow and the treatment of Sensitive Security Information which you have obtained from CATA, you should direct your questions to Mr. Doug Heins, who is CATA's Safety Manager.

Any vendor wishing to submit a bid or a proposal with respect to the above-referenced project, or to perform the work if a contract is awarded, must, as a condition and in consideration of being granted access to Sensitive Security Information, agree to the terms of this Agreement.

1. I hereby acknowledge that I have received instructions from CATA concerning the nature and protection of Sensitive Security Information, 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. I agree to protect Sensitive Security Information that I receive from CATA from unauthorized disclosure, in accordance with the terms of this Agreement, Federal laws and regulations and CATA directives.

3. I agree that CATA may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding of Sensitive Security Information under this Agreement.

4. I will not disclose or release any Sensitive Security Information provided to me by CATA 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 Federal laws and regulations, or CATA directives. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by CATA.

5. I agree that material which I have in my possession containing Sensitive Security Information 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 Federal laws and regulations, or CATA directives. I agree that I shall return such information to which I have had access or which is in my possession (1) upon demand by CATA; and/or (2) upon the conclusion of my duties, association, or support in connection with the above-referenced CATA Project; and/or (3) upon the determination that my official duties do not require further access to such information and/or (4) at such time those materials are no longer needed for investigative purposes or legally required to be kept.

6. I 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, unless such alteration or removal is authorized by CATA. 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 matter as the original.

7. I hereby agree that I shall promptly report to the appropriate CATA official 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 materials or data received from CATA in a manner consistent with the requirements articulated in the attached SSI Reference Guide.

8. If I violate the terms and conditions of this agreement, such violation may result in the cancellation of my access to the information covered by this Agreement, rejection of any bid or proposal, cancellation of any project awarded and disbarment from future procurements from CATA.

9. This Agreement is made and intended for the benefit of and may be enforced by the United States Government or the State of Michigan as well as by CATA. Those entitled to enforce this Agreement may seek any remedy in law or in equity to enforce this agreement including, but not limited to, the application for a court order prohibiting disclosure of information in breach of this Agreement and I shall be liable for all reasonable attorney fees and costs. I acknowledge that irreparable harm will result from a breach of this Agreement. I understand and agree neither CATA nor any entity with the right to enforce this Agreement has waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any Sensitive Security Information.

10. I agree that all conditions and obligations imposed upon me by this Agreement apply not only during the time that I am granted access, but also at all times thereafter.

11. 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.

12. 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.

13. 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 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)) or any similar law of the State of Michigan. The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. Signing this Agreement does not bar disclosures to State or Federal enforcement bodies that are essential to reporting a substantial violation of law.

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

16. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that CATA 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.

17. I agree that the information subject to this Agreement shall only be disclosed to employees, agents, co-workers or employees who have a need to know such information, and who have executed a copy of this Agreement. I shall provide CATA with a copy of the executed Agreement.

The undersigned, intending to be legally bound, hereby consents and agrees to the terms in this Agreement.

By: _____ _____

Date

_____

Company Name

_____

Address

_____

City, State, and Zip

_____

Phone #

_____

E-Mail Address

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.

Recognizing SSI

The following information constitutes SSI:

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

The purpose of this brochure is to provide transportation security stakeholders 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.

The SSI Office

TSA's Sensitive Security Information (SSI) Office:

- ✓ Develops SSI guidance, policies, and procedures to help others appropriately recognize and handle SSI.
- ✓ Analyzes and reviews records for SSI content.
- ✓ Trains TSA employees, clients, and stakeholders in identifying, handling, marking, sharing, storing, transmitting, and destroying SSI.
- ✓ Coordinates with stakeholders, other governmental agencies, and Congress on SSI-related issues.

www.tsa.gov

For more information:

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

Sensitive Security Information

✓Stakeholder Best Practices Quick Reference Guide

Transportation Security Administration

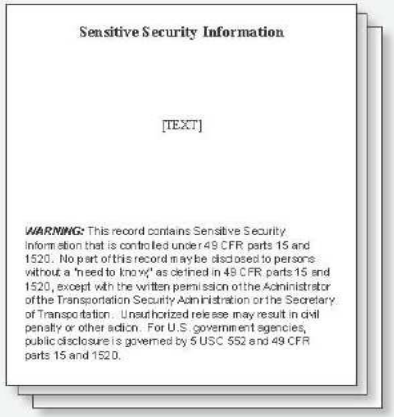
SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

You Must – Lock-up All SSI
When not in physical possession, store SSI in a secure container such as a locked file cabinet or drawer.

You Must – When No Longer Needed, Destroy SSI
Destruction of SSI must be complete to preclude recognition or reconstruction of the information.

You Must – Mark SSI
The regulation requires that 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 below.



When Combining SSI With Other Sensitive But Unclassified (SBU) Information, the document must be marked as SSI. SSI extracted from SSI documents requires the new document to be marked and protected as SSI.

Best Practices Guide

Reasonable Steps Must be Taken to Safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Office offers these best practices as examples of reasonable steps:

- ✓ **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 and DVDs** should be encrypted or password-protected and the header and footer should be affixed to the CD or DVD.
- ✓ **Portable Drives** including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all documents stored should be password-protected.
- ✓ **When Leaving Your Computer or Desk** you must lock up all SSI and should lock or turn off your computer.
- ✓ **Taking SSI Home** is not recommended, but if necessary, get permission from a supervisor and lock up all SSI at home.
- ✓ **Discussing SSI Over Cellular Telephones** should be done carefully to prevent eavesdropping. Land lines in non-public locations are more secure than cellular telephones.
- ✓ **Email** should not contain SSI in the body of the email. SSI should be emailed in a password-protected attachment. Passwords should be sent separately with no subject line or shared either in person or via telephone.
- ✓ **Passwords for SSI Documents** should contain at least 8 characters, have at least one upper-cased and one lower-cased letter, contain at least one number, 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 to retrieve the SSI once faxed.
- ✓ **SSI Should Be Mailed** by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping and the outside wrapping 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 on Network Folders** should either require a password to open or the network should limit access to the folder.
- ✓ **Destroying SSI** should be done using a cross-cut shredder which produces particles that are 1 ½ inch by ¾ inch or smaller.