SAFE SKIES

PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0008

February 2017

Findings and Practices in Sharing Sensitive Information

Synthesis Report

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Stephen Lehocky
Gloria Bender
Jessica Gafford
TransSolutions, LLC
Fort Worth, TX

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the Program for Applied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0008 PROJECT PANEL

Daniel Elroi *NorthSouth GIS*
Dr. Xiaogong Lee *Federal Aviation Administration*
Dawn Lucini *Telos ID*
Bill Marrison *McGhee Tyson Airport*
Susan Prediger *SP Consulting, LLC*
Lorena de Rodriguez *SSi, Inc*
Clint Welch *San Diego International Airport*

AUTHOR ACKNOWLEDGMENTS

The research conducted for this report was performed under PARAS 0008 Synthesis: Practices for Sharing Sensitive Information and Systems by TransSolutions, LLC.

Stephen Lehocky was the Principal Investigator for the project and primary author of the report. Gloria Bender provided review and advice. Prasanna Kavaipatti and Nadia Martinez assisted with the research and data collection. Jessica Gafford provided assistance with organizing, presenting, and editing the report and its many drafts.

The authors would like to express their gratitude to the members of the project panel for their support and insightful comments throughout this research project. The authors would also like to thank the many airports that participated in the research for sharing their data, insight, and time. Their experiences with efforts to improve the aviation industry and willingness to share those experiences enrich this report.

CONTENTS

LIST OF TABLES & FIGURES

SUMMARY

All airports generate important information that could be considered privileged but is not covered by federal designations such as Top Secret, Classified, and SSI. Airports must occasionally grant access to this non-regulated, privileged information to non-credentialed persons who have a need-to-know for work on airport projects, as part of the procurement process or for public information purposes. Such access is typically granted on an as-needed basis and limited to what is required to perform the work. Even if this information is subject to federal and state transparency laws, it is in the airport's best interest to have processes in place to create, access, control, store, share, track, and properly destroy the privileged information.

The objective of this synthesis project was to create a single, consolidated source of information on successful practices to share privileged information not classified by the federal government for use at US airports of all types and sizes. This synthesis report provides the findings and practices on effective ways that airports administer access, as well as control and recover information after it is no longer needed.

The life cycle of privileged materials can be categorized into six activities:

1. Identifying privileged materials
2. Accessing and controlling privileged materials
3. Storing and sharing privileged materials
4. Tracking privileged materials
5. Destroying privileged materials
6. Training and policies on managing privileged materials

At the beginning of this project, the Program for Applied Research in Airport Security (PARAS) panel and the research team expected the airports interviewed would provide a comprehensive and robust list of documents that they consider privileged, but are not classified under federal regulations. We also expected to find many examples of practices performed at airports to protect this information.

It quickly became apparent that not only did airports lack any formal or informal policies to handle this type of information, most of the airports could not provide the research team with examples of information that was privileged but was not already protected under a federal regulation or law. Many airports indicated that non-regulated, privileged information is considered public information due to open government laws and is not protected in any significant manner. For airports that are owned and operated by local and state governments, these transparency laws require airport leadership to disclose information and materials they might otherwise choose to control for operational, financial, or legal reasons.

However, the literature review provided several examples of information that could—and for some industries, should—be considered privileged enough to protect. This research showed that written and documented policies, coupled with formal training for employees, is the most effective way to prevent information breaches that may lead to operational, financial, or legal consequences or controversies. It also creates an environment in which employees feel empowered to deny access to privileged information to persons that do not have a need to know.

The research also showed that few airports perform special vetting or additional background checks on their employees that create, handle, and manage this privileged information. For most airports interviewed, the initial pre-employment background check is all that is needed to perform tasks that require access to privileged information. Other airports may require a Secure Identification Display Area badge as a minimum for all employees, regardless of position or responsibilities.

WHY IT MATTERS

Information that is not designated as sensitive by federal regulations should still be controlled and protected.

For example, when requesting proposals for a service at the airport, such as burying and relaying fiber optic cables, an airport will need to release drawings, maps, and specifications with the request for proposal (RFP) to obtain an accurate quote for services. By providing these drawings, maps, and specifications to any bidder, an airport may be providing persons that do not have a need to know with the information needed to completely cut off cloud-based services, voice over internet protocol services, and other connections to outside services. This could result in operational, legal, and financial risks and repercussions.

Some airports have found ways to circumvent these potential risks. In the fiber optics RFP example, an airport may require potential vendors to view and take notes on the maps and drawings in a supervised room of the airport. Because the map images are required to stay at the airport, the threat of an information breach is greatly reduced.

It is the airport leaders’ responsibility to determine what information warrants control to protect operational performance, legal risk, and financial consequences to the enterprise. This will be different for each airport based on its governance, financial situation, size, and history.

This report covers several types of regulated and non-regulated information. However, most of this report covers physical media (i.e., printed documents) and locally-stored digital media. This report does not go into detail on practices for securing and administering access to sensitive systems. For guidance on the practice of sharing access to sensitive systems, such as emergency management systems, please review the PARAS 0010 project: *Guidance for Protecting Access to Vital Systems Impacting Airport Security*.

In addition, this report only briefly touches on the subject of cybersecurity. For more guidance on cybersecurity at airports, please review the PARAS 0007 project: *Quick Guide for Airport Cybersecurity*.[1]

[1] Both PARAS 0010 and PARAS 0007 are scheduled for release in 2017.

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
ANSI	American National Standards Institute
AOA	Air Operations Area
ARFF	Aircraft Rescue and Firefighting
CCTV	Closed Circuit Television
CDC	Centers for Disease Control and Prevention
CD/DVD	Compact Disc/Digital Video Disc
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
ID	Identification
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
R&D	Research and Development
ROI	Return on Investment
SIDA	Security Identification Display Area

SOP	Standard Operating Procedure
SSI	Sensitive Security Information
SSN	Social Security Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Transportation Security Administration
XML	Extensible Markup Language

SECTION 1: INTRODUCTION

The objective of this report was to create a single, consolidated source of information on successful practices in sharing sensitive information not classified by the federal government at US airports of all types and sizes.

Initially, the Program for Applied Research in Airport Security (PARAS) panel and the research team expected to identify a comprehensive and robust list of documents that airports consider to be privileged, but not federally regulated. In addition, we expected a diverse list of practices airports perform to protect this information.

After the first few interviews, it became apparent that not only did airports lack any formal or informal policies to handle this type of information, most of the airports could not provide us with examples of privileged information at their facilities. However, the literature review provided several examples of materials that could be considered privileged enough to protect.

The resulting synthesis report provides the findings and practices on effective ways to administer access, as well as control and recover information after it is no longer needed, that were identified during the literature review and interviews.

1.1 Methodology

This section describes the methodology used during the research for this project.

1.1.1 Airport Selection

The authors invited 187 airports to participate in a short interview to discuss how they manage their sensitive information. These airports represented a complete range of airport sizes using the FAA size categories: large hub, medium hub, small hub, and non-hub. Contact information was gathered from a variety of sources, including:

- Authors' previous client contacts
- Business colleagues
- Conference rosters and attendee lists
- Industry organization membership directories, such as
    - American Association of Airport Executives (AAAE)
    - Airports Council International – North America (ACI-NA)

Of the 187 airports contacted, 20 replied to the invitation and participated in interviews with the authors. Figure 1-1 shows the percentage of airports that responded by their FAA size designation. Figure 1-2 shows the geographical distribution of the airports interviewed and color-codes the airports' governing body types. To protect the identity of the airports interviewed, names of airports or their governing body has been omitted.

Figure 1-1. Size Distribution of Airports Interviewed

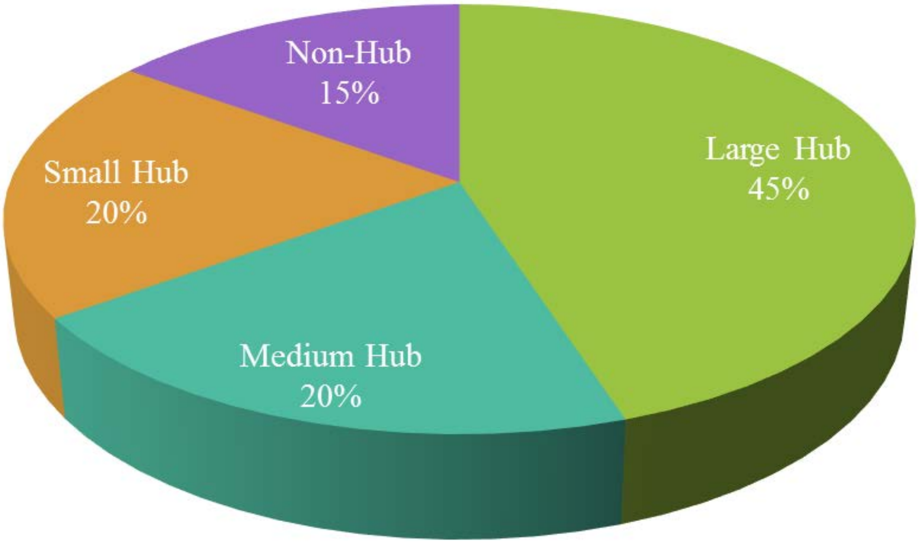
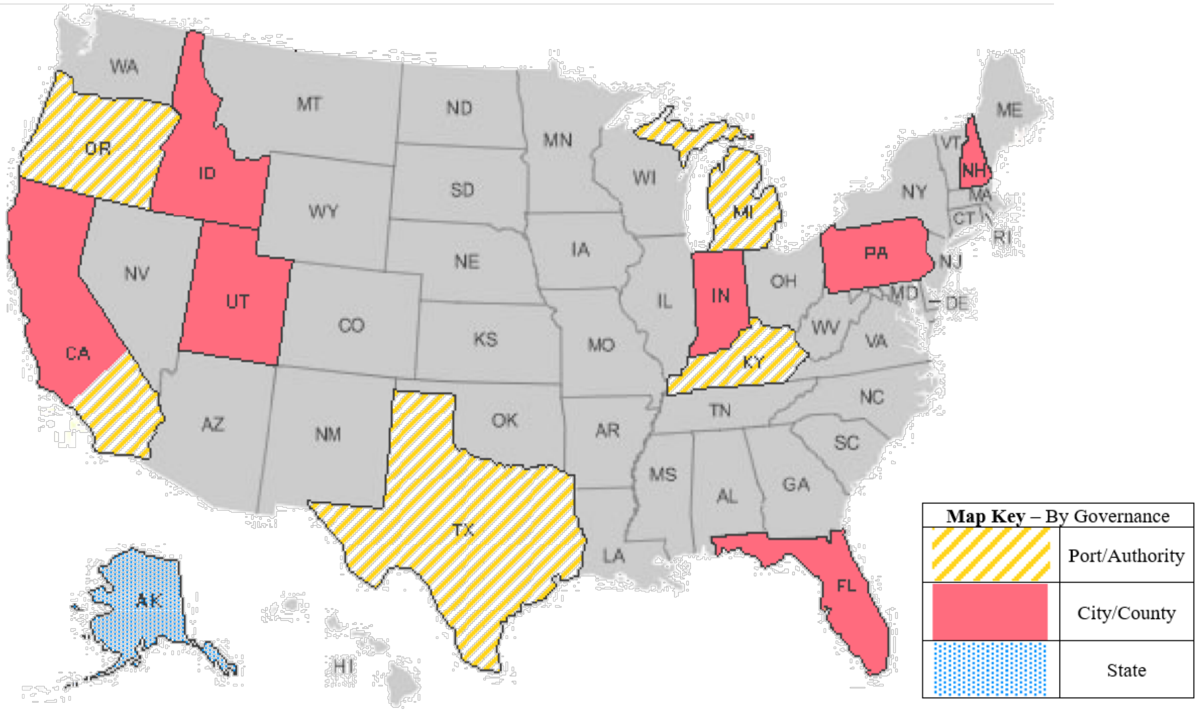


Figure 1-2. Geographical Distribution of Airports Interviewed



**Several states had more than one airport interviewed. States with multiple shadings indicate that the airports interviewed in that state had different types of governing bodies.*

The phone interviews included formal questions and open discussions designed to 1) document successful practices and processes that airports are currently using to manage and handle their privileged information, and 2) identify materials that airports consider to be sensitive. The interview questions are attached as Appendix A.

1.1.2 Literature Review

The authors conducted a literature review to document practices that have been shown to work successfully in non-aviation industries and international organizations. The authors utilized published ACRP reports and guidebooks; university search engines; public search engines; AAAE and ACI-NA published material; and Office of Personnel Management (OPM), Congressional Budget Office (CBO), and Government Accountability Office (GAO) published material to conduct the literature review. The authors also reviewed reports from relevant agencies, including the Office of Inspector General (OIG), DOT, DHS, and TSA. The research strategy sought pertinent information on practices in non-aviation industries and international organizations.

The literature review revealed that there is little information related to the handling and managing of privileged material that is not federally designated or classified. Examples of designations pertinent to airports include SSI, Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), Protected Critical Infrastructure Information (PCII), and other federally regulated and classified statuses.

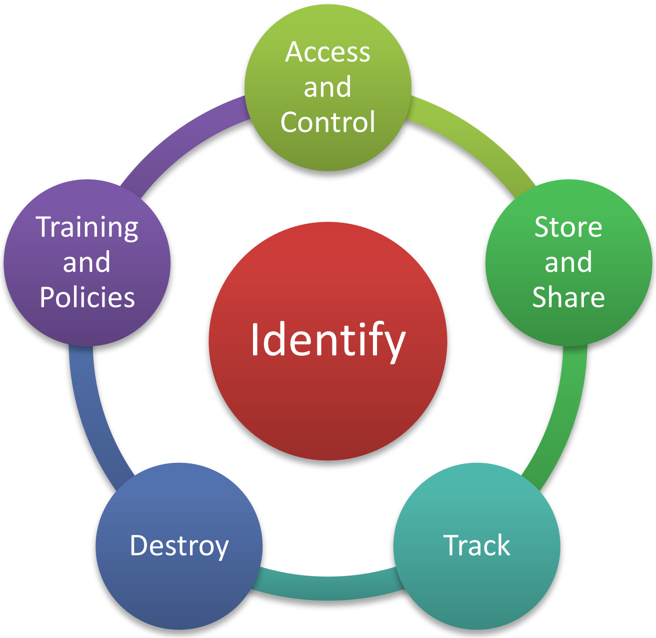
However, the literature review uncovered multiple policies and methods non-aviation industries and international organizations utilize to access, control, store, share, track, destroy, and train their employees for their variously classified and sensitive materials and information, including methods for handling SSI, SBU, PII, PCII, and other classified categories.

A more in-depth discussion on the difference between federally classified/designated material and privileged material can be found in Section 2.1: Identifying Privileged Materials.

1.1.3 Data Analysis

The data obtained during the literature review and interviews indicated elements that were common and/or essential to handling privileged information. The authors documented the results of the interviews and literature review by classifying the features into the six identified activities required for controlling privileged information, presented in Figure 1-3.

Figure 1-3. Six Critical Activities Required to Control Privileged Information



SECTION 2: FINDINGS

2.1 Identifying Privileged Materials

During the interviews, airports were asked to identify or describe information or materials considered privileged, but not classified or designated by federal or state regulations and laws. Most airports indicated that they do not consider any information sensitive or privileged enough to closely protect. In part, this appears to be due to state open government laws (also known as sunshine laws) requiring transparency and access to information controlled by the airport. Because documents that are not classified or regulated could be considered open to the public from a legal standpoint, many airports treat non-regulated documents and information as if they have already been presented to the public and freely share their information when requested.

However, two airports indicated that they treat all information—regardless of federal designation or sensitivity—as if it were SSI. While these two airports follow their open government laws when a request is submitted, documents and information in the interim are stored, shared, and destroyed in accordance with 49 CFR § 1520 regulations, which can be found in full at the Electronic Code of Federal Regulations website.

In general, airports do not have levels or hierarchies of privileged information. It is either protected by some federal or state regulation or it is not protected and is available through state Freedom of Information Act (FOIA) requests.

> The Freedom of Information Act (FOIA) of 1967 (5 U.S.C. Part 552) is one of the federal laws that allow for full or partial disclosure of information and documents controlled by the US Federal Government. FOIA grants the public the right to request and access certain records from federal agencies.

A compilation of documents and information considered as privileged by the interviewed airports includes:

- *Company/organization SOPs and policies
- *Intellectual property, including document names/titles (also known as proprietary information or trade secrets)
- ‡Closed-circuit television (CCTV) footage
- Procurement information, including working notes for
    - Request for proposal/request for information (RFPs/RFIs), including in-progress bid documents
    - *Contracts, including airline strategies
        - Landlord information, including company names and/or tenant information, budgets, and plans
- *Construction drawings/layouts and video, especially those showing
    - HVAC and utilities (electric and gas)
    - Security sensitive areas that do not fall under 49 CFR § 1520 and critical infrastructure laws
    - Fuel lines
    - ‡IT infrastructure
    - Operations
    - Hardware, such as doors and locks

- *Training documents (videos and physical materials)
- *Planning documents and associated working notes, including
    - Airport Emergency Plan (AEP)
    - Active shooter plans and policies
    - Disaster recovery plans
    - Bomb/hijack/terrorist policies
    - Security reports from the Security Department
    - Airfield winter operations
- *Schedules for security/police and special event assignments
- Open records/Freedom of Information Act (FOIA) requests
- Access control history/badge swipes
- IT network information and firewall information

Documents marked with an (*) may be protected under federal trade secret/proprietary laws, such as the Economic Espionage Act of 1996.

Documents marked with an (‡) are protected at some airports by state laws and are exempt from state FOIA requests. For instance, at least one state designated CCTV footage as sensitive. It may not be released, even for a state FOIA request.

Table 2-1 compares several types of regulated materials, including the 49 CFR § 1520 regulation’s 16 classifications of SSI, high-risk data (also considered PII), and examples of proprietary information and trade secrets gathered during the literature review.

Table 2-1. SSI vs. Proprietary vs. Trade Secrets

SSI	Examples of High-Risk Data	Examples of Proprietary Information and Trade Secrets	
• Security programs and contingency plans • Security directives • Information circulars • Performance specifications • Vulnerability assessments • Security inspection or investigative information • Threat information • Security measures • Security screening information • Security training materials • Identifying information of certain transportation security personnel • Critical aviation, maritime, or rail infrastructure asset information • Systems security information • Confidential business information • Research and development • Other information that TSA determines is SSI	• Name and initials in any combination • Home address or telephone numbers • Email address • Date of birth or age • Gender • Marital status • Nationality • Sexual orientation • Racial or ethnic origin • Religious beliefs • Social security number • State-issued or any other government-issued identification number • Mother's maiden name • Driver's license number or similar operating license information • Passport number • Credit and criminal history • Credit, ATM, and debit card numbers • Bank account numbers • Financial account numbers • Payment card information, such as expiration dates, PINs, magnetic strip data, and CVVs • Security codes, access codes, and passwords • Physical and psychological health status and history • Disease status and history • Medical treatment history • Diagnoses by healthcare professionals • Prescription information • Health insurance information and account number • Insurance claim history • Salary • Services fees • Other compensation information • Background check information	• Financial information • Supplier information • Vendor information • Customer information • Sales figures • Business plans and projections • Profit and performance reports • Software or technologies • Research • Artwork • Advertising schedules • Growth strategies • Customer lists • Product and service information • Vendor products being developed before vendor has authorized disclosure • Vendor goods and services pricing • Intellectual property • Techniques and methods of operation	• Business methods • Business plans • Business forecasts • Market analyses • Marketing plans • R&D information • Business relationships • Product information • Pricing information • Financial information • Profit margin information • Overhead information • Cost information • Purchasing information • Office techniques and systems • Manuals and standard operating procedures • Computer databases • Designs, drawings, blueprints, and maps • Machine processes

Table 2-2 compares the types of information and the regulations and laws that protect them. Information marked "Privileged" were specifically identified during the airport interviews. This table indicates that there may be some confusion among airport employees regarding what is regulated and non-regulated privileged information.

Table 2-2. Comparison of Types of Information and Their Protected States

Type of Information	SSI (49 CFR 1520)	PII (Privacy Act of 1974)	Trade Secrets / Proprietary (Economic Espionage Act of 1996)	Privileged (State/Airport Specific)
Security programs and contingency plans	▨		▨	▨
Security Directives	▨			
Information circulars	▨			
Performance specifications	▨		▨	
Vulnerability assessments	▨			
Inspection or investigation information	▨			
Threat information	▨			
Security measures	▨		▨	▨
Security screening information	▨		▨	▨
Training materials	▨		▨	▨
Personnel information	▨	▨		
Critical infrastructure asset information	▨			
Systems information	▨		▨	
Confidential business information	▨		▨	
Research and development	▨		▨	
Financial information		▨	▨	▨
Supplier/vendor information			▨	▨
Customer information		▨	▨	▨
Software or technologies			▨	
Designs, drawings, blueprints, and maps			▨	▨
Schedules			▨	▨
Business strategies			▨	
Product/pricing information			▨	▨
Databases			▨	▨
Information technology specifications			▨	▨
Procurement information			▨	▨

Each of these categories of regulated (SSI, PII, trade secrets/proprietary) and privileged information are especially important to different departments at the airport or governing body.

SSI is most often used by the Legal, Operations, and Security/Risk Management departments. Other departments and sub-departments, such as Procurement and Facilitates Maintenance, may occasionally use or create SSI material.

PII is most important to the Legal and Human Resources departments. Because this type of material is almost exclusively limited to personnel information, only the departments that are responsible for employment issues should have access to PII.

Trade Secrets and Proprietary information often passes through the Legal, Operations, and Marketing departments. Occasionally other departments and sub-departments, such as Procurement and Facilities Maintenance, may use or create information considered a trade secret or proprietary. More information on this topic can be found in the Glossary.

Privileged information can be created and used by every department. Once airport leadership determines what information constitutes privileged for their specific organization, then the departments that create and use that information can be trained on the required management policies and procedures.

It is the airport leadership's responsibility to determine what information warrants control to limit the airport enterprise's operational, legal, and financial consequences. Privileged information will be specific to each airport based on governance, financial resources, airport size, and past events. Airport leadership should take operational, legal, and financial implications into consideration when determining materials that need to be controlled.

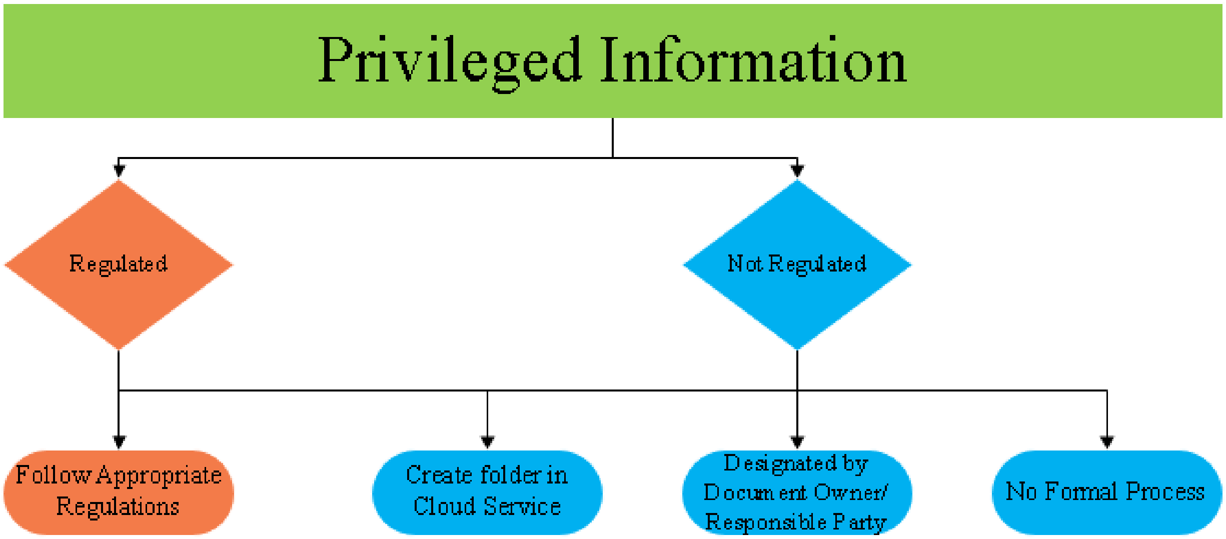
Operational Considerations	Legal Considerations	Finance Considerations
• Safety • Risk to others • Airport performance	• Negligence • Personnel issues/social justice • Civil liability	• Funding (including from government agencies) • Cost • Payroll

Airports that are governed by a port authority tend to have more policies in place for managing privileged information because their governance is more complex. This will factor into airport leadership's determination on what constitutes privileged materials.

None of the airports interviewed described a formal or written process for designating privileged information and the methods for handling that information. Only one airport had a consistent process for designating their privileged information that did not directly follow a federal regulation. For that airport, the information is considered privileged when it is uploaded to the project folder stored on an enterprise content management platform or cloud-based service. All other airports indicated that they (1) follow the federal regulations (most commonly 49 CFR § 1520), (2) allow the document to be designated privileged by the document owner/creator or its responsible party, or (3) have no formal process, as shown in Figure 2-1.

> Cloud-based services are internet-based services that provide additional storage capacity offsite (i.e., "in the cloud"). This offsite storage allows for additional protections and easier means of sharing, but the information still remains the responsibility of the airport or material creator.[2]

Figure 2-1. How Information is Designated Privileged

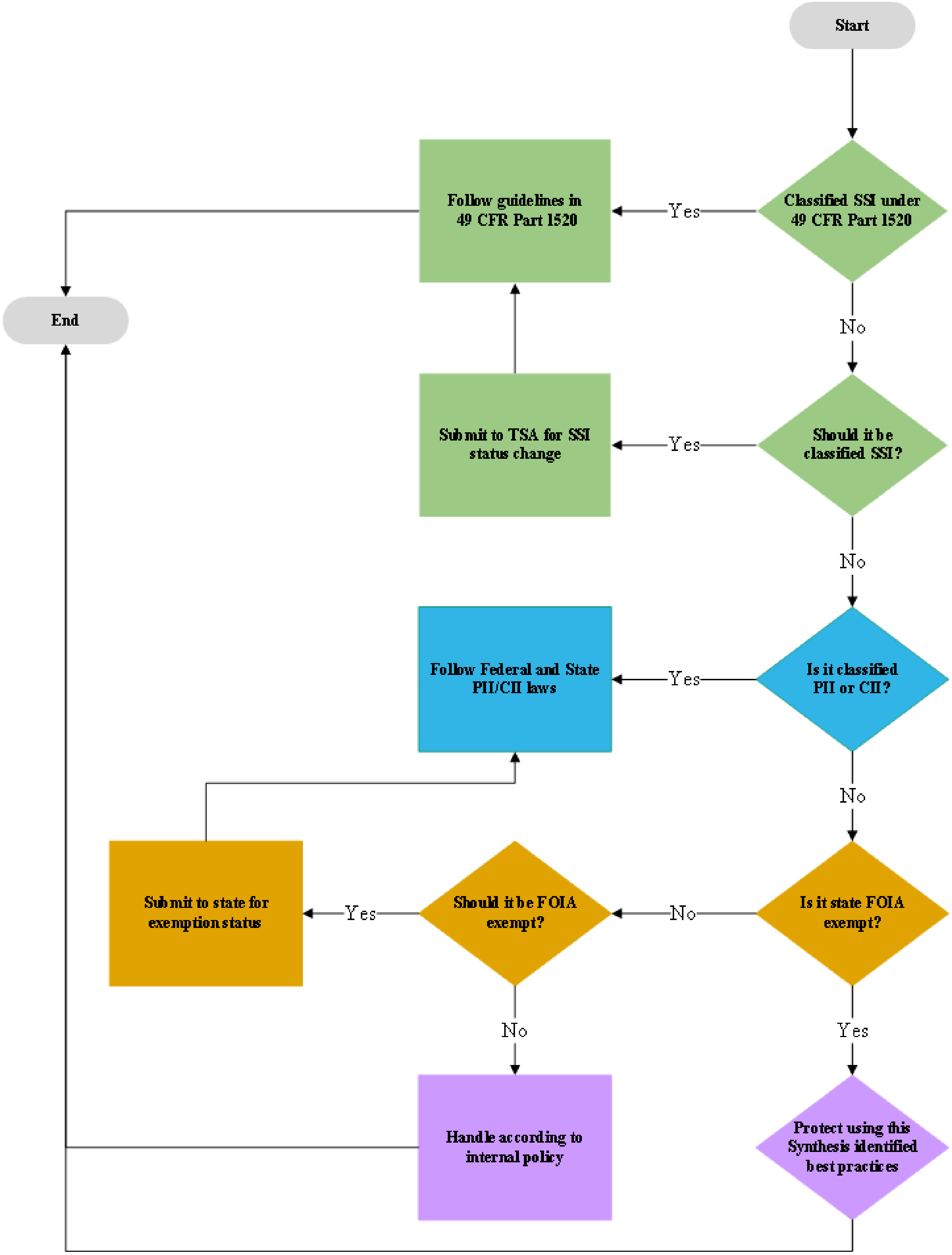

Privileged Information
Regulated
Not Regulated
Follow Appropriate Regulations
Create folder in Cloud Service
Designated by Document Owner/ Responsible Party
No Formal Process

Several airports indicated that their non-privileged and privileged information routinely overlaps, especially during the "working" or drafting phases and some of the procurement phases.

The flow chart, identified in the literature review and presented below in Figure 2-2, shows how airports might determine when privileged information falls under a federal or state regulation, and when to use best practices identified during this project's research.

[2] Additional protections may include services such as access to software, storage, computing power, IT infrastructure (e.g., servers and hard drives), redundant backups, disaster recovery protection, a higher level of facility security measures (e.g., badges, card readers, and/or biometric readers), multifactor authentications to access the data, and advanced firewall protection solutions.

Figure 2-2. Privileged Information Flow Chart


Start
Classified SSI under 49 CFR Part 1520
Yes
Follow guidelines in 49 CFR Part 1520
End
No
Should it be classified SSI?
Yes
Submit to TSA for SSI status change
No
Is it classified PII or CII?
Yes
Follow Federal and State PII/CII laws
No
Is it state FOIA exempt?
No
Should it be FOIA exempt?
Yes
Submit to state for exemption status
No
Handle according to internal policy
Yes
Protect using this Synthesis identified best practices

2.2 Accessing and Controlling Privileged Materials

2.2.1 Accessing

When determining access privileges and need-to-know, most airports have no formal process or procedure. Most airports determine need-to-know based on an employee's position/title or job duties. Some airports follow the instructions of the document's creator or responsible party to determine who has a need to know. At least two airports require employees who feel they have a need to know to complete a specific form or submit a written request to access the information.

All of the organizations and agencies identified during the literature review agree that only persons with need to know should be permitted to view or handle sensitive materials, including physical and intellectual properties, supplies, consumables, and equipment.

Some groups, such as the National Archives and Records Administration (NARA), require individuals to be escorted by NARA personnel or be under video surveillance when viewing privileged materials. In addition, that individual may not be left alone with the information and may not possess any device capable of photographing, recording, or transferring images or content.

Access to the privileged materials ranges from the informal to the highly secure. Current airport processes identified include:

- Informal request (asking as a coworker)
- Document request from the document owner or the division/department head
- Use of individual and unique passwords for each employee for network access
  - Access may be based on position/title or job duties
- Access to physical documents based on position/title or job duties
  - Includes access to long-term storage containers
- Access granted only during office hours
- Access granted/monitored by a gatekeeper

One airport shared a recent experience they had during a routine procurement process. The RFP necessitated the sharing of terminal drawings for bidders to give accurate estimates in their bidding proposals. During this particular circumstance, the security department reviewed the terminal drawings prior to them being included with the RFP. The head of the department noted that the drawings showed several markings relating to HVAC system access rooms and panels. While the drawings and the HVAC systems are not considered SSI by the TSA or the airport, the security department did not feel comfortable releasing the drawings to the public for safety reasons, but the drawings were necessary for the procurement process.

The security department compromised with the procurement department; the drawings would not be sent out with the RFP. Instead, potential bidders would be required to visit the airport security office to view and make notes of the drawings in a controlled environment under a security officer's supervision.

In addition, the airport decided to prevent similar, potential security issues in the future by creating a review board consisting of the heads of several departments and developing written formalized policies and procedures for their airport.

For more secure processes, such as access to specific folders or file cabinets, access privileges are determined by an authorizing agent. Airports, agencies, and organizations indicated the following people are authorized to grant access privileges for physical and/or electronic material:

- Manager level or higher, including senior staff, director, and division/department head
- Project liaison or project coordinator
- Material owner or client/consultant providing the material
- IT working group of department heads
- Security chief

Most organizations specify that sensitive digital information must be stored on network folders that require a password to access, or have limited access by personnel. Nearly all organizations and agencies follow this as an IT best practice.

With remote control software and mobile applications becoming more widely used, the threat of a cybersecurity breach is genuine. Policies that address the use of remote control software and applications may provide protection against theft, loss, malware, and unsafe software and applications on organization-issued IT hardware.

2.2.2 Controlling

After airport leadership identifies what information warrants protection, the level of control necessary for each type of document should be determined. Control is a spectrum, and where individual airports fall into that spectrum is determined by the airport's governance, financial resources, size, and past events.

While loosely controlling privileged and regulated material could lead to operational, legal, and financial consequences (e.g., releasing information that compromises personnel), rigid or over-control of material could also result in operational, legal, and financial repercussions.

There are many categories of protected information. Table 2-3 attempts to provide a basic review of information and markings protected by federal, state, and international laws. The table lists the main categories of protected information that are discussed or mentioned in this report.

Table 2-3. Classifications and Associated Markings

Classification	Document Control Marking(s)	Associated Law
SSI*	• SSI cover letter* and footer*	49 CFR 1520
PII*	• "For Official Use Only (FOUO) – Privacy Sensitive"* • Attorney-client privilege header‡	Privacy Act of 1974
Proprietary/Trade Secrets *‡	• Non-disclosure agreements (NDAs)‡ and contracts‡ • Copyright bug (©)* • Trademark bug (™)* • Registered trademark bug (®)* • "Confidential"‡ • Attorney-client privilege header‡ • "Limited Use Only"‡	Economic Espionage Act of 1996, Patent Act, dozens of state and international laws

Classification	Document Control Marking(s)	Associated Law
SBU*	• "For Official Use Only (FOUO) – Privacy Sensitive"*	Department of Defense Directive 5400.7
PCII*	• PCII Identification number* • PCII footer*	Critical Infrastructure Act of 2002
Privileged‡	• "Law Enforcement Sensitive" (LES)‡ • "Internal Use Only"‡ • Non-disclosure agreements (NDAs)‡ and contracts‡ • Attorney-client privilege header‡ • "Need-to-know"‡ • "Limited Use Only"‡	N/A

Classifications and markings with a (*) are federally protected and generally recognized internationally. These designations and markings may only be used with the approval of the associated federal agency.

Classifications and markings with a (‡) are not federally classified and are not protected under federal regulations. However, some documents that fall into these categories or contain these markings are protected under various state and international laws. Use of these markings is not prohibited, but does not necessarily protect the material from FOIA requests. Consult your legal department before marking documents with these classifications and markings.

Nearly all organizations and agencies require sensitive material to be marked or watermarked in a conspicuous manner in accordance with organization or agency regulations. For example, the United States Department of Agriculture (USDA) requires marking the material with "Sensitive but Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only." Microsoft, a public organization, requires information to be marked "Confidential" or "Proprietary." DHS permits employees to only print, extract, or copy sensitive information or material when the official need is not easily met using other means, presumably via verbal communications.

Airports occasionally mark privileged material with visible markings. Usually, these are watermarks on electronic materials and stamps on physical materials.

Many of the airports in states that actively promote transparent governance expressed concerns and frustrations about not being able to mark privileged and security-sensitive information as SSI or other federally regulated classifications. Despite this, airports must be careful when marking privileged material with federal classification markers (SSI, SBU, etc.) Federal classifications and designations may not be used on materials that do not fall into the specific categories, and should be avoided as a FOIA exemption strategy. Several airports stated that the TSA mailed letters asking them to remove SSI markings from documents because they were not considered SSI per 49 CFR § 1520.

Whether the document or information is regulated or non-regulated, materials considered privileged are usually marked using watermarks, stamps, a cover page, and/or footers. These markings are typically applied to the entire document, regardless of whether individual pages contain sensitive information. This is aligned with guidelines presented by DHS in their *SSI Quick Reference Guide for Non-DHS Employees and Contractors*, presented in full in Appendix B. Both airports and federal agencies use these markings.

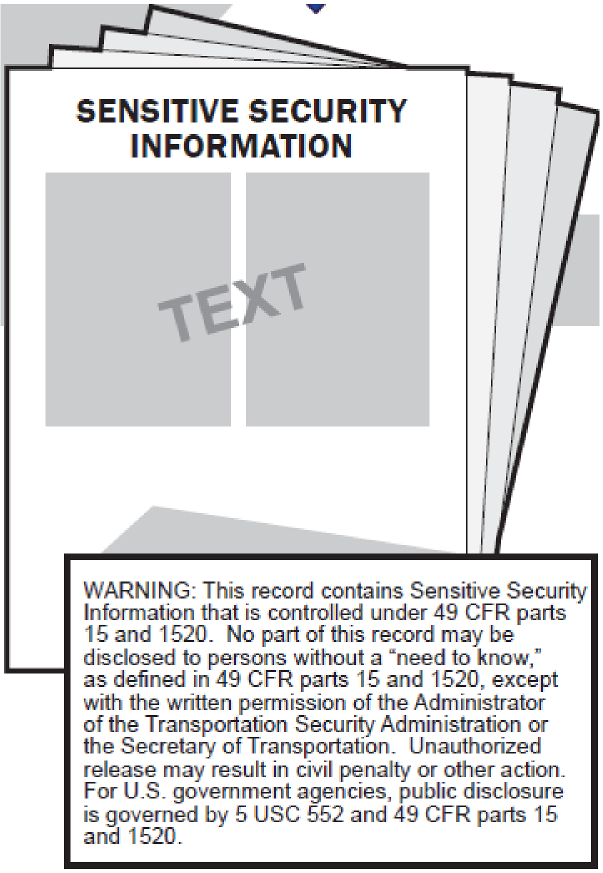
The markings and stamps typically seen at airports include:

- SSI
- LES
- FOUO
- Internal use only
- Attorney-client header
- Confidential

Often, the associated NDAs and contracts have language that covers the confidentiality of the material and the measures that must be taken to protect that confidentiality. Interestingly, the United Nations (UN) stipulates information may be considered privileged even if the documents are in draft form. The airports interviewed also consider draft or working documents to be privileged and unavailable for FOIA requests until they are completed.

TSA requires each document with SSI in it to have an SSI cover sheet, and every page of the document to be marked with the SSI header and footer, shown in Figure 2-3, even when only a small portion of the document contains SSI. This also includes electronic documents, presentations, and spreadsheets.

Figure 2-3. TSA Footer for Documents Containing SSI



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.

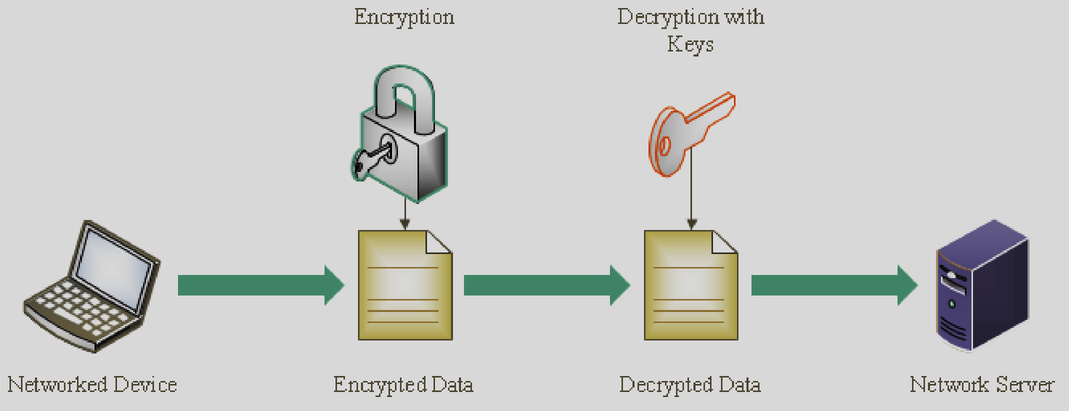
Source: TSA's Best Practice Guide for Non-DHS Employees and Contractors

It should be noted that the TSA requires that portable storage devices (CDs/DVDs, USB flash drives, portable hard drives, memory cards, and mobile devices) not be marked SSI. Instead, the TSA requires CDs/DVDs and portable storage devices to be encrypted or password protected (see Figure 2-4). For example, the Cyber Security Manual, written by the USDA, requires SBU and SSI information transmitted via any electronic media to be encrypted. Video and audio files stored on portable storage devices must have the header and footer on the cover and at the beginning and end of the program.

Figure 2-4. Encryption Process

Encryption vs. Password Protection

Encryption and password protection can be confusing.



At the macro-level, encryption involves two-steps of protection on data: encryption and decryption. It works as though you put the data through a shredder and collect all the pieces in a box and then place a lock on the box (the encryption step). If you break the lock without the key, all you would find is shredded bits of data. But, if you open the lock with the correct key, the shredded bits of data become whole again and can be read/accessed (the decryption step).

Passwords work similarly, but are obviously not as secure. It is as if you put the data into the box whole and put a lock on the box. If you have the key, you will find the data whole and in the box. But if you break the lock, you will still find the data whole in the box.

Using encryption methods/systems *may* incur significant additional cost to your airport.
In another example, GameStop, Inc., the video game and video game accessories retailer, requires personnel to maintain unique log-in credentials. Employees must never use or share a computer or account password, Personal Identification Number (PIN), or any type of access code exclusively assigned to another employee.

Nearly all the organizations and agencies reviewed require that passwords comply with the following standards to be considered secure:

- Contain at least eight (8) characters
- A mix of uppercase and lowercase letters, numbers, and special characters
- Must not be a word in the dictionary or a name

The UN requires devices (mobile phones, laptops, tablets, and workstations) to be configured with appropriate security systems, anti-virus software, password protection, and automatic timeout/lock features to restrict access. Logging out of devices helps prevent unauthorized access, especially if the device is lost or stolen. Log-on options could include fingerprint, passcode/password confirmation, or device encryption.

Christopher Hadnagy, a respected expert in the field of social engineering, states that one of the easiest ways to prevent technology breaches is to keep software updated, such as email clients and virus scanning software. All policies should be formalized and written in the organization or agency's policies and procedures to ensure compliance.

More information on cybersecurity and sharing access to sensitive systems can be found in PARAS 0007: *Quick Guide for Airport Cybersecurity* and PARAS 0010: *Guidance for Protecting Access to Vital Systems Impacting Airport Security*.

2.2.2.1 Vetting of Employees

Although the regulations only require access given to those with a need to know, some of the airports interviewed require a SIDA badge to handle privileged materials, and at least one airport has employees with Secret level clearance to handle SSI. However, most airports interviewed did not have vetting requirements for employees handling privileged information. These airports indicated that their hiring checks and processes were sufficient to handle information that is not federally regulated. This is similar to the employment suitability requirements of organizations and agencies identified during the literature review.

> "Suitability," as defined by OPM, "refers to a person's identifiable character traits and conduct sufficient to decide whether employment or continued employment would or would not protect the integrity or promote the efficiency of the service."

The different levels of suitability are consistent with the governing body's requirements, but are not the same as clearance levels. For instance, a city that owns and operates an airport may perform the standard pre-employment background check with an additional fingerprint check on all employees, regardless of which department controls the airport operations. However, for some of the airports interviewed, the aviation/airport department is located at the airport, in which case all the department employees maintain security ID media, although not necessarily a SIDA badge. Aviation/airport departments located at the city hall or other building off airport property generally do not require an airport ID badge for employees.

Several airports require SIDA badges or security ID media for all of their airport department employees, regardless of location, access requirements, job duties, or position/title. Some do not require a badge for their employees that work off-site, but do require a standard background check and a fingerprint check. Some only require the standard pre-employment background check, but may also include a warrants check. Others will check the TSA No Fly list or other watchlists.

Generally, the only additional checks performed on employees are the two-year recurrent Criminal History Records Checks (CHRCs) and Security Threat Assessments (STAs) for SIDA badge holders. SIDA badge holders are also required to self-report any disqualifying convictions under 49 CFR § 1542.209. Because airports do not have multiple levels of suitability, there are no additional checks performed based on an employee's access to a specific level of privileged material. For the airports interviewed, an employee is either authorized to handle privileged information or the employee is not authorized.

The non-aviation organizations reviewed did not mention specific background checks or vetting of their employees for their suitability to handle and manage privileged information. In the case of public organizations, such as GameStop and Microsoft, it is presumed that the standard pre-employment background and biographic check, coupled with the person's suitability for the position/title, is enough for the organization to feel confident in their employee's ability and professionalism.

Documents that must be signed before a job offer may also protect the organization to some extent. Depending on the position/title, GameStop and Microsoft employees sign an NDA-like contract that stipulates the confidentiality of documents that belong to the organization. All of the organizations and agencies reviewed specify that the duty of confidentiality continues even after a person is no longer employed by the organization or agency.

Government agencies follow similar guidance, although US federal agencies follow OPM's guidelines for suitability in addition to applicable federal regulations, such as 49 CFR §§ 1542.209 and 1544.229. International government agencies have their own regulations that are similar to OPM's suitability requirements.

For more information on the vetting and suitability of aviation workers, please see PARAS 0001: *Criminal History Records Checks (CHRCs) and Vetting of Aviation Workers Guidebook.*[3]

2.3 Storing and Sharing Privileged Materials

2.3.1 Storing

Organizations and industries, including airports, are required by federal laws to protect their regulated material in a secure container, such as a locked desk, locked file cabinet, or locked room. This not only covers documents in paper form, but also digital devices, such as removable and portable storage devices and laptops. All files, folders, and boxes should be labeled so that their content, dates, and sensitivity classification are clear. Some of the airports interviewed indicated that gatekeepers were used outside of locked storage rooms. This is usually a check-in/check-out desk with an employee stationed there during work hours.

The literature review indicated several commonsense best practices that are in alignment with federal requirements:

- Personnel must ensure information is not easily seen on computers screens or workstations
- Computers should be locked when personnel are away from their computer and/or workstations
- Computers must be shut down and sensitive material should be locked away at the end of the work day

US federal agency employees, when required by official duties, can store information on mobile systems, computers, and personal electronic devices so long as the information is encrypted. However, personnel should not disclose the information, and must not retain the information after the specific work transaction is complete.

The airports interviewed had similar and relatively simple ways of storing their privileged materials. Many of their storage methods reflected the regulations put forth by the TSA in 49 CFR § 1520. Electronic documents are, at a minimum, stored on a network drive or individual work computer with unique log-in credentials for each user. Some airports separate the documents on the network by division or department, consistent with IT best practices.

At least one airport stores their materials, except for working documents, in a cloud-based storage service that is protected with unique log-in credentials. Storing information in cloud services (such as

[3] Planned for release in 2017

SharePoint and Basecamp) should be carefully considered. Some cloud services are more secure with your airport's virtual information than others.

2.3.2 Sharing

Airports receive and share privileged materials from a variety of third-party/outside sources, such as:

- Manufacturers and vendors
- Software developers
- Military
- Tenants/concessionaires
- Contractors and their subcontractors, such as architects and consultants
- Law enforcement
- Government officials (state and federal)
- Job applicants
- Other divisions/departments
- Other airports

Federal regulations are specific in the requirements and limitations regarding the sharing of regulated materials, but these practices could be, and at many airports are, applied to privileged information because the procedures and technology are already being utilized.

Government agency regulations prevent personnel from discussing regulated information on unsecured telephones and wireless devices. Sending regulated information via fax should be avoided, but if necessary, ensure an authorized person will receive the fax. It is important to note that most fax technology may inadvertently retain virtual or ghost copies of faxed materials on unsecured devices.

Personnel should not discuss or work on regulated information in public places where conversations can be overheard by third parties, including company cafeterias, non-secure hallways, and lobby areas. This is also true when using open networks (such as hotel Wi-Fi) as it is possible for non-authorized persons to hack into a device connected to an open network.

Airports already send most physical documents as if they were regulated documents. If the material is being mailed, it is most often sent through trackable or traceable mail, or through a courier service. If the third party that needs the document is near the airport, a representative may be sent to collect the document from the airport. If the airport feels that the information is especially sensitive, though not regulated, they may require a representative of the third party with need-to-know be dispatched to view the material on-site at the airport under supervision. Usually, this method prevents any copies being made of the materials on display, including pictures.

However, almost all airports distribute and collect materials, internally and externally, via email. If the sender feels the information is sensitive enough, he or she may password protect or encrypt the document. More often, privileged but non-regulated material is sent via email without this additional protection. Sharing of electronic material between departments is often done via a shared location on the local server, especially if the document's file size is too large to send through email. When transmitting electronic SSI, TSA requires attachments to be password protected and to send the password in a separate email or by phone.

DHS prohibits storing regulated material on intranets and browser-based enterprise content management platforms if unauthorized individuals have access to the platform. In contrast, Microsoft employees must upload the password-protected document to the project SharePoint and send a link to that document, never attach it. Only persons with the SharePoint link and the password would have access to the document or file.

At least one airport uses a cloud-based service to send and collect materials, using project folders in the cloud system to keep the documents separated. This method also allows the airport's employees to send links to the document, which may be password protected or require log-in credentials. Persons outside the airport may be granted access to specific folders that allow them to upload material related to that project.

2.4 Tracking Privileged Materials

All organizations and agencies identified during the literature review stress the importance of restricting access to privileged materials. However, sometimes it is necessary to share privileged material with personnel outside of the organization or agency. When sharing material with contactors, vendors, or other entities, most require an NDA to be executed prior to granting access to the data. GameStop requires the written release of contractor, vendor, supplier, or customer information before it can be released for any reason, including procurement activities.

Airports are only occasionally given mandates on handling privileged information from third-parties. When this does occur, the mandates are almost always noted in the document itself or in the NDA and/or contracting language, but are sometimes verbally communicated in an informal manner. According to the airports interviewed, this happens rarely because the materials are either protected under some state or federal law, or are not considered privileged enough to merit additional protection. Because there are few written or formal policies regarding the subject of privileged material at airports, airports indicated that employees rely heavily on professional knowledge and experience to determine how to handle the privileged materials they deal with.

However, when the material must be protected, the methods of conveying the requirements to airport employees include:

- Email
- Managers/supervisors
- Cover letters and markings on the document
- Contracts and NDAs
- Memos
- Discussions during meetings

If privileged information must be mailed, most organizations and agencies—including the airports interviewed—require it to be mailed by traceable delivery service using an opaque envelope or wrapping. Interoffice mail should also be sent in an unmarked, opaque, and sealed envelope. This is consistent with TSA's SSI guidelines.

In some cases, electronic information is posted in a cloud-based service or an organization's intranet, which is how Microsoft personnel manage their material. Access to these sites should be monitored closely and should be approved by project managers. Using cloud-based services allows the project managers to quickly see what changes have been made and who downloaded a copy of the document.

The airports interviewed indicated that they do not perform formal audits on the third-parties with access or copies of the information once the information is delivered. Any audits are performed in an informal manner, usually through casual observations during visits. Only city auditors and government officials perform internal audits on the airport. This seems to be consistent across all the organizations and agencies identified during the literature review—only government officials perform formal audits on the handling and management of privileged and regulated information once it has been delivered.

In general, it is the department head or project manager that ensures privileged materials, including regulated materials, are handled per regulations and policies.

2.5 Destroying Privileged Materials

States have specific laws that regulate the retention period for privileged material. All government agencies—including city and county governments—are required to define a retention period to store privileged material for a specific number of days, months, or years. Each state has different regulations for this retention period. When the retention period is over, organizations and agencies are permitted to destroy or declassify their privileged materials.

Many organizations also utilize a retention policy and schedule. These reflect legal obligations while meeting organizational need. Once the retention period is complete, the material should be destroyed without delay. According to the USDA, working documents that are no longer in progress should also be destroyed using the organization's or agency's destruction policies. The UN requires its personnel, with the assistance of the IT department, to regularly organize and remove material on computers and network locations that have met their retention periods.

It is a consensus across all organizations and agencies reviewed that privileged information that has reached the end of its retention period should be destroyed in such a way that it cannot be read or reassembled. Destruction of material must not be performed by unauthorized personnel, and the UN recommends that the process be supervised by a high-level officer.

Each state has its own retention schedules for different documents. Most airports either follow their state's retention laws or save everything indefinitely. Only one airport indicated they have created their own retention schedule for their documents, which exceeds the state requirements.

Physical materials are usually destroyed by shredding via a cross-cut shredder, manually cutting into squares smaller than a ½ inch, or destroying by fire with the use of a burn bag. Some organizations use a trusted third-party company that will shred material collected in shred bins. If an organization uses one of these third parties, the UN recommends establishing a contract that outlines the transfer and destruction of the material, identifies who will supervise the destruction, and what document logs will be kept of the destruction process.

All the responding airports indicated that they utilize their cross-cut shredder or incinerator to destroy their documents, regardless of sensitivity level. This also adds a security feature to the shredded material—adding non-sensitive and non-regulated material waste to the same bin as regulated and privileged material waste makes it more difficult to find and reconstruct the documents. Some airports have onsite incinerators, and a few airports use a third-party shredding company to pick up and shred their documents.

For electronic and digital material, the information must be completely and permanently removed from the storage device. It is important to note that most standard office devices (computers, fax machines, copiers, servers, etc.) store ghost copies on their hard drives, and these files should be periodically removed. This might include using a software designed to overwrite the information, or employing the expertise of the IT department. Most of the airports interviewed have their IT departments wipe and/or archive the data securely. The airports indicated that electronic materials are generally kept on the airport's servers—including email servers—and, as such, tend to fall under the responsibility of the IT department to archive or remove electronic copies of materials, regardless of sensitivity level. Material stored on individual work computers will usually be moved to the local Recycle Bin or Trash Folder and emptied periodically.

> Ghost files are files that your device (computer, server, fax machine, photo copier, etc.) creates in order to provide a backup of the original file. There are several useful reasons for creating these ghosts, but they also create certain security risks. Even after deleting or removing the original files, ghost files can remain on the device until it is overwritten. This is especially important to consider when disposing of computers, printers, servers, copiers, and other devices that contain some sort of hard drive. It is an IT best practice to allow your IT department to destroy and remove all data, including ghost files.

At least one airport sends its outdated hard drives and storage devices to be destroyed by a third party. Microsoft also sends its outdated hard drives and storage devices to a third party after being wiped of data. Generally, Microsoft has the devices refurbished with this third party so that the devices can be donated or reused. Special consideration should be given when selling or disposing of multifunction copiers, as these devices contain a hard drive.

When possible, the destruction of materials should be as environmentally friendly as possible. Paper should be recycled if possible, but the UN recommends always prioritizing security over other considerations.

> At least one airport has all copies of documents and emails stored on a separate server, regardless of level of sensitivity, retention period, or document longevity. It should be noted that the state this airport resides in maintains long-term retention requirements and has several open government laws that require more transparency.

2.6 Training and Policies on Managing Privileged Materials

Once policies and procedures are established in an organization or agency, the literature recommends that personnel be trained on how to follow them. Social Engineer Hadnagy believes that the best way to prevent security breaches of privileged and regulated information is to have strong policies and procedures in place that give specific guidelines and steps for personnel to follow. Once these are in place, employers should ensure their employees are trained on the policies.

In addition to training, the UN recommends the development and establishment of a sustainable records management program. The program would provide a clear definition of program objectives, responsibilities, and authorities. It should formalize the process for handling and maintaining privileged and regulated material. It should contain the organization or agency's retention period and emergency recovery-of-records plan.

Most organizations and agencies require that privileged projects and materials be managed by a specific position in the company. For instance, GameStop requires disclosure of information to be authorized by someone in the company at the Vice President level or above. TSA requires a supervisor to give permission for personnel to take privileged information out of the workplace. The policies and procedures should clearly define who is responsible for ensuring information security and who is authorized to qualify someone as having the need-to-know.

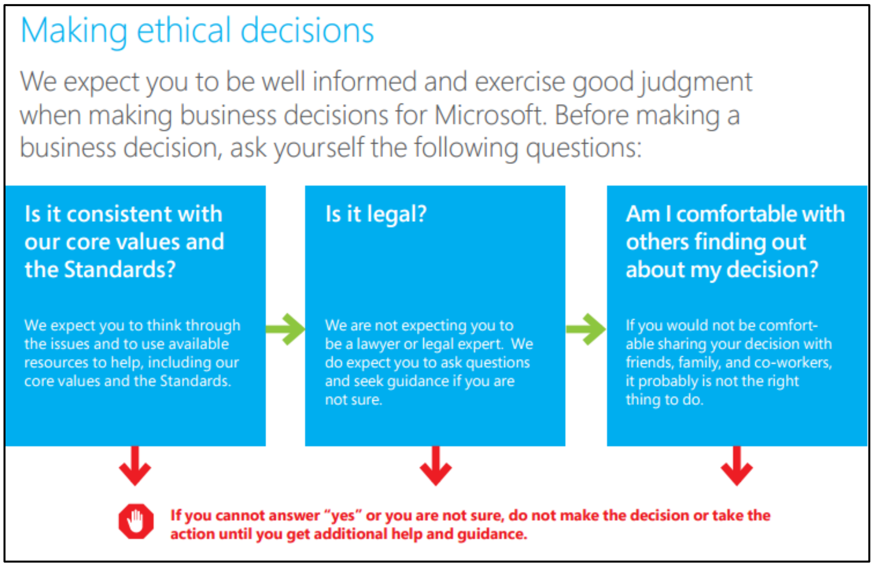
Most airports already require a manager or supervisor to manage privileged and regulated information, although almost all airports interviewed indicated that this was more of an informal policy and not explicitly written in their SOPs.

All airports interviewed have little in the way of formal training on handling privileged information outside of the DHS's SSI training. Most airports have some sort of hiring training and/or videos, but these only briefly touch on the subject of regulated information, and usually only SSI material. At least one airport has regular meetings with managers and supervisors in which the head of security reiterates the airport's policy for regulated and privileged information. This ad hoc training is meant to filter down to the employees in the managers' departments.

A few airports have a Code of Ethics and/or Code of Conduct handbook that goes into greater detail on privileged information, but again, these tend to focus specifically on SSI material.

Microsoft presents a simple flow diagram in their Code of Ethics, shown in Figure 2-5, to help its employees make ethical decisions. This provides their employees with the confidence to answer questions with potentially privileged information, find the answer in the organization's SOPs, or approach a manager for assistance.

Figure 2-5. Microsoft Flow for Making Ethical Decisions



Making ethical decisions

We expect you to be well informed and exercise good judgment when making business decisions for Microsoft. Before making a business decision, ask yourself the following questions:

Is it consistent with our core values and the Standards?

We expect you to think through the issues and to use available resources to help, including our core values and the Standards.

Is it legal?

We are not expecting you to be a lawyer or legal expert. We do expect you to ask questions and seek guidance if you are not sure.

Am I comfortable with others finding out about my decision?

If you would not be comfortable sharing your decision with friends, family, and co-workers, it probably is not the right thing to do.

If you cannot answer "yes" or you are not sure, do not make the decision or take the action until you get additional help and guidance.

Source: Microsoft's Standards of Business Conduct

While the diagram and underlying message is relatively simple, it was designed to instill a sense of confidence in Microsoft's employees and give them a company-approved way out of situations that make them feel uncomfortable. Social Engineer Hadnagy also recommends providing employees with a company-approved message to provide when confronted with an uncomfortable situation involving sharing of privileged information.

While airports may not have a similar diagram written in their policies, all of the airports interviewed indicated they have a similar, though informal, process; their employee training is mostly on the job training or "commonsense" training (i.e., ask a manager or supervisor if confronted with an unknown situation). DHS has provided a Best Practice Guide for Non-DHS Employees and Contractors, presented in Appendix B, which airports may use.

2.7 Breaches of Controlled Materials

None of the airports interviewed indicated that they have a formal process for remediation of a breach of controlled materials. It should be noted that if the airports do have a formal policy, it is not well known and/or has never been needed. Most airports indicated that they would report the breach to their manager and/or the airport's legal department or attorney. If the material was shared accidentally through email or other electronic means, the IT department would be contacted and an attempt to recall the material would be performed.

Depending on the seriousness of the breach and the intent behind it, all of the airports indicated that an investigation would be conducted and new processes would be put in place to prevent future breaches.

Very few organizations and agencies—including airports—described their formal disciplinary policies regarding the mishandling of privileged material. Most indicated that the disciplinary action would depend on the circumstance, i.e., how serious the mishandling was and the intent behind it.

2.7.1 State FOIA Requests

In the case of state FOIA requests, every state has different requirements, regulations, and procedures. However, airport procedures can be summed up in four categories:

- Reviewed and/or distributed by a single person (e.g., a FOIA coordinator, an airport employee, or a city/state official)
- Reviewed by legal department or attorney
- Reviewed by department heads
- Reviewed by security department or risk management department

Most states have a government information specialist—such as Utah's Government Records Access and Management Act coordinator—who receive, filter, and distribute FOIA requests. Some airports have an airport employee or a city official who reviews and/or distributes the requests to the appropriate department. However, almost all airports filter requests through their legal department before fulfilling those requests. Occasionally, the requests are also reviewed by the department heads or security/risk management department, depending on the available resources.

Because each state requires different levels of transparency, some airports have the authority to refuse access to materials, while other airports may have to surrender the information. For instance, at least one airport's CCTV footage is considered SSI and is therefore exempt from state FOIA requests.

> All 50 states have freedom of information or open government laws (colloquially called Sunshine Acts) that govern documents at the state and local levels. The provisions of these laws vary from state to state, with some states providing more access to material than others. The National Freedom of Information Coalition has created a webpage with links to each state's Freedom of Information Laws:
> http://www.nfoic.org/state-freedom-of-information-laws

SECTION 3: NEXT STEPS

3.1 Evolving Trends

Technological advances are creating a new environment that prizes digitization over physical and printed media. The transition to digital or paperless content management may require additional resources and increased cost. Knowing the evolving trends in digital technology may offer airports some additional issues to consider when converting to a paperless enterprise.

Cloud Services: Cloud-based services (sometimes referred to as cloud computing) are internet-based services that provide processing resources and data to computers and other devices on demand, such as networks, servers, storage, applications, and other services. Cloud computing and storage solutions offer users and organizations the ability to store and process their data in such a way that it can be accessed anywhere, as long as the user has internet access and log-in credentials. Advocates of the service claim that this type of data management allows for lower infrastructure costs because there is no need to purchase hardware such as servers. Instead, the user or organization pays for a subscription service, which varies by service provider and the amount of storage/services needed. Common examples of cloud-based services identified during the literature review and airport interviews include SmartSheet, SharePoint, and Basecamp. Other cloud services not identified during the interviews include Dropbox, Box, OneDrive, and Google Drive.

Mobile Applications: Organizations are increasingly embracing mobile applications (apps) to improve productivity. In the digital age, mobile apps allow access to personnel resources (e.g., schedules, paycheck stubs, etc.), organization emails, and document sharing via cloud services. Some airports have integrated communications platforms that control both critical and non-critical systems and can be accessed using mobile apps. These apps allow for a more productive and efficient workplace, but pose security threats if the digital device is stolen or lost.

Fax Machines, Photocopiers, and Printers: Nearly all enterprise multifunctional copiers—including fax machines—contain a hard drive that stores data from each document copied, scanned, faxed, emailed, or printed by the machine. When multiple departments use a single multifunction copier, there is significant potential for hundreds of privileged and regulated documents to be stored on that copier hard drive. In addition, faxes are often sent via email attachments, and may be kept on local email servers. Airports should consult their IT department for erasing the information before disposing or selling any device.

Voice over Internet Protocol (VoIP) Services: VoIP systems leverage the internet as an infrastructure for voice communications. While this service reduces cost and consolidates systems, it also places greater demand on the local network/intranet. Some voicemail messages are sent as email attachments and these messages may be kept on the local email server. In addition, if an organization’s network is compromised, then the communication system is also compromised, and potentially sensitive conversations could be recorded.

Virtual Private Network (VPN) and Remote Access: VPNs and remote access software/apps allow users to access otherwise restricted company networks. They provide functionality, security, and network management benefits to the user (usually an employee) while they are out of the office. Documents can be transferred between the networked device and the remote device using the software or other services, such as email or cloud service. VPN and remote access services can be installed by malware, allowing unauthorized access to the network, device storage, and hardware (such as cameras).

Two PARAS research projects that are currently underway and scheduled for release in 2017 may offer additional resources for airports looking for best practices in sharing and protecting digital privileged information:

- PARAS 0007: *Quick Guide for Airport Cybersecurity* suggests guidance to establish and/or enhance a cybersecurity posture for safe operations of airports, and includes an accompanying interactive tool to facilitate implementation.
- PARAS 0010: *Guidance for Protecting Access to Vital Systems Impacting Airport Security* discusses best practices for administering and managing access to vital systems (e.g., video management/surveillance systems, access control, and credentialing) and physical spaces where those systems reside.

3.2 Suggestions for Further Research

The authors' research has shown that there are little to no industry-defined standards for handling privileged material. There is not even a clear understanding of what constitutes privileged material. Most airports indicated that if it is not classified by a government agency, it is subsequently open to FOIA requests, and therefore, further protection is unnecessary.

Further research should be focused on establishing standards and/or best practices to determine and categorize privileged information based on different risk levels (e.g., whether information could be misused, either intentionally or unintentionally).

Additional research should be conducted to look at state and federal laws that protect privileged materials, such as working drafts. While state laws vary, it may be possible to identify types of documents that are standardized across the country. For example, airports interviewed acknowledged that while a contract is in the bidding process there is a period in which the documents are kept confidential to avoid unfair competition.

Templates or examples of relevant policies and procedures should be provided or developed for the guidebook. When possible, metrics or measurement tools should be identified or created to determine if an airport's policies and procedures are effective.

A detailed guidebook should be developed to identify best practices in the six activities discussed in this synthesis paper.

REFERENCES

Aviation and Transportation Security Act of 2001, Pub. L. 107-71, 115 Stat. 597. https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf

Consumer Partnership for eHealth. (2010). *Protecting Sensitive Health Information in the Context of Health Information Technology*. *http://www.nationalpartnership.org/research-library/health-care/HIT/protecting-sensitive-health.pdf*

Critical Infrastructure Information Act (CIIA) of 2002, codified at 6 U.S.C. §§131 – 134. https://www.fas.org/sgp/crs/RL31762.pdf

Economic Espionage Act of 1996, Pub. L. 10-294, 110 Stat. 3488. https://www.congress.gov/104/plaws/publ294/PLAW-104publ294.pdf

Exec. Order No. 13587, 76 Fed. Reg. 198 (October 13, 2011). https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

Federal Records Act of 1950, as amended, codified at 44 U.S.C. chapters 21, 29, 31, and 33. http://www.archives.gov/about/laws/fed-agencies.html

Freedom of Information Act (FOIA), codified at 5 U.S.C. chapter 5. https://www.foia.gov/

GameStop. (2005). *Code of Standards, Ethics & Conduct.*

Hadnagy, C. (2011). Prevention and Mitigation. In *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley.

Hadnagy, C. (2016, July 14). Phone interview.

Information Commissioner’s Office. (2016). *The Guide to Data Protection*. https://ico.org.uk/for-organisations/guide-to-data-protection/

International Civil Aviation Organization (ICAO). (2014). *Aviation Security Manual*, 9*th ed*. Quebec, Canada: ICAO.

Maritime Transportation Security Act of 2002, Pub. L. 107-295, 116 Stat. 2064. https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

Massachusetts Institute of Technology. (2008). *Sensitive Data: Your Money AND Your Life. http://web.mit.edu/infoprotect/docs/protectingdata.pdf*

MaxFilings. *Do I Have Trade Secrets to Protect?* https://www.maxfilings.com/incorporation-knowledge-center/Trade-Secrets-to-protect.php

Microsoft. *Standards of Business Conduct.*

National Freedom of Information Coalition. *State Freedom of Information Laws.* http://www.nfoic.org/state-freedom-of-information-laws

Port of Portland. (2011). *Secure File Transfer Application: Quick Reference Guide.*

Presidential and Federal Records Act Amendments of 2014, Pub. L. 113-187, 128 Stat. 2003. https://www.congress.gov/113/plaws/publ187/PLAW-113publ187.pdf

PricewaterhouseCoopers. (2010). *Protect your organization's sensitive information and reputation with high-risk data discovery*. http://www.pwc.com/us/en/it-risk-security/assets/high-risk-data-discovery.pdf

Protection of Sensitive Information, 49 C.F.R. § 1520 (2002). https://www.gpo.gov/fdsys/pkg/CFR-2011-title49-vol9/pdf/CFR-2011-title49-vol9-part1520.pdf

Relyea, H. C. (2008). *Security Classified and Controlled Information*. New York, NY: Nova Science Publishers.

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I assess the quality of my office's records systems*? https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Recordkeeping%20Quality.pdf

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I ensure records are secure*? https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Secure%20Records.pdf

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I protect records from loss or damage*? https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Protecting%20Records%20from%20Loss.pdf

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I protect records in an emergency*? https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Protecting%20Records%20in%20Emergency.pdf

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I protect sensitive information*? https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Sensitive%20Information.pdf

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: When and how can I destroy records?* https://archives.un.org/sites/archives.un.org/files/uploads/files/Guidance%20Destroying%20Records.pdf

United States Department of Agriculture (USDA). (2005). *Cyber Security Manual: Sensitive but Unclassified (SBU) Information Protection.* https://www.ocio.usda.gov/sites/default/files/docs/2012/DM3550-002%5B1%5D.pdf

United States Department of Homeland Security. (2014) SSI Training for DHS Stakeholders. http://www.hsuniversityprograms.org/default/assets/File/Data%20Sharing%20Workshop%202014-SSI%20Training.pdf

United States Department of Homeland Security. (2012). *Handbook for Safeguarding Sensitive Personally Identifiable Information.*

https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

United States Office of Personnel Management. Taking Adverse Actions Based on Suitability or Security Issues [PowerPoint slides]. Retrieved from https://www.opm.gov/policy-data-oversight/employee-relations/training/presentationsuitabilitysecurity.pdf

United States Transportation Security Administration. *Sensitive Security Information: Best Practices Guide for DHS Employees and Contractors*. https://www.tsa.gov/sites/default/files/ssi_quick_reference_guide_for_dhs_employees_and_contractors.pdf

United States Transportation Security Administration. *Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors*. https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf

ABBREVIATIONS, ACRONYMS, & INITIALISMS

AAAE	American Association of Airport Executives
ACI-NA	Airports Council International – North America
AEP	Airport Emergency Plan
CBO	Congressional Budget Office
CCTV	Closed-Circuit Television
CHRC	Criminal History Records Check
DHS	Department of Homeland Security
DOT	Department of Transportation
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GAO	Government Accountability Office
IATA	International Air Transport Association
LES	Law Enforcement Sensitive
NARA	National Archives and Records Administration
NDA	Non-Disclosure Agreement
OIG	Office of Inspector General
OPM	Office of Personnel Management
PARAS	Program for Applied Research in Airport Security
PCII	Protected Critical Infrastructure Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
RFI	Request for Information
RFP	Request for Proposal
SBU	Sensitive but Unclassified
STA	Security Threat Assessment
UN	United Nations
USDA	United States Department of Agriculture
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

GLOSSARY

Freedom of Information Act (FOIA)
FOIA (5 U.S.C. § 552) is one of the federal laws that allow for full or partial disclosure of information and documents controlled by the US Federal Government. The act grants the public the right to request and access certain records from federal agencies. There are currently nine exemptions that protect information regarding personal privacy, national security, and law enforcement.

Exemption 1: Information that is classified to protect national security

Exemption 2: Information related solely to the internal personnel rules and practices of an agency

Exemption 3: Information that is prohibited from disclosure by another federal law

Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged

Exemption 5: Privileged communications within or between agencies, including:

- Deliberative Process Privilege
- Attorney-Work Product Privilege
- Attorney-Client Privilege

Exemption 6: Information that, if disclosed, would invade another individual's personal privacy

Exemption 7: Information compiled for law enforcement purposes that:

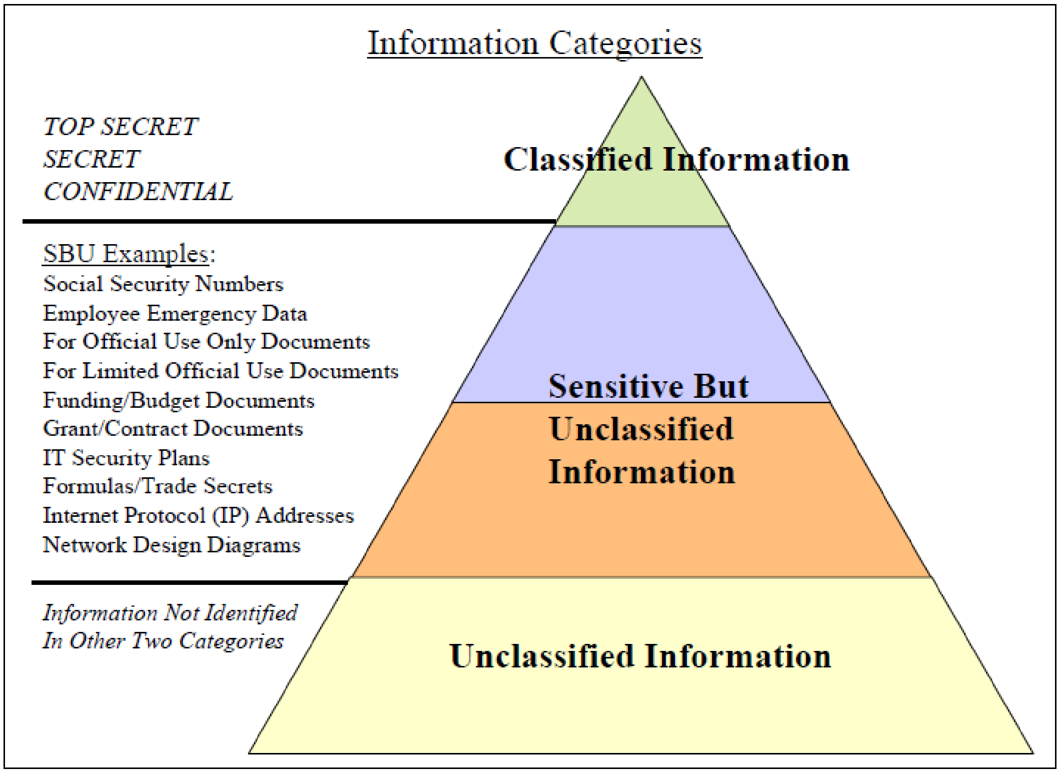
a. Could reasonably be expected to interfere with enforcement proceedings
b. Would deprive a person of a right to a fair trial or an impartial adjudication
c. Could reasonably be expected to constitute an unwarranted invasion of personal privacy
d. Could reasonably be expected to disclose the identity of a confidential source
e. Would disclose techniques and procedures for law enforcement investigations or prosecutions
f. Could reasonably be expected to endanger the life or physical safety of any individual

Exemption 8: Information that concerns the supervision of financial institutions

Exemption 9: Geological information on wells

Material that falls under one of these nine exemptions will fall into one of the categories shown in Figure G-1.

Figure G-1. USDA Information Categories



Source: USDA Cyber Security Manual, 2005

SBU is divided into two categories because it is a broad category that includes the regulated means of protecting information, such as SSI, and unregulated means of protecting information, such as FOUO and LES.

HIGH-RISK DATA AND PII

PricewaterhouseCoopers, an auditing and consulting company, describes sensitive information (or high-risk data) as "…any information that, when lost, can lead to significant contractual or legal liabilities; serious damage to [the] organization's image and reputation; or legal, financial, or business losses." Examples include:

- Name and initials, in any combination
- Home address or telephone numbers
- Email address
- Date of birth or age
- Gender
- Marital status
- Nationality
- Sexual orientation
- Racial or ethnic origin
- Religious beliefs
- Social security number
- State-issued or any other government-issued identification number
- Mother's maiden name
- Driver's license number or similar operating license information
- Passport number
- Credit and criminal history
- Credit, ATM, and debit card numbers
- Bank account numbers
- Financial account numbers
- Payment card information, such as expiration dates, PINs, magnetic strip data, and CVVs
- Security codes, access codes, and passwords
- Physical and psychological health status and history
- Disease status and history

- Medical treatment history
- Diagnoses by healthcare professionals
- Prescription information
- Health insurance information and account number
- Insurance claim history
- Salary
- Service fees
- Other compensation information
- Background check information

Much of this information is also considered PII, which DHS defines as "…any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

PROPRIETARY

Proprietary information is protected under US and international intellectual property laws, such as the Economic Espionage Act of 1996, US Copyright Law, US Patent Law, US Trademark Law, and dozens of international treaties. Information is considered proprietary if there is a substantial likelihood that a reasonable investor would consider it important in making a decision to trade in the public securities of the company.

Anti-trust and fair competition laws, such as the Federal Trade Commission Act of 1914, prohibit anti-competitive behavior. These laws include exposing competitively sensitive information (such as proprietary material and trade secrets) that could be used to gain an advantage in stock trading or the competitive market.

GameStop and Microsoft give several examples of proprietary material in their code of conduct manuals. These include:

- Financial information
- Supplier information
- Vendor information
- Customer information
- Sales figures
- Business plans and projections
- Profit and performance reports
- Software or technologies
- Research
- Artwork
- Advertising schedules
- Growth strategies
- Customer lists
- Product and service information
- Vendor products being developed before vendor has authorized disclosure
- Vendor goods and services pricing
- Intellectual property
- Techniques and methods of operation

Trade secrets are also considered proprietary information and are defined by the Economic Espionage Act of 1996 as "…all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible […] if –

a. The owner thereof has taken reasonable measures to keep such information secret; and
b. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public."

Examples of common trade secrets include:

- Business methods
- Business plans
- Business forecasts
- Market analyses
- Marketing plans
- R&D information
- Business relationships
- Product information
- Pricing information
- Financial information
- Profit margin information
- Overhead information
- Cost information
- Purchasing information
- Office techniques and systems
- Manuals and standard operating procedures
- Computer databases
- Designs, drawings, blueprints, and maps
- Machine processes

SSI

Federal law 49 CFR § 1520, *Protection of Sensitive Information*, defines SSI as "…information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would:

1. Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

2. Reveal trade secrets or privileged or confidential information obtained from any person; or

3. Be detrimental to the security of transportation."

STATE FREEDOM OF INFORMATION LAWS, OR OPEN GOVERNMENT LAWS

All 50 states have freedom of information laws or open government laws (colloquially called Sunshine Acts) that govern documents at the state and local levels. The provisions of these laws vary from state to state with some states providing more access to material than others. The National Freedom of Information Coalition has created a webpage with links to each state's Freedom of Information Laws: http://www.nfoic.org/state-freedom-of-information-laws

APPENDIX A: INTERVIEW QUESTIONS

1. Contact information

Airport Three-Letter Code

Airport's FAA Category Size

Airport’s Owning and Operating Body

Approximately how many employees are onsite?

Approximately how many employees manage or work with sensitive information?

2. Generating Sensitive Information

What documents or types of information does your airport consider sensitive, regardless of SSI designation?

What types of sensitive information does your airport generate?

What are the different levels of sensitive information your airport uses?

How are your documents designated sensitive information?

Is there a process the material must go through to be designated sensitive information?

If so, how is this information distributed outside the airport?

Do you include mandates on how materials outside the airport are handled?

How do you audit outside sources to ensure they are complying with your airport's mandates?

3. Processes

What is your airport's process for collecting sensitive information internally?

What is your airport's process for storing sensitive information?

What is your airport's process for accessing sensitive information?

What is your airport's process for transporting sensitive information?

How is "Need to Know" determined?

Who determines access privileges?

What is your airport's process for recovering and disposing of sensitive information, both physical copies and electronic?

4. Outside Sources' Sensitive Information

What types of industries provide your airport with sensitive information?

Do these sources (other than state and federal sources) mandate how the information is handled?

How are the mandates from outside sources communicated to your employees? (e.g., via email or NDAs)

How is your airport audited for compliance with the mandates?

5. **Security**

What type of vetting is in place for people granted access to sensitive information?

How do the vetting requirements change based on the level of sensitive information?

How do you ensure vetting of persons with access is up-to-date?

How are employees trained to handle sensitive information?

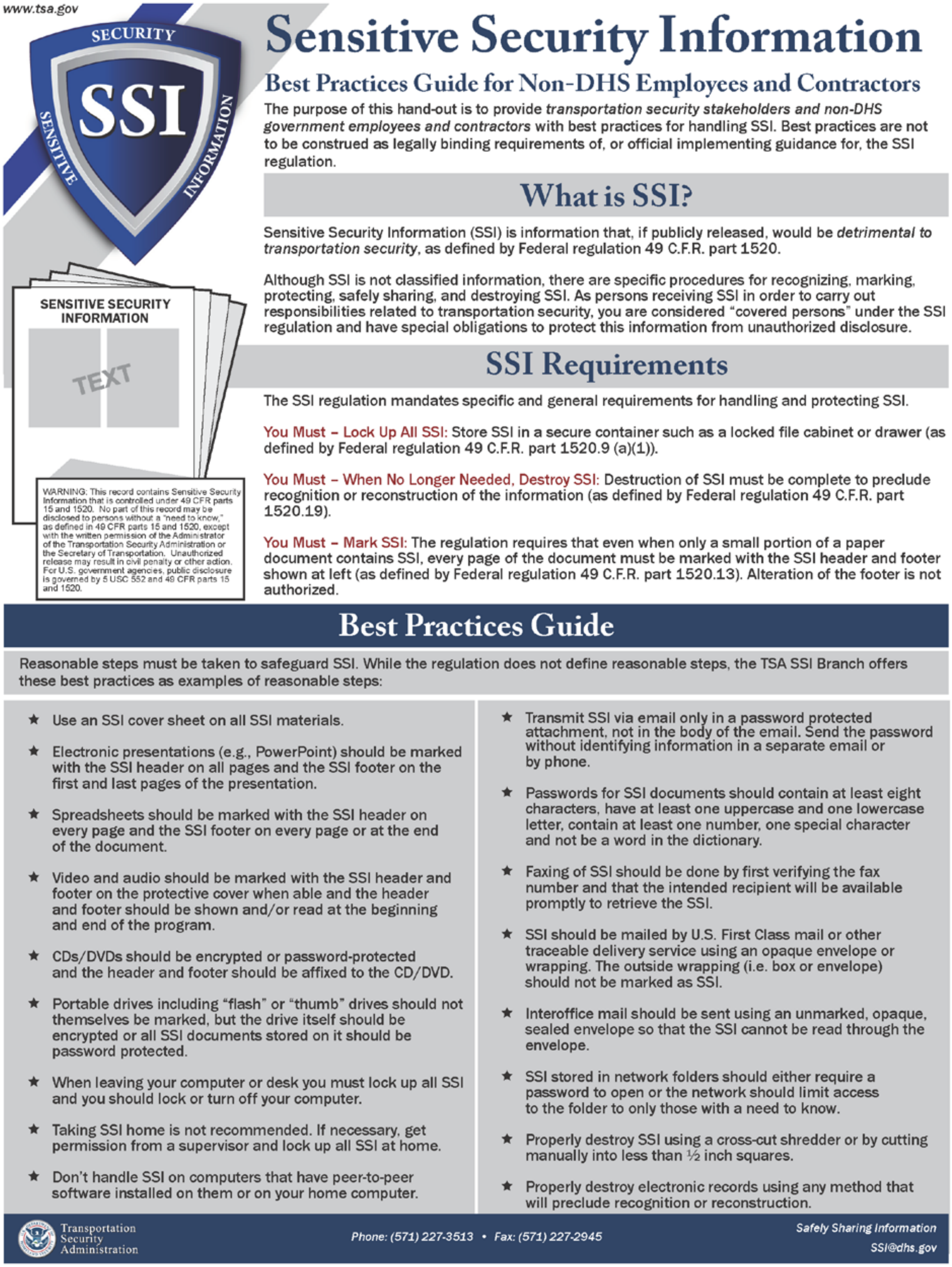
What is your airport's process if there is a breach of sensitive information materials?

6. **Requests for Access**

Do persons seeking sensitive information use your state's Freedom of Information laws?

How do you handle requests for sensitive information made through your state's Freedom of Information laws?

APPENDIX B: DHS BEST PRACTICE GUIDE FOR NON-DHS EMPLOYEES & CONTRACTORS


SECURITY
SSI
SENSITIVE
INFORMATION
SENSITIVE SECURITY INFORMATION
TEXT

www.tsa.gov

Sensitive Security Information

Best Practices Guide for Non-DHS Employees and Contractors

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.

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.

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 reconstruction.

Transportation Security Administration

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

Safely Sharing Information
SSI@dhs.gov