

SSI – Sensitive Security Information – Processes and Procedures

Table of Contents

- Introduction;
- What is SSI? – CFR 49, Part 1520 and Part 15;
- SSI at DEN;
- Project Limitations;
- If SSI...;
- SSI Requirements;
- Best Practices Guide;
- Attachments
 - o DEN Policy 10003 – Protection of Sensitive Security Information (SSI)

Introduction

This section of the Tenant Development Guidelines addresses the relatively recent concern of how we handle and process the “Sensitive Security Information” (SSI) that we may come in contact with as we go about executing our design and construction projects.

What is SSI? – the Code of Federal Regulations (CFR) 49, Part 1520 and Part 15

SSI is information that, if publically released, would be detrimental to transportation security. It is rigorously defined by the Code of Federal Regulations (CFR) 49, Part 1520 and Part 15. Only excerpts considered relevant to design and construction of tenant facilities at DEN are referenced below.

CFR 49 Part 1520 lists many types of information that may be considered SSI, but the types of information that we may come into contact with as we design, construct or reconstruct airport facilities are the following:

- Critical aviation infrastructure or asset information;
- Security measures such as specific details of aviation security, both operational and technical;
- Performance specifications including any description of a test object or a test procedure;

Persons subject to the requirements of part 1520 are called Covered Persons and include:

- Airport Operators (including their employees);
- Aircraft Operators (airlines and their employees);
- Any person who receives SSI.

All Covered Persons have a duty to protect information as per the following:

- Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure;
- Disclose, or otherwise provide access to, SSI only to Covered Persons who have a need to know;
- Refer requests by other persons for SSI to TSA or the applicable component or agency within Department of Transportation (DOT) or Department of Homeland Security (DHS);
- Dispose of SSI as specified in §1520.19;
- When a Covered Person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly notify the Airport Security Coordinator on duty via the

Communications Center (x4020) or via the Project Manager.

Consequences of unauthorized disclosure of SSI:

- Violation of this part (1520) is grounds for a civil penalty and other enforcement or corrective action by DHS. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.
- City and County of Denver – Department of Aviation violation of Part 20. Violation Notice hearing may be required, which may lead to revocation of airport ID badge privileges.

Destruction of SSI:

- In general, a Covered Person must destroy SSI completely to preclude recognition or reconstruction of the information when the Covered Person no longer needs the SSI to carry out his function within transportation security measures.

SSI at DEN

You can see from this very brief excerpt from Part 1520 that the subject of SSI can become very complicated and the requirements for handling and marking SSI, non-disclosure of SSI, the consequences of unauthorized disclosure, the safekeeping and eventual destruction of SSI, etc. can be very onerous. One of the ways to remedy this is to not come into contact with SSI at all.

At DEN, we have determined that the most likely occurrence of contact with SSI during a tenant-funded design and construction project would be if the project required changes in or additions to the access control system. In response to this determination, we have taken steps to meet the needs of the tenant and his designer and subsequently his construction contractor. Here are the procedures that we will follow:

- The tenant project manager will inform the DEN PM that there is a need to touch the access control system for the specific project;
- DEN PM will schedule a Pre-Design Meeting to include the DEN PM, tenant project manager, tenant project designer, DEN Security Office representative, DEN Access Control Team representative;
- If all parties to the meeting agree, the DEN PM will transmit stock base drawings/schedules for the impacted systems to the tenant project designer. These drawing files will not be SSI as they have had removed all SSI information. The content of the drawings will be generic items of general and electrical construction, items that will be required to be installed by the tenant's general contractor and his electrical subcontractor.
- These drawing files can be inserted into the project drawing files without causing the project drawing file to be considered SSI;
- At the same time, a similar procedure will occur with the project specifications – the DEN PM will transmit a specification for the subject hardware and systems that has had all SSI removed.
- These specification sections can be inserted into the project specification without causing the project specification to be considered SSI;
- The resulting drawings and specifications can be published to the contracting community without concern that the information is SSI and must be controlled per CFR49, Part 1520.

With the above information, the tenant project designer will design the layout of the access system and its major components (doors, frames, and all electrical power required by the system).

During construction, the tenant project building contractor will construct/install exactly the items shown in the drawing files and called out in the specifications, exactly for type, quantity, quality, cable/conductor size, position,

location, electrical service, etc. The components of the constructed system will include:

- Raceways and junction boxes;
- Cables and conductors;
- All doors, frames and hardware;
- All electrical power needs as it relates to the Access Control System.

The DEN Access Control Team (ACT) will inspect the construction/installation and will require modifications/corrections where the installation does not meet the requirements of the drawings/specifications. When the installation meets all DEN requirements, the construction/installation will be accepted and DEN ACT will begin its installation and commissioning process to provide the tenant a fully functioning system at the end of the project.

As you can surmise, this procedure saves the tenant and his contractor the need to deal with all the requirements of SSI control, making the project more efficient and saving costs. In addition to the control of SSI, the tenant project contractor is relieved of the need to apply for and secure an Access Control System Permit No. 3B from the City and County of Denver Office of Development Services (Building Department).

Project Limitations

The process detailed above will suffice for 99% of the projects undertaken by a tenant that impact Access Control at DEN. The typical small projects will include one or two main items of Access Control equipment with the accompanying infrastructure. At the present time, the costs incurred by DEN Life Safety for executing these projects will be borne by DEN. There is the possibility, however, that a tenant will require a larger scope of work and the impact on the Access Control System will be greater. This will be determined early in the process if the tenant PM will communicate fully with the DEN PM and will agree to attend a Pre-Design Meeting.

If the impact on the Access Control System is greater than described above, DEN Life Safety will contract with a trusted contractor to shoulder the responsibility for the system design, installation and commissioning process. The costs of this contracting process will be reimbursed to DEN by the tenant. Negotiations will commence with the DEN Property Office, Commercial and/or Finance shortly after the Pre-Design Meeting to determine the best method to execute the reimbursement.

If SSI is required by the Tenant Project Team, or if the Team inadvertently receives any SSI

Even with the procedures implemented as described above, there may be times during projects where the distribution of SSI must occur. The following is a description of SSI Requirements and a Best Practices Guide that should be implemented amongst the entire Project Team.

SSI Requirements

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

- Lock Up All SSI: stove SSI in a secure container such as a locked file cabinet or drawer (as defined by Federal regulation 49 CFR Part 1520.9 (a)(1));
- 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 CFR part 1520.19);

- 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 (as defined by Federal regulation 49 CFR Part 1520.13).
 - o Header: **“SENSITIVE SECURITY INFORMATION”**
 - o Footer: **“WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 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 US Government agencies, public disclosure is governed by 5 USC 552 and 49 CFR Parts 15 and 1520.”**

Best Practices Guide (practical recommendations to meet the spirit of the Federal regulation)

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 presentation (e.g. PowerPoint) should be marked with the SSI header on all pages and 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 reconstruction.

Attachments:

- Policy 10003 – Protection of Sensitive Security Information (SSI)



PROTECTION OF SENSITIVE SECURITY INFORMATION (SSI)

No. 10003
Series: 10000 – Airport Operations
Issue Date: 03/30/05
Revision Date: 05/12/11; 08/01/15

PURPOSE:

To establish a process for the documentation, use, and recovery of Sensitive Security Information (SSI) of a specific origin.

APPLICABILITY:

For departments handling documents or materials containing SSI information.

RESPONSIBILITY:

The Code of Federal Regulations (CFR) 49 Part 1520 and Part 15 describes the handling and protection of SSI and, among other things, the release of information that the Transportation Security Administration (TSA) has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack. SSI disclosure is limited to persons or entities under criteria identified in federal regulations, subject to a strict “need-to-know” standard, and as otherwise determined by TSA or the Department of Homeland Security (DHS).

Relevant to this policy, one category of SSI is information that describes airport programs or designs, which could be misused for purposes detrimental to the airport.

In addition to other City and Denver International Airport (DEN) policies regarding the release of information, this policy must be adhered to for the release and security of any SSI information in its custody; unauthorized access or loss of SSI information are violations of federal law and regulations.

POLICY:

This policy is intended to assure control of SSI records in accordance with 49 CFR Part 1520 and Part 15.

Authorized DEN staff have a duty to protect SSI and steps are necessary to safeguard SSI. When SSI is not in an authorized person’s possession, SSI must be stored in a secure container, such as a locked desk, locked file cabinet or locked room.

If there is an indication, or it is believed that SSI records have been tampered with, the on duty Airport Security Coordinator must be notified.

- **Companies under contract:** Prior to receiving SSI, these companies must sign the Confidentiality and Non-Disclosure Agreement, attached, stating that SSI will be guarded from unauthorized persons, that materials will be controlled while in use and secured when

not in use, and that all SSI plans and materials will be returned to the DEN project manager or destroyed following the completion of the project.

- *Note: Companies that receive Notice to Proceed (NTP) must contact Airport Security to be established as a Participant in the Airport Security Program if the work is being conducted within the Sterile Area, Secured Area and/or within a Controlled Area. All individuals working at the airport must comply with the Denver Municipal Airport Systems Rules and Regulations. If a company receiving NTP does not follow the aforementioned process, the contract will be suspended until the process is complete. Any charges incurred during the delay are at the contractor's expense.*
- Contractors are to control the access to, handling of, and recollection of SSI disseminated to any and all Subcontractors. The SSI Return or Destruction Compliance Form, attached, provides direction for the handling of, and accounting for SSI.
- **Companies not selected during the bidding process:** Prior to receiving SSI, these companies must sign the Confidentiality and Non-Disclosure Agreement, attached, stating that SSI will be guarded from unauthorized persons, that SSI materials will be controlled while in use and secured when not in use, and that all SSI plans and materials will be returned to the airport, or destroyed, immediately following the announcement of bid results.
 - The Confidentiality and Non-Disclosure Agreement form is available online and can be filled out prior to the pre-bid meeting.
- **Project Managers:** Must keep the Project Manager Control List of SSI Released and Recovered Documents, attached, of all SSI material released during a project, with company information as well as release and recovery dates of the SSI. This record will act as a ledger from which to track SSI material. It may be determined that the content of selected SSI is of such a sensitive nature that the use of said documents must be restricted to the airport premises.
- **Companies who have done business with Denver International Airport:** These companies will be sent both Confidentiality and Non-Disclosure Agreement and Request for Disclosure forms, attached. A description of SSI materials held by these companies must now be kept, as it is not feasible to request that all old records be returned. SSI holders have the option of destroying those records or marking them in accordance with Parts 1520 and 15. Protection policies must be adhered to by companies known to be SSI holders.
- **SSI materials must be clearly labeled with the following markings:**
 - **Top of document (header):**
 - **SENSITIVE SECURITY INFORMATION**
 - **Bottom of document (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 U.S.C. 552 and 49 CFR parts 15 and 1520.

- This policy is meant to create a system of accountability for records that are now considered SSI which have not been returned to DEN by the companies to which they were distributed. This will ensure that the appropriate storage and/or disposal practices of SSI are adhered to, under the control of the City, in accordance with directives by the TSA.



PROJECT MANAGER CONTROL LIST OF SSI RELEASE AND RECOVERY

Project _____

Project Manager _____

Company	Material	Release Date	Recovery Date

This document is the property of the Department of Aviation and is to be used only for the purposes intended. It is not to be distributed outside the Department of Aviation.



REQUEST FOR DISCLOSURE

The City and County of Denver, and Denver International Airport is requesting that you, as a current or former contractor provide a list of all Sensitive Security Information (SSI) records you possess.

SSI is defined as information that describes airport programs or designs, for example, which could be misused for purposes detrimental to the safety of passengers. SSI disclosure is limited by a strict "need-to-know" basis as determined by TSA.

These records could be in the form of any writing, drawing, map, tape, film, photograph, or other means by which information is preserved, irrespective of format.

Section 1520.9 (1) specifies that persons who receive SSI must protect it from disclosure. Therefore, it is the responsibility of these persons to ensure that the information entrusted to them remains secure and confidential. This includes the availability and accessibility of the information.

Company:

Please list SSI items or documents below, use additional pages if necessary:

SSI materials must be clearly labeled with the following warnings per Federal Regulations:

- **Top of document:**
 - **SENSITIVE SECURITY INFORMATION**
- **Bottom of document:**
 - **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 U.S.C. 552 and 49 CFR parts 15 and 1520.**



CONFIDENTIALITY AND NON-DISCOLOSURE AGREEMENT

1. I, _____, am an employee of _____
("Contractor").
2. Contractor, under contract (the "Contract") with Denver International Airport, is executing the acceptance of its responsibilities for Airport Security at Denver International Airport (referred to herein as the "City").
3. Pursuant to the Contractor's work for the City under the Contract, the Contractor has and will request that the City provide it with various documents or other records (collectively, "documents").
4. I understand the following with respect to any documents, or information therein, that are provided by the City to me, or which come into my possession pursuant to the Contractor's work for the City:
 - a. These documents may be considered Sensitive Security Information ("SSI") under applicable federal regulations:
 - b. These documents may be protected from disclosure under the Colorado Open Records Act;
 - c. These documents may be protected from disclosure under the federal Freedom of Information Act.
 - d. These documents are considered by the City to contain information that is vital to the security and safe operation of Denver International Airport, whether or not these documents are otherwise classified by any other entity or law as containing such information.
 - e. These documents are considered by the City to possibly contain information that is commercially or financially sensitive or which is a trade secret.
5. I agree to the following with respect to any documents, or information therein, that are provided by the City to me, or which come into my possession pursuant to the Contractor's work for the City:
 - a. I will safeguard these documents, and the information therein, to prevent inadvertent disclosure of them by keeping the documents under the control of authorized persons, when in use, and storing the documents in a secure container, such as a locked desk, file cabinet, or locked room , when not in use;
 - b. I will not release these documents, or the information therein, to any party, company, person, organization or entity for any reason that does not expressly serve the Contractor's obligations to the City under its contract with the City, as determined by the Contractor's employee with appropriate supervisory and decision-making authority;

STANDARD POLICIES AND PROCEDURES

- c. I will not release these documents, or the information therein, pursuant to the request under the Colorado Open Records Act or the Freedom of Information Act without affording the City the opportunities under those laws to protect these documents from disclosure;
 - d. I will notify the City if a request is made for these documents, or the information therein; and
 - e. I shall return, or destroy, these documents following the completion of the agreed upon contract, or following the bidding process, if not selected as the Contractor; and
 - f. Specifically with regards to SSI,
 - 1. I shall comply with the broadest possible interpretation of the federal regulations in handling SSI (49 CFR § 15 and 1520, as amended);
 - 2. I shall provide the Airport with an SSI Return or Destruction Compliance Form, listing all SSI material that I have destroyed.
6. I further understand that the City may seek appropriate legal remedies for any violation of my agreements here.

By my signature below, I hereby affirm and agree to the matters set forth above.

Witnessed,

Printed Name

Printed Name

Signature Date

Signature Date

Title

Title

Company

Manager/Project Manager,
City and County of Denver,
Denver International Airport



SSI RETURN OR DESTRUCTION COMPLIANCE FORM

Destruction (or return) of SSI must be done in a timely manner. Companies under contract must return or destroy all SSI material following the completion of the project. Companies not selected during the bidding process must return or destroy all SSI material immediately following the announcement of bid results.

The intent of this policy, addressed within the Confidentiality and Non-Disclosure Agreement form, is to follow all Federal Regulations with respect to SSI records.

Company:

SSI Items List Destroyed	Date Returned / Destroyed	Method Used If (Shred, Incinerate, Etc.)
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

By my signature below, I hereby affirm and agree to the matters set forth above.

Print Name

Signature

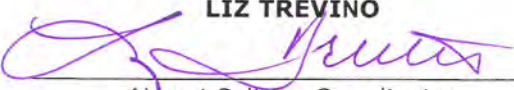

Date

Title

2013-01-01 10:00 AM

**DENVER INTERNATIONAL AIRPORT
POLICY & PROCEDURE
RECOMMENDED AND APPROVED**

Policy Description: 10003 - Protection of Sensitive Security Information (SSI)

<p> LIZ TREVIÑO _____ Airport Policies Coordinator</p>	<p> DAVID LAPORTE _____ Senior Vice-President Airport Operations</p>
--	---

This document is the property of the Department of Aviation. It is to be used only for the purposes for which it was prepared. It is not to be distributed outside the Department of Aviation.