PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0044 June 2023

Strategies for Aviation Security Stakeholder Information Sharing

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Don Zoufal
CrowZnest Consulting, Inc.
Chicago, IL

Sean Cusson
Del Ray Solutions, LLC
Alexandria, VA

Michele Freadman
M. Freadman Consulting, LLC.
Attleboro, MA

Douglas Wendt
Jessica Gafford
TransSolutions, LLC.
Fort Worth, TX

Mary Ann Pantle
Rochester, IL

COPYRIGHT INFORMATION

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 ASSIST (Airport Security Systems Integrated Support Testing) 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 POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), 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 of 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 PARAS Program Manager*

PARAS 0044 PROJECT PANEL

Ethan Barske *Portland International Airport*
Mark Crosby *McCarthy Building Companies*
Stephanie Lane *Dallas Fort Worth International Airport*
Greg Principato *National Aeronautic Association*
Joan Stasiowski *Pittsburgh International Airport*
Christian Terry *Delta Air Lines*
Nikola Vucicevic *John F. Kennedy International Airport*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0044 Research Team would like to acknowledge the following organizations and individuals for their contributions to the development of this research. First, National Safe Skies Alliance and Jessica Grizzle for facilitating the research and providing guidance. Second, the PARAS 0044 Project Panel members who provided significant review and individual interviews. And finally, the Research Team would like to thank the dozens of airport operators; aviation association leaders; aviation service providers; federal, state and local government leaders; and non-aviation experts who took time out of their busy schedule to discuss information sharing with us. Without cooperation and assistance from these individuals, PARAS research documents would not be as successful. We are withholding acknowledgment of individuals and their organizations to protect the confidentiality of the interviews.

CONTENTS

TABLES & FIGURES

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

2FA	Dual-Factor Authentication
A4A	Airlines for America
AAAE	American Association of Airport Executives
AAM	Advanced Air Mobility
ACI-NA	Airports Council International – North America
ACS	Access Control System
ADIAC	Aviation Domain Intelligence Integration and Analysis Cell
A-ISAC	Aviation Information and Analysis Sharing Center
ALEAN	Airport Law Enforcement Agencies Network
AOC	Airport Operations Center
ASAC	Aviation Security Advisory Committee
ASC	Airport Security Coordinator
ASP	Airport Security Program
BOLO	Be on the Lookout
CAA	Cargo Airline Association
CAD	Computer-Aided Dispatch
CASP	Civil Aviation Security Program
CBP	Customs and Border Protection
CII Act	Critical Infrastructure Information Act of 2002
CISA	Cybersecurity and Infrastructure Security Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Service
CLT	Charlotte Douglas International Airport
COC	Combined Operations Center
CUI	Controlled Unclassified Information
DOD	Department of Defense
DOS	Department of State

DSAC	Domestic Security Alliance Council
EMS	Emergency Medical Services
EOC	Emergency Operations Center
eVTOL	Electric Vertical Take-off and Landing
FBO	Fixed-Base Operator
FIO	Field Intelligence Operator
FIS	Federal Inspection Services
FLL	Fort Lauderdale–Hollywood International Airport
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTP	File Transfer Protocol
GRID	Global and Regional Intelligence Digest
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICE	US Immigration and Customs Enforcement
ICP	Incident Command Post
IDMS	Identity Management System
III	Interstate Identification Index
IMAP	Insider Mitigation Assessment Program
IOC	Integrated Operations Center
IPAWS	Integrated Public Alert and Warning System
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Officer
LES	Law Enforcement Sensitive
MFA	Multifactor Authentication
MOA	Memorandum of Agreement

NACo	National Association of Counties
NCIC	National Crime Information Center
NDA	Non-Disclosure Agreement
ODNI	Office of the Director of National Intelligence
OSAC	Overseas Security Advisory Council
PCII	Protected Critical Infrastructure Information
PHI	Protected Health Information
PII	Personally Identifiable Information
PIO	Public Information Officer
PSAP	Public Safety Answering Point
QR	Quick Response
RAA	Regional Airlines Association
SAGE	Structured Analytic Gateway for Expertise
SBU	Sensitive but Unclassified
SEADOG	Southeast Airports Disaster Operations Group
SeMS	Security Management System
sFTP	Secure File Transfer Protocol
SIPRNet	Secret Internet Protocol Router Network
SMS	Safety Management System
SOC	Security Operations Center
TIN	Transportation Intelligence Note
UAS	Unmanned Aircraft Systems
VMS	Video Management System
WEA	Wireless Emergency Alert
WESTDOG	Western Airports Disaster Operations Group

INTRODUCTION

Information sharing among airports and their stakeholders is essential in understanding, identifying, and mitigating security threats and vulnerabilities. Several after-action reports, including the 9/11 Commission Report, have highlighted the critical importance of information sharing to aviation security. However, the processes for receiving and sharing relevant information present challenges. As the 9/11 Report noted, “The biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information.”

Consider the following hypothetical scenarios that highlight the importance of sharing information between airport stakeholders:

- Scenario 1: Intelligence reports of international threats to aviation operations in the US have resulted in the TSA imposing new regulatory requirements. The airport has heard vague news reports that likely relate to the intelligence, but struggles to understand what the actual risk is to their operation and how they can respond. Further, the requirements impose a burden on their tenants who do not understand the reasons for the new requirements. The airport wants to implement appropriate security measures and manage its security culture by communicating with stakeholders. How can the airport obtain information to better understand the potential threat? And how can information about the threat and enhanced security measures be better shared in the airport community?
- Scenario 2: There are reports of a rise in catalytic converter thefts in the communities around the airport. How can the airport gain information and share it to better protect its parking facilities and rental car garages?
- Scenario 3: An airport tenant has expressed suspicions that a couple of their employees have been using their badges to access their restricted facility outside of their working hours. The airport is concerned that this activity may occur more broadly within its facilities, and wants to implement a strategy that educates relevant stakeholders on the issue and promotes reporting of such incidents. How can the airport share access control, surveillance, or other sensor data to investigate this type of conduct?

This guidance was developed to assist airports in achieving more open information sharing. It provides insights on various types and sources of information, how to better collect it, and how to better share it within the constraints of measures designed to safeguard the information.

HOW TO USE THIS REPORT

This section summarizes each major section of the report and highlights some of the findings and observations of the research. Readers can turn to the relevant section for more detailed discussion of each topic.

Section 1: Information Classification – This section outlines the classification and designation schemas commonly applied to security-related information. This section also discusses compliance, operational, and incident-related information that pose different challenges for classifying and controlling security information. Key takeaways include:

- Airports must understand the classification schema that apply to security information to ensure its proper collection and handling.
- Statutory developments since 2020 has resulted in TSA reexamining the SSI designation of some information.
- There are a number of documents created in response to regulatory requirements that need to be treated as SSI.
- Operational data collected in systems such as CCTV and access control present challenges and opportunities for information sharing. Airports should develop arrangements with key stakeholders to share this data.
- Sharing systems information requires addressing both real-time and archived access.
- Ownership of the system and its technical capabilities can significantly influence the sharing of system data.
- Operations centers (e.g., Security Operations Center, Airport Operations Center) can help airports advance information sharing and enhance operations at the airport.

Section 2: Sharing Sources – This section examines the common sources of shared airport security information. The primary sources of airport security information identified by the research were federal partners, industry organizations, and airlines. Other sources include stakeholders within the airport community and global, regional, state, and local partners. Key takeaways include:

- Familiarity with stakeholders will improve the airport's understanding of their perspective, what information they may have or need, and how they share or receive that information.
- Most airports identified the TSA, FBI, and local law enforcement as their principal sharing partners for security information.
- The TSA provides extensive security information to airports through formal memoranda and reports, conference calls, and briefings.
- Federal agencies operate several programs and sharing platforms that can provide airports access to information about airport threats and vulnerabilities.
- Some federal agencies, such as Customs and Border Protection (CBP) and FAA, do not regularly share security information with airports but work closely with airports regarding specific issues, such as staffing of the CBP areas, laser strikes, and unruly passengers.
- Some sources, such as the Aviation Domain Intelligence and Analysis Cell (ADIAC), share classified intelligence with airport security staff who have the appropriate clearances.

- Federal committees and working groups provide access to a range of resources across the aviation industry, both nationally and internationally, to address growing security threats and vulnerabilities.
- Airlines—particularly large legacy carriers—have extensive intelligence resources and access to public and private networks for collecting security information.
- Airport and industry associations are rich sources of information sharing; airports should consider membership and participation in these organizations where possible.
- State and local fusion centers offer significant resources and information to airports.
- Airport consortiums and ad hoc groups have been created to share information and resources.
- Some airports utilize authorized signatories as a channel to share security information, but this is not appropriate for some types of information.
- Dedicated information sharing or intelligence positions provide useful intelligence and analysis but can be costly.
- Airport law enforcement often serves as the conduit to information and intelligence from federal law enforcement partners.
- Airport service providers have the potential to be vital sources of security information, but most airports have limited engagement with these stakeholders.
- Airports should consider including and engaging frontline workers and the traveling public in information-sharing programs.

Section 3: Building Trust and Improving Engagement – This section examines the industry practices designed to build trusting relationships with stakeholders and improve engagement with information-sharing programs at the airport. Included is a discussion of airport meeting practices, maintaining institutional knowledge, training and education, development of reporting channels and incentive programs, and improving messaging. The section pays particular attention to the growing number of communication systems being utilized by airports. Key takeaways include:

- While classifications and restrictions on release of information need to be respected, airports should consider taking a need-to-share approach to build a trusting network of sharing partners.
- The development and enhancement of trusting relationships is a key factor in sharing information with internal and external stakeholders.
- Building relationships with stakeholders allows the airport to learn how to better share and receive information and determine what method of information sharing (e.g., verbal, written, etc.) is preferred.
- The research identified meetings as the primary source of information sharing in airports, allowing for management to disseminate security information and gain immediate feedback.
- Turnover and attrition rates greatly affect the community knowledge base, and efforts should be made to record badge holder knowledge.
- SOPs should be developed and regularly reviewed to maintain the community knowledge base.
- Badge holders, particularly security and guard forces, should be able to access SOPs and regulations through mobile technology or non-technical approaches.
- Airports can use the credentialing process as an opportunity to implement new policies and training during new badge holder orientation.
- Security consortiums at airports allow for better information sharing among critical security partners.

- Training, which can be delivered through a variety of methods, engages the community, and can be used to encourage reporting and ensure better protection of shared information.
- Developing several reporting programs and methods can encourage participation among stakeholders and increase information flow.
- Applications and mobile technology for reporting and two-way communication can enhance information sharing.
- An email address dedicated to reporting security issues can provide an alternative reporting option for resource-constrained airports.
- Airports utilizing websites and social media to collect information need to ensure that website administrators and social media managers know when and where to forward security-related information.
- Airports can promote security incident reporting programs through initial training, hotline numbers printed on badges, and display boards.
- Airports should consider becoming an authorized alerting authority to quickly send Wireless Emergency Alerts to mobile devices at the airport.
- Cultivating information-sharing relationships during tabletop and emergency exercises can improve day-to-day information-sharing practices.
- To prevent information overload, airports should carefully curate the content of their messages and deploy multiple delivery strategies.
- Airports can use several digital strategies to send information to relevant stakeholders, including email distribution lists and newsletters.
- Audio messaging remains an important information-sharing channel, particularly in emergency situations.

Section 4: Minimizing Unauthorized Information Access – This section affords insights into techniques and tools to ensure that only persons with proper authorization can access security information. It addresses measures to limit further dissemination of information through agreements and other legal measures, and examines concerns related to open records laws. It examines programs and supporting infrastructure to limit and monitor access to materials, and it includes a discussion of records management programs for digital and physical files and materials. This section also covers document or record preparation and creation and discusses techniques for redacting or sanitizing information for lower security levels. Key takeaways include:

- Legal strategies, such as the use of non-disclosure agreements and MOUs, can help facilitate access to security information while controlling further dissemination.
- Provisions in airport leases or rules and regulations can be used to help control the unauthorized dissemination of shared security information by airport tenants and service providers.
- Airports should carefully design access privileges and deploy technology to reduce the likelihood of unauthorized access.
- Digital records can be managed through digital rights programs and access control privileges.
- Airports should carefully weigh the advantages and disadvantages of on-premises versus cloud-based storage.
- Information-sharing platforms can be utilized to share security documents, such as the Airport Security Program, with stakeholders while minimizing the potential of unauthorized access via user rights management programs.

- Records management programs that outline the policies and procedures for securing, retaining, and destroying documents and files can help the airport maintain orderly storage management.
- Airports do not routinely redact information to share with stakeholders, but creating and following redaction guidelines can help the airport share more information.
- Open Records laws vary from state to state. Policies should be created to comprehensively address Open Records requests to ensure legal requirements for disclosure are met while respecting the information protection requirements.
- Some documents are clearly designated SSI or Personally Identifiable Information and are typically shielded from disclosure, but other data, such as CCTV images, are less clear and should be carefully reviewed before disclosure.

SECTION 1: INFORMATION TYPES

The US Federal Government has created multiple security classifications and designations to manage the protection of sensitive information, including the creation, marking, sharing/dissemination, storage, and destruction of information that is considered inappropriate for public release and that could cause harm to transportation security; law enforcement activities, investigations, and operations; federal programs; or operations essential to the national interest. Information that could adversely affect the interest or conduct of national defense, foreign policy, or federal programs, or information that could breach the privacy of individuals may be protected under an Executive Order or Act of Congress.

The type of information dictates whether airports or stakeholders can share the information and how that information can be shared. The airports and stakeholders must understand whether the information they have is classified under federal, state, or local protections and what responsibility they have to protect that information.

These classifications generally do not apply to materials an airport generates during the course of its operations, but in some circumstances the airport's information may require classification. It is important for security professionals to understand the requirements for each classification type so that information is properly protected.

As a technical matter, only select federal agencies can officially designate or direct the designation of materials under the classification schema, and only the agency that designated material can remove the designation. The criteria for what can be designated and the process for designation is set by federal statute or regulation. If airports wish to share protected information with individuals at a lower security level, it is advisable to consult with the designating agency.

1.1 Information Classification

The following discussion identifies the core information types that airports and airport stakeholders may need to make operational and security decisions. Understanding these information types provides a basis for later discussions on how and when to share the information.

Classified Information consists of Top Secret, Secret, and Confidential categories as defined in Executive Order 12356 and used for National Security Information and atomic energy information. Airports occasionally receive Secret information, but this research found that it is uncommon. Federal intelligence agencies have created stakeholder groups to facilitate and improve sharing of classified information; these groups are further discussed in Section 2.1.

Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI) is an umbrella designation for unclassified information that still requires protection. In 2009, the Atomic Energy Act created a new program to manage SBU, now known as CUI. Government agencies are working to implement the new program, but SBU is still commonly used within the aviation industry. The level of security and protection requirements vary by the information category. Categories protected as SBU include the following types:

> ***Protected Critical Infrastructure Information (PCII)*** is protected under the Critical Infrastructure Information Act of 2002 (CII Act), and is information that if released could have a critical impact on "security, national economic security, national public health or safety, or any combination of these matters." PCII is exempt from Open Records requests (also known as Freedom of Information Act [FOIA] or Sunshine Law requests). US airports are considered part

of the critical infrastructure and may produce PCII information. Of note, the CII Act prohibits the disclosure of PCII outside of individuals with homeland security duties. Unauthorized disclosure of PCII may result in a fine up to $250,000, imprisonment up to one year, and/or removal from office or employment.[1]

Sensitive Security Information (SSI) is the most common protected information type in the aviation industry. SSI is defined in 49 CFR § 1520 as "information that, if publicly released, would be detrimental to transportation security." TSA is the principal source of SSI for airports, but airports create and receive SSI material regularly, and nearly all badge holders are required to take some level of SSI training. SSI, in both physical and digital form, must be appropriately marked, safeguarded, and protected from unauthorized disclosure. This is most commonly done with locks or safes for physical documents, and passwords or encryption protections for digital files. In some cases, SSI is shared verbally over phone calls and in virtual meetings, or at in-person stakeholder meetings. Unauthorized disclosure of SSI may result in civil penalties by the DHS.[2]

Personally Identifiable Information (PII) is protected under the Privacy Act of 1974 and defined by the National Institute of Standards and Technology as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." This type of information is most often found in airport credentialing offices and human resources departments. Examples include name, date of birth, social security number, driver's license number, and financial account numbers. PII related to credentialing processes are commonly stored in Identity Management Systems (IDMS) with consent given by the individuals participating in the badging process. There is a growing body of state law governing PII protection.[3] Penalties for disclosure of PII may include civil and criminal penalties. Airports should consult with their legal counsel to determine how PII is defined and protected in their particular jurisdiction.

Protected Health Information (PHI) is information protected under the Health Insurance Portability and Accountability Act of 1996 Privacy Rule. Airports most often manage PHI of their badge holders in their human resources department. During epidemics and pandemics, the airport may request PHI from employees and travelers to help protect the traveling public. This has been the case during the severe acute respiratory syndrome, bird flu, and Ebola epidemics, and the COVID-19 pandemic. Unauthorized disclosure of PHI may result in civil and criminal penalties.

For Official Use Only (FOUO) is a designation used by a number of federal agencies to identify "unclassified information that may be exempt from mandatory release to the public under […] [Freedom of Information Act] FOIA."[4] Information designated FOUO must have the author's permission to be disseminated and is not automatically exempt from Open Records requests. Similar designations include Limited Official Use and Official Use Only. Unauthorized disclosure of FOUO may result in civil or criminal penalties.

[1] Department of Homeland Security, *Protected Critical Infrastructure Information Procedure Manual,* (2009). https://www.cisa.gov/resources-tools/resources/pcii-program-procedures-manual

[2] Transportation Security Administration, *SSI Policies and Procedures Handbook*, (2015)

[3] https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx

[4] Department of Defense (DOD) Directive 5400.07

Law Enforcement Sensitive (LES) is a designation that protects information that could cause harm to law enforcement activities or jeopardize law enforcement investigations or operations. All Points Bulletins and Be on the Lookout (BOLO) notices fall into this designation. LES may only be released to law enforcement agencies and departments, such as sheriffs, airport police, FBI, etc. The restriction on release of LES information can be a significant barrier to information sharing for airports without a dedicated police departments or police officers in security positions at the airport. However, airports with dedicated police departments or trusting relationships with their municipal or state police indicated that the police chiefs/commanders were willing to share certain information that may affect the airport. Unauthorized disclosure of LES may result in civil or criminal penalties.

Criminal Justice Information (CJI) is information designated as part of the FBI's Criminal Justice Information Services (CJIS). It includes a range of information products utilized in connection with law enforcement activities that are provided by the FBI as part of a nationwide information system. This includes state records accessible through the Interstate Identification Index (III), which is a national index of criminal histories (or rap sheets) maintained by the FBI at the National Criminal Information Center (NCIC). Law Enforcement Officers (LEO) are authorized to use the III to request name-based criminal history records information in connection with law enforcement activities. This is a different process than airports conducting a fingerprint-based criminal history records check through a designated aviation channeler. Inquiries to the FBI's NCIC in criminal investigations are made directly through state-operated systems or through systems that connect via the National Law Enforcement Telecommunications System. Airports should work with LEOs to share relevant security updates and CJI, as appropriate. However, airports should understand that sharing of this type of information will be extremely limited.

1.1.1 Over Classification

Almost twenty years after the 9/11 Commission Report, concerns regarding over classification still exist. The 9/11 Report noted that the need-to-know approach is often unsuccessful because it presumes that "… it is possible to know, in advance, who will need to use the information." The report went on to observe:

> Current security requirements nurture over classification and excessive compartmentation of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information."
>
> ***
>
> "Agencies uphold a need-to-know culture of information protection rather than promoting a need-to-share culture of integration.

The TSA, which is the primary source of security-related information for airports, continues to note the importance of information sharing.[5] Recently, there have been significant congressional efforts to address over classification by agencies such as the TSA, including the National Defense Authorization Act of 2022.[6] Key provisions of the law include:

- Ensure SSI is clear and consistent, including reasonable security justifications for the designation
- Develop a schedule to regularly review and update SSI identification guidelines

[5] TSA, *2020 Biennial National Strategy for Transportation Security*, May 29, 2020

[6] *National Defense Authorization Act of 2022*, PL117-8, §6423

- Develop a tracking mechanism for SSI redaction and designation
- Conduct stakeholder outreach to raise awareness of the policies governing the designation and use of SSI
- Ensure inclusion of aviation stakeholders in the development and implementation of Security Directives and Emergency Amendments, and document their input during this process

This statute has resulted in a TSA initiative to publish regulatory requirements (e.g., Security Directives) as non-SSI so that these documents can be published on TSA's website, as they did with the mask mandates in response to the COVID-19 pandemic.

Over classifying information limits airports' ability to share information that may be useful to their stakeholders. However, protection requirements must be fully respected until the entity specifying the classification chooses to declassify the information or release it at a lower tear line. Any concerns about over classification should be raised with the agency imposing those classifications to ensure that classification schemas are not preventing information from flowing to individuals and organizations who may benefit from that information.

Over classification or over protection of sensitive information is a common approach taken by airport operators. However, it should be noted that over classified documents or materials may not receive exemption from Open Records requests.

1.2 Compliance and System Information

Documents and materials related to regulatory requirements, and documents related to the specifications of secure areas or systems are often subject to the classification schema described in the previous section.

Most regulatory documents issued by TSA have SSI designations, including Security Directives and National Amendments. Documents generated by airports to meet those regulatory mandates, such as Airport Security Programs (ASP), will also have SSI designations. The list of information designated as SSI is shown in the box to the right.

These regulated materials will require the appropriate markings, cover sheets, and header and footer language as specified in 49 CFR § 1520.13. These markings alert recipients to the material's protection designation and appropriate protection requirements, including dissemination, storage, and destruction.

Airports may need to share information that contains SSI with stakeholders, such as new requirements in Security Directives. In these instances, airports must consider whether the stakeholder has a need to know and decide what information needs to be shared.

The following information constitutes SSI (as defined in 49 CFR § 1520):

1. Security programs, security plans, and contingency plans
2. Security Directives
3. Information Circulars
4. Performance specifications
5. Vulnerability assessments
6. Security inspection or investigative information
7. Threat information
8. Security measures
9. Security screening information
10. Security training materials
11. Identifying information of certain transportation security personnel
12. Critical transportation infrastructure asset information
13. Systems security information
14. Confidential business information
15. Research and development
16. Other information as determined in writing by the TSA Administrator

Regulatory requirements are typically driven by an inciting event or incident. The context in which the requirements have been created provides an understanding of the "why" of policy changes, the knowledge of which often results in better compliance. Sharing the "why" with stakeholders when updating security requirements fosters a need-to-share culture and provides real-world examples of the consequences of non-compliance.

Airports' system and infrastructure designs represent another example of sensitive information that can be difficult to share because of security concerns. These materials document the existence and function of systems to support security operations and can reveal an airport's physical infrastructure vulnerabilities. Examples include engineering and architectural drawings; specifications of security technology and systems such as intrusion detection, access control, communication, command and control, and CCTV camera deployments.

Securing and sharing documents and materials related to security technology systems or infrastructure vulnerabilities is challenging. The large number of construction projects at airports and the competitive nature of public procurements requires sharing these documents with multiple stakeholders, many of which may be unknown to the airport. Several airports have developed strategies to mark and control documents they release to contractors and bidders during the procurement process for security projects. These are discussed in Section 4.9.

1.3 Operational Information

Operational information is generated in the routine course of operating an airport and providing public services. The proliferation of digital and automated sensor systems has presented opportunities and challenges for airports sharing operational information. Sensor systems generate security data and may also capture PII. However, they also collect significant amounts of non-security information with potentially significant value to the airport and its stakeholders.

Airport CCTV systems and access control systems (ACS) contain a wealth of security data. Airports have differing programs and strategies to share CCTV and ACS data.

1.3.1 CCTV Data

Airports must consider how they will manage requests for and control subsequent dissemination of CCTV data. CCTV systems are one of airports' most robust data platforms for both security-related and non-security-related information. Airports reported that their stakeholders routinely seek access to this data, including local law enforcement entities, TSA, and tenants identifying security risks in their operational areas. Other stakeholders, such as contractors and the traveling public, submit formal requests through Open Records requests or airport processes for non-security related data (e.g., parking lot images for vehicle damage).

SYSTEM CAPABILITIES

Airport CCTV systems have varied capabilities for sharing data. This is often a result of the differing ages of the systems, as developments in technology have resulted in significant enhancements for sharing system data. Newer digital technologies allow for real-time sharing of information through web-based portals and other interfaces. Video management systems (VMS) can facilitate retrieval and review of relevant video. Legacy systems, particularly those utilizing analog technology, have more limited sharing potential unless modified with digital technologies.

The policies and procedures for sharing video need to be aligned with system capabilities. Automated sharing systems have the advantage of:

- Automatically restricting access to certain types of information, such as specific camera feeds, based on the user's permissions
- Limiting the level of access to the information, such as viewing and download permissions
- Developing an audit trail of access to information, including when it was accessed and by whom

As airports increasingly digitize information, these types of features in automated systems should be considered to assist the airport when sharing CCTV images.

SYSTEM OWNERSHIP

System ownership also has significant impact on information-sharing practices. A growing number of airports are taking the position that CCTV images are owned by the airport. This is particularly true for larger airports that have sought to develop consolidated camera networks that include tenant-controlled systems. Tenants are often permitted or, in some cases, may be directed to install cameras in their areas, but the images are captured by a centralized system operated by the airport.

At other airports, tenants or tenant organizations are permitted to own and operate their own CCTV systems in their areas, such as areas with Exclusive Area Agreements and Federal Inspection Services (FIS) areas operated by US Customs and Border Protection (CBP). The tenants must operate those cameras according to parameters set by the airport. While airports do not need to access tenant cameras frequently, it is important for the airport to ensure they understand the structure of the camera system and have access to video data, both in real time and for investigative purposes.

Airports that have been denied access to tenant camera systems should consider installing their own cameras in these areas, particularly common areas such as gate holdrooms and the check-in lobby. Airports may also consider implementing rules or regulations that compel access. In general, airports indicated that their relationships with airport stakeholders allow them to gain access to tenant-operated camera systems when necessary.

As a best practice, airports should document access permissions in a formal or informal agreement, or in an airport CCTV policy or regulation. This will ensure smooth requests for images for all parties, regardless of ownership. These agreements may be tenant security agreements, CCTV agreements, MOUs, leases, and airport regulations. More information on these agreements can be found in Section 4.1.

An example of an airport regulatory structure creating control over camera images and discussions of tenant agreements in general can be found in PARAS 0025 – *Security Regulatory Compliance at Tenant Facilities*.[7]

ACCESS TO AIRPORT OWNED OR CONTROLLED CCTV DATA

Sharing airport-owned CCTV data involves potentially sensitive data and privacy concerns. For this reason, airports should develop data management protocols that consider CCTV management practices, information request processes and requirements, access permissions, and deletion requirements.

[7] **PARAS 0025:** https://www.sskies.org/images/uploads/subpage/PARAS_0025.SecurityComplianceTenantFacilities_.FinalReport_.pdf

Several airports indicated that they require stakeholders to request CCTV images through request forms. Occasionally, these are the same forms utilized for public Open Records requests. These forms assist airports in tracking who is interested in the information, to whom they provide the information, how the information will be used, and, in some cases, how the information is to be managed and destroyed after it is shared. The process to request CCTV images should consider the following:

- Where requests should be directed (e.g., security department or legal department)
- Guidelines for requests
- Information that cannot be shared due to its sensitive nature
- Fees associated with retrieving the requested data and financial details needed to complete payment
- What information should be included in the request
    - Date, time, and location of the requested images
    - Purpose for which the request is being made (e.g., criminal investigation, disciplinary investigation, legal claim, operational need) – particularly when requesting data that includes SSI or PII
- The airport's approval process, including timeframes for response and method of delivery

The nature of the material requested and the entity requesting the information will affect the airport's decision to approve the request for CCTV images. Some airports require these requests to be submitted by specific stakeholder departments or personnel, such as the organization's legal department or security manager. Requests for CCTV images as part of a criminal investigation often must be submitted through the local or airport police department. In establishing these processes, many airports have included requirements for review by the Airport Security Coordinator (ASC) or designee, airport legal counsel and, in some cases, review by TSA.

Many airports choose not to provide the information as a digital file to the tenant. Instead, they invite the requester into the security office to view the images on the airport's monitors. This allows the airport to maintain control over the data.

REAL-TIME ACCESS

Airports grant real-time access to airport-operated CCTV systems only in very limited circumstances. Typically, real-time access is limited to specific operational areas of interest to the requester. For example, many airports afford TSA real-time access to video of TSA operating areas, such as the checkpoint areas, baggage screening areas, etc., but some airports reported that they only provide CCTV images to TSA upon request. It should be noted that not all CCTV systems are capable of real-time sharing. If real-time sharing is desired, the system must be designed for that capability.

In most cases where real-time access is permitted to the TSA, the images are transmitted to monitors located near the checkpoint or a TSA operation center. Real-time viewing is generally limited to specific areas or camera views. While the TSA may be permitted to view real-time images, the ability to download or store images is often restricted. To do so, TSA is required to submit a request to the airport for archived images. This allows the airport to maintain control over its CCTV data and keep a record of the shared data. An example of an MOU with TSA affording real-time access to images on an airport CCTV system is attached as Appendix A.

At one CAT X airport, TSA was provided with office space in the terminal area to set up a TSA operation center. The center has real-time access to the airport's CCTV system to view camera feeds of TSA checkpoints and baggage screening rooms. This supports TSA's ability to resolve events and incidents in these areas, particularly those regarding possible breaches at the checkpoint. The operation center is linked to external TSA resources and a larger airport communications center to facilitate communications.

At another CAT X airport, TSA was afforded space within the Airport Operations Center (AOC) where they were granted access to airport CCTV feeds of the TSA operations areas. The TSA's AOC space also has the capability to access internal TSA communications systems. Collocation of this function in the airport's AOC affords TSA quick access to other airport personnel for expedited information exchange during an event or incident, such as a checkpoint breach.

Several airports raised concerns that TSA could use access to the airport's camera systems to cite the airport for security violations. However, airports that share with TSA in real time indicated that the CCTV images had not been used for compliance enforcement matters.

Some airports stated that they have real-time viewing policies for airline tenants within their operational areas. Many airports indicated they felt more comfortable sharing data with airlines than other tenants because airline regulations are similar to those placed on airports.

At one CAT X airport, some airline representatives are able to view the cameras covering their own operational areas. Prohibitions against unauthorized download are governed both by technical restrictions in the VMS and airport regulations.

Airport governance of shared CCTV images is addressed in greater detail in Section 4.1 of this report.

ARCHIVED DATA

At most airports, access to view archived data is less restricted than real-time access, but still needs to be secured and protected. Archived CCTV data is useful for investigations, but it raises several information-sharing challenges.

Most airports grant TSA universal viewing access to archived images. The same viewing rights are generally extended to tenants, such as airlines, if they can prove a need-to-know and the images are connected to a security or criminal concern. Airports generally deny airlines access to archived images for reasons such as timekeeping or employee work-related conduct.

One CAT I airport shares CCTV images with airline management if they work for a Part 1544 airline and sign a non-disclosure agreement (NDA). The airport never provides camera data to ground handler companies or concessionaires.

Images of passenger checkpoints and baggage screening areas are generally considered SSI to protect the specifics of TSA's procedures, systems, and equipment. This may also extend to other areas that show airport security procedures, such as exit lanes and vehicle gates, or suggest the location or blind spots of the surveillance cameras. However, this determination will be made based on the local TSA and relevant state and local laws.

At one CAT X airport, TSA determined that all CCTV images were SSI, even in areas beyond the passenger screening checkpoint. This included coverage of landside queueing areas and concourses in the Sterile Area.

The airport did not contest TSA's position because it allowed for greater restriction of Open Records law access for CCTV images and had no operational impact on the airport's use of the CCTV images. This arrangement emphasizes how rules can be tailored to each airport. It also suggests the advantage of coordinating with the TSA over concerns about access to CCTV images.

Airports should work closely with their legal counsel and local TSA to determine the criteria for CCTV images to be considered SSI and exempt from Open Records requests. Specifying in writing the restricted information can help resolve requests for images more quickly and provide a clear citation for denial.

1.3.2 Access Control System Data

Data produced by the ACS is security related as it tracks the movements of badge holders through restricted areas. Additionally, since ACSs are often integrated with the credentialing processes, these systems typically include PII. Accordingly, any dissemination of ACS materials should involve considerations for PII release.

ACS methods of operation can vary. While an increasing number of airports have a single, unified system they control, that is currently not the model in most airports. In several airports, tenants operate their own independent ACS at their leased facilities. This is often true if tenant facilities are located in more remote areas of the airport's property, such as rental car facilities. Sharing data from independent ACSs located on airport property will require cooperation with the ACS owner. This can be facilitated by airport regulations and tenant security agreements. Examples of provisions in ACS agreements are provided in PARAS 0025 – *Security Regulatory Compliance at Tenant Facilities*.

ACS data can be useful to airports as they manage their credentialing and unescorted access programs. It is an integral tool to identify, investigate, and mitigate insider threats as it provides the history of employees' access transactions in restricted areas. ACS data provides a record of individual access over a period of time, which can be analyzed to determine patterns that might suggest insider threat activity. This could include badge holders accessing areas of the airport where the employee has no job responsibilities or when the badge holder is off duty. Technologies such as IDMS and artificial intelligence (AI) systems are able to analyze ACS data for access patterns and identify anomalies that might require further investigation. However, effective use of those systems would likely require access to employee schedules and attendance records, which is not typically stored in the ACS and is rarely shared by tenants.

Real-time sharing of a tenant's employment and attendance records with the airport is necessary for these systems to be effective for identifying potential threats. Achieving this would necessitate careful integration of information systems and balancing interests around employee privacy and the stakeholder's proprietary business information. Both the airport and stakeholder would need to freely share sensitive data, share the control and safeguarding of that information, and adhere to the processes necessary to keep it updated. This places pressure on both the airport and the stakeholder, and some stakeholders have expressed concern over sharing of this type of information directly with the airport.

The best method to manage this type of situation is not clear. Generally, the tenant possesses the employee data and the airport owns the ACS data. Both the airport and the tenant need to access the other's information in order to identify potential red flags for risk mitigation.

Some airports allow tenants to request reports of activity over a specified period of time for active airport-issued badges. This activity monitoring is often performed in conjunction with badge auditing, and allows the tenants to manage their employees' unescorted access privileges and eliminate badges for terminated employees. These reports help companies exercise better accountability over their employees' badges; some airports actively facilitate access to this type of data.

Most airports expressed concern over releasing ACS data for reasons other than legitimate security interests. Several airports indicated that requests for ACS were often from an employer monitoring employee time records or in connection with disciplinary investigations. Many airports noted that airport ACS data was not designed as a timekeeping tool for airport stakeholders. Given the sensitivity of ACS data from both a security perspective and its relationship to PII, the sharing of that data requires a legitimate security need on the part of the requester.

1.4 Event and Emergency-Related Information

Information flow during events and emergency incidents is complex and dynamic. Many airport stakeholders and a wide range of external partners may be involved in the response depending on the scope of the incident. Further, the information is constantly changing as security updates are sent and threats and risks emerge.

1.4.1 Emergency Communication Processes

It is difficult to overstate the importance of prior coordination for real-time information sharing with adjoining law enforcement agencies and other first responder organizations. These organizations are critical partners in responding to major events and incidents at airports. Advance planning for information flow will ensure the response is well-coordinated, which includes the implementation of concepts such as Meta-leadership, discussed in Section 3.9. Pre-event work to establish relationships improves cross-entity information sharing and collaboration during emergencies.

Where possible, paths and processes for information sharing should be set out in mutual aid agreements and shared contingency plans. Having formal agreements in place assists in addressing what sensitive information each party will share, whether that information will be shared in advance or after a triggering event, and how parties should execute the information sharing. These agreements will mitigate concerns related to sharing SSI, PII, and sensitive business information during high-pressure events.

The active shooter incident at Fort Lauderdale–Hollywood International Airport (FLL) in 2017 highlights the critical need to create information sharing processes with law enforcement and other responding agencies before emergency incidents.[8] The incident's after-action report emphasizes FLL's lack of processes and supporting technology to enable information sharing, which hindered the airport and first responding agencies when coordinating their response. The report stresses the need for airports to develop processes and deploy communications technologies that are compatible with supporting agencies.

As far back as the findings of the 9/11 Commission Report, it has been clear that information sharing is an important element of successful emergency response and recovery practices.[9]

[8] Fort Lauderdale–Hollywood International Airport, *Active Shooter Incident and Post-Event Response January 5, 2017: After-Action Report*

[9] ACRP Synthesis 60: *Airport Emergency Post-Event Recovery Practices*

1.4.2 Organizational Structures and Facilities for Information Sharing

Information sharing improves by introducing separate information streams and different operational groups and systems into common workspaces. With the advent of technology platforms to support information sharing, an increasing number of airports have developed centers to leverage this technology. These can take the form of small operations and security dispatch centers in office space at CAT II and III airports, or large, off-site facilities at CAT X airports. Example operations include AOCs, Security Operations Centers (SOC), Public Safety Answering Points (PSAP), Integrated or Combined Operations Centers (IOC/COC), and Emergency Operations Centers (EOC).These organizational structures can also use virtual locations.

The case study attached as Appendix B presents examples of the types of technology commonly used to support operations in one of these centers. More in-depth information on planning and designing communication centers can be found in PARAS 0043 – *Guidance for Security Operations Center Planning and Design*[10] and ACRP Report 182 – *Design Guidance for Planning, Design, and Operations of Airport Communications Centers*.[11]

In addition to these more permanent facilities and information-sharing arrangements, temporary tactical sharing arrangements are commonly established during incidents or events. These Incident Command Posts (ICP) are established in accordance with the National Incident Management System (NIMS). In many airports, ICPs can be created around temporary structures or command vehicles that have specialized communications equipment. ICPs allow for the coordination of the activities of first responders and supporting personnel during major incidents or events. They are generally established close to the scene of an event or incident. Guidance documents and training materials and programs on NIMS are available to airports through FEMA.

AIRPORT OPERATIONS CENTER

Traditionally, the main focus of an AOC is the day-to-day operations of an airport and occasional emergency and incident response activities. The AOC is typically a 24/7/365 operation in larger airports. While the information shared in these centers has security value, the focus on information sharing is not on security-related issues.

SECURITY OPERATIONS CENTER

Generally, SOCs perform two principal functions. First, they serve as a platform to collect information from a range of sources to provide situational awareness for command personnel. Second, they serve as a platform for the exercise of command and control over the allocation and deployment of security resources and capabilities. SOCs are often designed to monitor alarms, CCTV cameras, and the ACS.

These centers routinely work with SSI and CJI.

PUBLIC SAFETY ANSWERING POINT

PSAPs receive and process emergency calls and event notifications for a specific area. These facilities dispatch public safety personnel such as police, fire, and emergency medical services (EMS) in response to calls for service. Many PSAPs fall under the SOC’s operations, but some airports separate operations, even where centers are collocated.

[10] **PARAS 0043:** https://www.sskies.org/images/uploads/subpage/PARAS_0043.SOCPlanningDesign_.FinalReport_.pdf
[11] **ACRP Report 182:** https://crp.trb.org/acrpwebresource2/guidance-for-planning-design-and-operations-of-airport-communications-centers/

INTEGRATED OR COMBINED OPERATIONS CENTER

IOCs and COCs combine the functions of an SOC and an AOC into a unified center. These centers are found predominantly in larger airports. The multidisciplinary nature of these centers facilitates rich information sharing with airport stakeholders.

Airports utilizing this type of organizational structure must ensure that security information is properly protected and only accessible by properly trained individuals with a need to know.

One CAT X airport provides all personnel working in the IOC with CJIS training to help address concerns over unauthorized access. The physical layout of the IOC was also adjusted to separate areas where security information is processed to guard against unintentional disclosure.

At that airport, the IOC serves as a focal point for decision making on a wide range of security, non-security, and emergency issues. When a non-emergency event or incident occurs, the managers of affected departments and operational areas convene an informal meeting at the IOC to decide on a course of action. This meeting may result in the creation of a task-organized team within the IOC or activation of the airport's EOC to address concerns.

EMERGENCY OPERATIONS CENTER (EOC)

An EOC's primary focus is on managing emergencies and crisis events. An EOC may be a temporary, pop-up facility or it may a permanently established facility, often near the SOC/AOC, that is typically unoccupied until it is activated by a triggering event.

SECTION 2: SHARING SOURCES

Airports provide information to and receive information from a variety of stakeholders. Primary sharing sources include federal partners; aviation industry associations and organizations; airport internal partners; and global, regional, state, and local partners.

By sharing information with stakeholders, airports can incorporate multiple perspectives into their security programs, creating a more robust security posture. Additionally, information sharing within the airport community strengthens the security culture as stakeholders begin to think in a more security-conscious way. Sharing information facilitates relationship building, strengthens readiness for emergency response events, educates stakeholders, and creates partnerships to foster collaboration.

The following sections discuss many airports' security-related stakeholders, their relevance to airport security information sharing, and examples of information they may be able to share with airports or that airports can provide them.

2.1 Federal Partners

Federal agency partners are often airports' main sources of security intelligence and information. Some of these agencies also create and enforce security requirements and recommended practices. Airports regularly receive intelligence reports, operational information, and compliance information from their federal partners, as well as emergency and incident information.

2.1.1 Transportation Security Administration

TSA is airports' most significant resource for security information and intelligence. TSA headquarters provides high-level policy guidance and intelligence reports from national and international perspectives.

TSA's Intelligence and Analysis office has Field Intelligence Officers (FIO) assigned to every major airport in the US. FIOs liaise with members of the airport community in order to share key security information and intelligence and provide security briefings, including recent global and domestic security incidents and notable trends that may impact aviation security.

Some airports indicated that their airport law enforcement agency often receives threat and incident information from their TSA Assistant Federal Security Director – Law Enforcement. Airports may be able to leverage this relationship to open more security information–sharing channels.

TSA-HOSTED CALLS AND BRIEFINGS

TSA headquarters engages with airport operators monthly through its National Airport Stakeholder Call hosted by TSA's Policy, Plans, and Engagement office. These calls address airport policy concerns and priorities, checkpoint operations, compliance concerns, and a multitude of other matters relevant to airports. TSA elicits topics from the airport associations, encourages airport operators to request specific topics be covered, and opens the floor for discussion. Attendance on the monthly call continues to grow. Some airports reported better engagement with their local TSA agents after inviting them to participate on the call.

Occasionally, TSA hosts ad hoc airport stakeholder calls to address specific policy concerns. For example, TSA hosted stakeholder calls to address the implementation of Rap Back, ID media accountability policy changes, and the implementation of TSA's Centralized Revocation Database. The calls assist airports in understanding TSA's regulations, and help the TSA better understand the differing needs of airports.

TSA REPORTS AND ASSESSMENTS

TSA disseminates a variety of intelligence reports, including the Transportation Intelligence Note (TIN), which provides information or analysis on a single topic or issue. TINs are distributed to TSA officers and transportation security partners at the classified and unclassified levels.

The monthly Global and Regional Intelligence Digest (GRID), formerly the Transportation Suspicious Incidents Report, includes a summary of incidents, suspicious activities, and surveillance directed against transportation modes. It also includes regional and global trend analyses. The GRID is available to transportation security personnel through email and secure web-based portals.

Other assessments provided by TSA include threat analyses, targets and tactics, and a review of vulnerabilities. These documents are produced at the classified and unclassified levels and cover:

- Annual modal threats
- Special event threats
- Tactics, techniques, and procedures
- Semiannual current airport threats
- Cities and Airport Threat Assessment
- Transportation Sector Security Risk Assessment

TSA SHARING PLATFORMS

TSA utilizes its Transportation Security Information Sharing and Analysis Center, hosted on DHS's Homeland Security Information Network (HSIN) platform, to share unclassified and SBU information, including SSI. TSA also utilizes its Aviation Web Boards to post regulatory and policy documents and other security-related information. More information on HSIN and the Aviation Web Boards can be found in Section 4.4.1.

TSA's Intelligence and Transportation Sectors Network Management office sends infrequent emails to transportation organizations that include unclassified and SBU security-related information, such as known or suspected threats and vulnerabilities.

TSA INDUSTRY ENGAGEMENT AND THE AVIATION SECURITY ADVISORY COMMITTEE

TSA also engages with the aviation community through aviation industry associations and groups. TSA leverages these resources to disseminate and gather information when they are considering regulatory or operational changes. TSA representatives regularly attend association meetings to speak on current security issues and topics.

TSA also engages airport stakeholders and the broader aviation community through the Aviation Security Advisory Committee (ASAC), a statutory committee composed of individual members representing private sector organizations affected by aviation security requirements. The TSA Administrator appoints individuals to represent key constituencies (e.g., airport operators, airlines, general aviation, aircraft manufacturers, private organizations, etc.), which provides a balanced perspective and subject-matter expertise from across the aviation network. The ASAC receives taskings from TSA and Congress to conduct research on a broad range of aviation security matters and develop recommendations based on that research. The ASAC also advises the TSA Administrator on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives.

This advisory body is built on effective information-sharing practices across constituencies, cooperation between the various ASAC subcommittees, and collaboration between government and the private sector.

2.1.2 US Customs and Border Protection

CBP does not typically share operational information with airports, and many airports indicated they receive relatively little security information from them. When information is shared, CBP usually protects it with the LES designation.

Airports that regularly engage with CBP indicated more effective information-sharing experiences. Airports with FIS facilities have established links with CBP for approval of the custom seals that badge holders need to access the FIS areas. These airports also engage with CBP to establish or enhance CCTV coverage of the FIS. However, unlike the TSA, the CBP mandates that cameras within FIS areas must operate exclusively under CBP control.

CBP can benefit significantly from airport operational information that might affect passenger numbers or flow, such as terminal maintenance issues or other activities in the airport. This information can help create operational efficiencies for CBP by allowing them to plan staffing requirements based on anticipated demand.

2.1.3 Federal Aviation Administration

While most airports indicated that the FAA is an important information-sharing partner, most of that centers on operational information in support of airport emergency planning. The major FAA guidance on this topic comes through FAA Advisory Circular “Airport Emergency Plan.”

With the growing focus on unmanned aircraft systems (UAS) and counter-UAS operations, as well as the advent of Advanced Air Mobility (AAM)/Electric Vertical Take-off and Landing (eVTOL) aircraft, the FAA is growing as an operational security partner and source for security-related information. The FAA is a member of the ASAC subcommittee that is facilitating the emergence of AAM/eVTOL as a new mode of air transportation and addressing security and operational implications and issues.

Many airports indicated that FAA representatives attend stakeholder meetings, and that they participate in security exercises and are typically included in emergency responses to incidents, diversions, and disruptions.

2.1.4 Federal Bureau of Investigation

Although the FBI has no direct control over airports, the agency often gathers important security information affecting the aviation industry. The FBI disseminates their information with airport stakeholders in the following ways.

FBI AIRPORT LIAISON AGENTS

All TSA-regulated airports are assigned FBI airport liaison agents through the Civil Aviation Security Program (CASP), which is part of the FBI’s Counterterrorism Division. Airport Liaison Agents are task force agents or special agents. The CASP program was designed to enhance response to aviation-related threats, assist with joint FBI-airport threat and vulnerability assessments, and facilitate interaction between the FBI and private-sector stakeholders at airports.

Airports indicated that FBI agents are more likely to attend security meetings at airports where they are stationed. In instances of off-site liaisons, which is far more common, a liaison's attendance is more on an occasional or "as requested" basis.

FBI JOINT TERRORISM TASK FORCE

At some larger airports, FBI agents are stationed at the airport as part of the Joint Terrorism Task Force (JTTF), a multi-agency partnership including federal, state, and local law enforcement agencies responsible for investigating terrorism (domestic and international) and terrorism-related crimes.

JTTFs are operational units that conduct field investigations of actual or potential terrorist threats. At airports, they are typically composed of a variety of federal, state, and municipal LEOs who exchange interagency information to further terrorism investigations. Airports with an on-site JTTF noted that it facilitates relationship building, collaboration, and information sharing between the law enforcement community and the airport/aviation community.

Most airports reported receiving information from JTTFs, mostly through local law enforcement agencies participating in or linked to a JTTF. Airports should consider working with their local law enforcement stakeholders and assigned FBI liaisons to develop links with their JTTF.

FBI INFORMATION-SHARING PROGRAMS

Information from the FBI may be accessible to airports, directly or indirectly, through two FBI information-sharing programs:

InfraGard

InfraGard enhances information sharing among security professionals across sixteen areas of critical infrastructure, including aviation. There are currently over 50,000 InfraGard members. The program is open to individuals who have been employed in critical infrastructure for at least three years, who meet citizenship requirements, and complete an application that includes policy and privacy agreements. Membership benefits include:

- FBI and DHS threat advisories, intelligence bulletins, analytical reports, and vulnerability assessments
- Invitations to regional and national InfraGard events
- FBI and other government agency presentations to InfraGard chapters at member events
- Direct engagement with the FBI and other government agencies and private-sector experts at the local level
- Admittance to a members-only web portal that provides access to FBI intelligence and opportunities to collaborate and share assessments and critical infrastructure–protection information
- Opportunities to attend training events and briefings held by the FBI and its law enforcement partners
- Access to thousands of subject-matter experts within critical infrastructure to share real-time threat information

Domestic Security Alliance Council

The Domestic Security Alliance Council (DSAC) is a strategic partnership program between the FBI, DHS, and private-industry partners. This initiative is modeled after the Overseas Security Advisory Council, and enables two-way flow of vetted information between the FBI and participating members to prevent, detect, and investigate threats impacting US businesses and economic and national security.

In 2022, the DSAC website reported a membership of more than 600 partners.[12] The organization is only open to for-profit organizations, excluding airports from participation. Airports should work with DSAC stakeholders to stay aware of potentially relevant security information.

In interviews, at least one airline cited DSAC as a valuable resource for sharing security intelligence and information. It also affords access to a members-only website that hosts many resources, including:

- Liaison information reports – FBI analyst reports on a range of threats
- FBI and DHS intelligence reports
- DHS daily component reports – significant operational activities of DHS component entities, such as US Immigration and Customs Enforcement (ICE), CBP, TSA, etc.
- FBI counterintelligence newsletter
- NCIC Weekly Analytic Synopsis Product
- Member and expertise locator – networking tool for member sharing

2.1.5 Department of Homeland Security

DHS oversees eight agencies that have relationships with airports: CBP, Secret Service, TSA, FEMA, Coast Guard, Citizenship and Immigration Services, ICE, and Cybersecurity and Infrastructure Security Agency (CISA). DHS is a significant source of security intelligence for airports, although the majority of this information is filtered through the TSA.

CISA

CISA was established in 2018 to lead US efforts to "understand, manage, and reduce risk" to cyber and physical infrastructure. It serves as an information clearinghouse for intelligence threats and system vulnerabilities. CISA engages with government, private, academic, and international partners to gather information to address threats to critical infrastructure.

CISA maintains their CISA Services Catalog, which outlines the services they offer, many of which are provided at no cost to participating organizations.[13] Services include assessments, tabletop exercises, analyses, testing, and information-sharing opportunities. CISA's website also hosts a range of bulletins and informational resources, many of them open source.[14]

A 2022 National Amendment (TSA-NA-21-05) requires airports to report cybersecurity incidents to TSA and CISA and to designate personnel to receive CISA notifications. This new reporting

[12] **DSAC.gov:** https://www.dsac.gov/

[13] https://www.cisa.gov/publication/cisa-services-catalog

[14] https://www.cisa.gov

requirement is intended to enhance information sharing regarding cyber and infrastructure threats and vulnerabilities in the aviation sector.

2.1.6 Office of the Director of National Intelligence

The Office of the Director of National Intelligence (ODNI) reports to the President of the United States and performs a critical role as the head of the US Intelligence Community. Every year, the ODNI works with DHS and TSA to solicit feedback from critical infrastructure sectors, including aviation, on their top five intelligence needs. ODNI then attempts to address this feedback to improve intelligence sharing.

2.1.7 Department of Defense

Department of Defense (DOD) information is not routinely utilized by airports. The only airports that indicated having access to DOD-related information were airports with collocated National Guard facilities. The information they receive is primarily related to the security of those DOD-related operations.

2.1.8 Department of State

The Department of State (DOS) publishes a wide range of open-source, travel-related information. The DOS uses classified and unclassified government resources and open-source information to assess threats and offer analysis reports, benchmarking, briefings, and one-on-one consultations.

The DOS established the Overseas Security Advisory Council (OSAC) to enhance information sharing. OSAC manages regional and country chapters and provides centralized research and analysis functions. Country chapters meet regularly to share information with the DOS country teams. The OSAC maintains a website with a variety of resources, some of which are accessible to the public while others require OSAC membership.[15]

Anyone may become a limited-access OSAC member. Full-access membership is limited to employees of OSAC-approved organizations or US law enforcement, government, or military personnel. There is an application process through which full-access applicants are vetted.

OSAC also has interest communities, including one for aviation, for organizations with similar international operations. Most of the major airlines is an OSAC member and reports substantial use of OSAC resources. Airports should develop relationships with OSAC member organizations or personnel to keep informed of relevant OSAC resources and information.

2.1.9 Aviation Domain Intelligence Integration and Analysis Cell

The Aviation Domain Intelligence Integration and Analysis Cell (ADIAC) is a partnership between federal agencies and the aviation private sector that serves as a central institution and repository to facilitate intelligence sharing relevant to the Global Aviation Community of Interest. TSA is the lead agency operating the ADIAC with the support of the ODNI, DHS, and the Aviation Sector Coordinating Council.

[15] https://www.osac.gov/

ADIAC members include government agencies, industry organizations, global airlines, and US airports. Currently, only a small percentage of airports are members.

This organization receives intelligence from the Intelligence Community and other federal agencies. Six agencies produce the majority of releasable intelligence: TSA Intelligence and Analysis, DHS Intelligence and Analysis, FAA, FBI, CBP, and DOS OSAC. That intelligence is shared with ADIAC members through ODNI's Structured Analytic Gateway for Expertise (SAGE), DHS's HSIN, and via daily virtual meetings.[16]

ADIAC also offers classified On-Site Intelligence Industry Days, which are one-day training sessions that provide education on special topics and share threat intelligence with participants.

Relevant intelligence and information are shared with members and partners at the lowest possible classification level and to the widest extent possible. ADIAC requires individual participants to be a US citizen and possess a Secret Clearance or higher.

2.2 Aviation Industry Associations and Organizations

Aviation industry associations and organizations are dedicated to sharing information between airport stakeholders, government, and global entities, although this information covers all operations and not just security. Industry associations interact with regulators and lawmakers to advocate for their constituents. Most of these associations and organizations host regular meetings and annual conferences to educate their members and share aviation information.

2.2.1 Airport Associations

Airport industry associations play a major role in information sharing. They facilitate communication between airports and federal agencies, airlines, and other industry stakeholders. They often work with legislators to advocate for policy changes on behalf of the airport community. These associations also work with the Intelligence Community to receive relevant information.

There are two major airport associations in the United States: Airports Council International – North America (ACI-NA) and American Association of Airport Executives (AAAE). Both associations focus on providing advocacy, services, and resources for US airports and airport-governing bodies of all sizes. They facilitate committee meetings and working groups that discuss security, technology, and cybersecurity topics, among many others. These two associations work closely with airports, federal partners, global partners, and other industry associations to create open information-sharing channels. Members are given information through annual conferences and email distribution lists created for specific areas of interest.

ACI World represents airports at the global level. The association fosters information sharing through coordination of regional committees, conferences, working groups, and reports. Further, ACI World represents airports at International Civil Aviation Organization (ICAO) meetings. ACI World is one of only a few organizations that have "observer status" with ICAO. This provides access to some of their information-sharing forums and invitations to some ICAO meetings. Representatives from US airports serve in leadership positions on the ACI World Security Standing Committee, which allows them to share ideas and practices and facilitate information sharing on an international level.

[16] See Section 4.4.1 for more information on SAGE and HSIN

2.2.2 Airline Associations

Airlines for America (A4A) works with multiple stakeholders and government agencies on behalf of its airline members. Airports are not permitted to join, but all the major airlines and most smaller carriers are current members. This association shares security intelligence and information with its members, and members will often share that intelligence with airports.

The Regional Airline Association (RAA) represents North American regional airlines and the suppliers of products and services that support the regional airline industry. Membership is exclusive to these entities. The association advocates for its members before Congress, FAA, DOT, and other federal and state agencies. RAA's support network connects regional airline partners, industry business partners, and government regulators to share best practices and promote airline interests in changing policy. Members are provided with security and operational information and webinars, and are invited to the annual convention. Membership is exclusive to regional airlines, suppliers, and service providers.

The Cargo Airline Association (CAA) actively supports and fosters relationships between cargo airlines, aviation industry partners, and policymakers. CAA publishes periodic newsletters for its members on new policies and other relevant updates. Airports are permitted to join this association.

International Air Transport Association (IATA) is a trade association representing airlines at the global level. The association advocates on behalf of their members to country regulators and governments and creates process standards. IATA collaborates with airports worldwide and offers some services and resources to them, but the association's focus is on airlines.

One major US airline reported extensive participation in organizations such as DSAC, OSAC, and A4A. The airline's security personnel also participate in the International Security Management Association, an invitation-only organization. The networking and information gained from these associations and organizations was deemed invaluable.

2.2.3 Airport Law Enforcement Associations

Airport Law Enforcement Agencies Network (ALEAN) serves as a knowledge repository, information-sharing channel, and advocate for law enforcement agencies that provide airport support. ALEAN members are vetted, and membership is restricted to airport law enforcement personnel.

Airports with law enforcement officers serving in security leadership positions could benefit from membership in ALEAN as the association provides its members with specialized training and intelligence briefings. ALEAN offers a range of information-sharing channels to its members, including:

- Biannual conferences where presentations are offered on a range of security-related topics such as response to active shooter incidents, dealing with unruly passengers, human trafficking, response to bomb threats, etc.
- A monthly investigations call where current investigatory information is shared on matters confronted by local airport law enforcement.
- A members-only web portal where bulletins of law enforcement interest, contact information for airport law enforcement agencies, and other resources are posted. ALEAN also uses the portal to issue surveys on topics of specific interest.

- Notification systems that send out email notices and bulletins of significant importance to ALEAN members. These include an email notification system designed for command members and a separate forum for investigative personnel.

Airports can access information created and circulated through ALEAN through their assigned law enforcement personnel.

2.2.4 Aviation Information and Analysis Sharing Center

Founded in 2014, the Aviation Information and Analysis Sharing Center (A-ISAC) is a private organization that facilitates information sharing among members, aviation associations, cybersecurity agencies, and third-party analysts. Members include airport operators, airlines, and other aviation industry stakeholders from twenty-one countries.

The organization hosts a secure threat intelligence platform for members to access intelligence reports and newsletters, educational and training materials, and forums. It has working groups focused on network security architecture, product security, airport technology, compliance and third-party risk, threat actors, and fraud. The A-ISAC also holds an annual conference.

2.3 Global, Regional, State, and Local Partners

There are many information-sharing partners and resources at the global, regional, state, and local levels that airports can leverage to receive information.

2.3.1 International Civil Aviation Organization

The International Civil Aviation Organization (ICAO) is the United Nations' aviation agency. It is funded and directed by 193 national governments. ICAO works to create air transportation policies, standards, and recommendations for international civil aviation. Membership is only available to countries (member states), but anyone can purchase the standards and recommendations documents on the ICAO web store. TSA, FAA, and aviation industry associations and organizations implement and comply with ICAO standards as appropriate.

2.3.2 Fusion Centers

At the regional, state, and local level, considerable information-sharing duties are performed by fusion centers. In the wake of 9/11, fusion centers have sprung up across the country to enhance information sharing. They are present in every state as well as some territories and larger metropolitan areas. As of 2023, the DHS website identifies eighty fusion centers operating in the US and its territories.[17]

Like JTTFs, fusion centers facilitate information sharing among federal, state, local, and tribal partners. They collect information and have trained analysts that evaluate the information for intelligence value. However, they generally have a broader focus for law enforcement-related sharing.

One CAT II airport reported successful sharing of information with the state's fusion center in connection with a gang-oriented operation of catalytic converter thefts in airport parking lots.

[17] https://www.dhs.gov/fusion-center-locations-and-contact-information

DHS reports that fusion centers offer a range of products and services within their jurisdictions including:

- Responses to Requests for Information
- Situational awareness products – reports on developing events or incidents
- Bulletins – criminal threats, incidents, potential terrorist threats
- Intelligence bulletins – reports on specific or imminent threats
- Advisory notifications – cyber and physical security incidents and trends
- Threat assessments
- Risk assessments

It is possible that fusion centers are underutilized because they are not airport focused. While many interviewees indicated they use JTTF information, fusion center collaboration was much less frequently referenced. The comparative chart below, prepared by DHS, suggests that airport outreach to fusion centers might be beneficial.

Table 3-1. Fusion Centers vs. JTTFs

Fusion Centers	JTTFs
Focus on terrorism, criminal, and public safety matters in support of securing communities and enhancing the national threat picture.	Focus primarily on terrorism and other criminal matters related to various aspects of the counterterrorism mission.
Receive, analyze, gather, produce, and disseminate a broad array of threat-related information and actionable intelligence to appropriate law enforcement and homeland security agencies.	Conduct counter-terrorism investigations and provide information for assessments and intelligence products that are shared, when appropriate, with law enforcement and homeland security agencies.
Owned and operated by state and local authorities and include federal, state, local, tribal, territorial, and private sector partners from multiple disciplines, including law enforcement, public safety, fire service, emergency response, public health, and critical infrastructure.	Multi-jurisdictional task forces managed by the FBI and include other federal and local law enforcement partners which together act as an integrated force to combat terrorism on a national and international scale.

Source: DHS, Fusion Centers and Joint Terrorism Task Forces[18]

2.3.3 Local Law Enforcement Agencies

Threats occurring off airport property or at airports without a dedicated police force also require coordination and information sharing with law enforcement in surrounding jurisdictions. Local law enforcement may be needed to address threats such as man-portable air-defense systems, lasers, and drones. Information sharing with surrounding jurisdictions is a growing necessity. Federally sponsored joint assessment programs that examine threats emanating from jurisdictions surrounding the airport may serve as a basis for extending information-sharing activities.

[18] https://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces

2.3.4 Informal Organizations

In addition to formal organizations, the airport community has also developed some informal or ad hoc organizations. These organizations started organically, often in response to specific operational concerns or a perceived need for more focused sharing. As these organizations expand, they sometimes gain support from larger, more established industry organizations, such as AAAE or ACI-NA. The informal nature of these organizations reduces the potential barriers to entry for some smaller airports, such as membership fees. However, the reliance on donated resources (staff time and infrastructure) can make sustained information sharing difficult.

SEADOG AND WESTDOG

Two examples of successful informal organizations that gather on a regular basis are the Southeast Airports Disaster Operations Group (SEADOG) and Western Airports Disaster Operations Group (WESTDOG). These are regional groups of airports that have created airport-to-airport mutual aid programs for disaster recovery. Membership is open to all airports in their designated region. SEADOG maintains an active social media and internet presence, particularly during hurricane season. It also maintains a community hub presence on their website.[19]

SEADOG's and WESTDOG's primary goal is to organize voluntary airport support for airports experiencing catastrophic damage. During severe weather incidents, such as hurricanes, the groups use notification software to provide regular updates. The groups operate without full-time staff, which is often a limiting factor. For more information on SEADOG and WESTDOG, see ACRP Report 73: *Airport-to-Airport Mutual Aid Agreements*.[20]

AD HOC AIRPORT MEETINGS

Many airports have informal meetings, calls, or email groups with nearby airports to share and discuss region-specific security and operational information. These are seldom scheduled and tend to occur when one of the participating airports receives relevant information or experiences an emergency event.

> One CAT I airport and three nearby small airports began a monthly, informal information-sharing conference call for their ASCs. The initiating airport felt they lacked the resources necessary to attend some of the national trade organization calls and conferences. About forty airports across the country now participate in the call and topics are organized around the ASCs' interests. The call serves as a forum for ASCs to share information that would otherwise be out of reach for some airports.

2.4 Airport Internal Partners

An airport's internal partners include tenants leasing space on airport property (airlines, law enforcement, cargo operators, concessionaires, etc.) and the multiple departments responsible for creating or enforcing security policies and regulations.

2.4.1 Airlines

Airlines are regulated entities with federal transportation security requirements similar to airports, which often results in airports feeling comfortable with sharing information with their airline tenants. Information and intelligence from airlines can also be very important for airports. Airlines have a

[19] https://seadogops.com/

[20] **ACRP Report 73:** https://nap.nationalacademies.org/read/22754/chapter/1

nationwide and global perspective on the aviation security posture, and often partner with other airlines for an even larger intelligence network. However, while most airports indicated that airline stakeholders were important sharing partners, few airports indicated receiving significant amounts of information from the airlines.

Major airlines receive information and intelligence from the US government, foreign governments, and non-governmental sources. Corporate-level security personnel for the major airlines communicate with each other weekly and sometimes daily. They often share information concerning measures taken in response to common threats. Much of the information managed by airlines is Secret, so airline personnel maintain varying clearance levels and have infrastructure and processes in place to handle classified information. At the corporate level, most airlines utilize Secret communication channels such as secure telephone units and Secured Internet Protocol Router Network (SIPRNet) access terminals. This equipment is rarely available for airport security operations.

Airlines' sources often limit their permission to share information, and airlines are concerned about providing information directly to airports as it may compromise the terms under which the information was received. Airlines are also concerned that an airport might receive inconsistent information or become overwhelmed if they receive information from multiple airlines instead of from the authoring federal agencies. Building relationships with management at local stations and company headquarters, and setting up formal and informal processes for sharing information can help overcome these concerns and facilitate access to valuable security information and analysis.

2.4.2 Authorized Signatories

TSA's National Amendment 19-02 defines the authorized signatory's role as a "representative authorized to sponsor individuals, collect and transmit biographical data to the airport badging office, and request airport ID media for sponsored individuals." This definition limits the signatory's role to badging office–related operations. However, airports often communicate with their tenants' authorized signatories to share relevant security information with the company's headquarters and their shift employees.

While not their primary function, the authorized signatories typically serve as the company's point of contact with the airport. Many airports routinely send relevant emails or notifications to authorized signatories with the expectation that the information will be pushed to the shift employees. Strong relationships with authorized signatories are important to build trust and encourage two-way communication on security issues.

Airports using authorized signatories as a communication channel need to be mindful of the fact that these individuals may not be executives or high-level employees in their companies, so their ability to direct action based on shared security information may be limited. Communication through the authorized signatory is not a substitute for direct communication with company management. However, it may supplement other information-sharing strategies.

2.4.3 Intelligence Roles

A small number of airports have appointed dedicated intelligence analysts to gather, review, and share information from a variety of sources. Ideally, these individuals would be police officers at the lieutenant level or higher with a Secret clearance to afford access to more information sources and channels. Airports that created dedicated intelligence positions indicated that the individuals are responsible for managing federal level intelligence and LES, including BOLO and FOUO; analyzing local, state, federal, and global level threats and trends; providing briefings to airport leadership; and hosting badge-holder trainings.

A dedicated intelligence role or a team of intelligence analysts benefits an airport by providing solid intelligence, threat analyses, and supporting information for security-related business decisions. However, most airports reported lacking the necessary resources to maintain dedicated intelligence personnel.

Unlike most airports, major airlines have a significant budget and personnel resources for intelligence and information sharing and processing at the corporate level. Airlines routinely recruit security intelligence professionals from government organizations such as DOS, FBI, and US Secret Service to serve in their internal security, intelligence, and information-sharing infrastructure. The networks and trust relationships of those individuals gathered over years of public service are seen as valuable assets to airline security–information gathering. These individuals were often recruited through organizations such as the DSAC and OSAC. Hiring security professionals with intelligence backgrounds may help airports open more communication channels for information sharing.

One major airline reported having over one hundred personnel assigned to information analysis and intelligence in the immediate wake of 9/11. While that number has been reduced, it emphasizes a significant commitment to information collection, processing, and sharing that is common among major airlines.

Many airlines contract with private intelligence organizations to receive overflight information and relevant intelligence. Airports may contract a third-party intelligence vendor to provide them with security intelligence, but most airports indicated that they did not have the budget to contract these vendors. They could also collaborate with airlines to share intelligence that may affect them.

Another major airline reported using third-party intelligence vendors to help them make security and business decisions. They use multiple vendors who each provide a different type of intelligence, including overflight, flight routes, and global security intelligence. The airline has a dedicated budget for these vendor contracts.

2.4.4 Airport Law Enforcement

The nature of the relationship between the airport security department and the airport's law enforcement agency will have a significant impact on the success and efficiency of information-sharing efforts.

Airports with a police force that operates independently of the security department, or that is not stationed at the airport (e.g., local or state police), may experience communication barriers as a result of the operational separation or physical distance from the airport. These airports should endeavor to include their police force in stakeholder meetings and meet regularly to discuss relevant security matters and build trust and familiarity.

Almost all interviewed airports indicated including law enforcement personnel in regular stakeholder meetings to share law enforcement–related security information with the airport community.

When a Chief of Police also functions as the ASC, the airport benefits from additional security channels only available to law enforcement entities. Police departments that work in conjunction with the airport security department may also be able to provide this benefit, but if the ASC is not a LEO they will not have direct access to law enforcement CJIS platforms, such as NCIC and III.

CJIS is a national sharing program operated by the FBI that provides access to several information systems commonly utilized by airport law enforcement as part of their routine responsibilities. Information inquiries are run through the FBI's NCIC and a number of state and international criminal justice databases, such as driver's license and vehicle registration records, and International Criminal Police Organization (INTERPOL).

This information can only be utilized by law enforcement officers for law enforcement–related purposes. Officers are required to take user training and log into the system with a unique username and password. Inquiries will require information on the case being investigated, and law enforcement agencies are routinely audited to ensure compliance with the system's security requirements.

2.4.5 Airline Service Providers

The employees of airport service providers represent a significant population at airports. They offer services such as air cargo processing, aircraft security, catering, deicing, fueling, and passenger services.

Airport service providers often perform work for domestic and international airlines, and must meet the training and operational requirements unique to each airline they serve, including compliance with the same federal, state, and local regulations. Corporate- or local-level management may receive reports of suspicious activities from their front-line workers. Building relationships with these managers can provide additional information channels.

Service provider companies may be members of the Airport Service Providers Association, which provides members with resources to improve operations, including security, and represents members before policy makers. Generally, this association does not share security information, except for compliance requirements, but they may have access to information not available to any other stakeholder.

2.4.6 Frontline Workers

Airports indicated that frontline workers of tenant companies and airport service providers produce little actionable information but are still valuable sources of security information on the activities occurring in the terminal, airfield, and public spaces. They are the most capable of recognizing suspicious or unusual activities occurring in the spaces they see every day. Airports could leverage this population's knowledge through engagement and reporting strategies.

Frontline workers are rarely invited to airport stakeholder meetings because there are so many individuals and there is a high turnover rate in the population. Engagement can be accomplished through emails, newsletters, posted notices, etc., but airports could also invite these individuals to engage in information-sharing and reporting programs to encourage open, two-way communication. Social media and mobile applications may make this type of communication easier to achieve. Some airports have enlisted technology solutions to improve engagement with these stakeholders.

2.4.7 Public

The public, including cab and limousine companies and rideshare companies, is also a valuable source of information. These individuals may observe suspicious behaviors or activities in fellow passengers or airport workers that could alert airports to potential threats. Additionally, videos and images captured by the traveling public during emergency incidents and events are often used for investigative and forensic purposes.

Some airports stated that it is difficult to engage with this population, and the information they provide is rarely actionable outside of disciplinary measures. Airports may find value in collaborating with their designated Public Information Officer (PIO) to craft information bulletins, newsletters, or press releases to share security information on the airport's website, social media platforms, and other public channels with the traveling public.

SECTION 3: BUILDING TRUST AND IMPROVING ENGAGEMENT

Trust and relationship-building are the foundation of collaborative information sharing. However, the lack of incentive to share and lack of trust are the biggest barriers to open communication in the aviation sector. The 9/11 Commission's Report highlights the reason many people choose not to share information is that "[t]here are no punishments for *not* sharing information." As a result, there is more incentive to hold onto the information than to share it. The 9/11 Report recommends enhancing sharing through incentivizing sharing behaviors and the development of trusting relationships.

By identifying the benefits of information sharing and creating incentives for participating in information-sharing programs, airports and their stakeholders will increase their familiarity with each other and build the trust necessary for effective information-sharing programs. Consistent with the findings and recommendations of the 9/11 Report, airports that engage their stakeholders and emphasize the important role stakeholders have in shaping the airport's security posture are more likely to see effective collaboration with all partners and discover more information-sharing channels.

Airports might consider the following strategies to encourage information sharing and build trust with their stakeholders:

- Invite stakeholders to security meetings
- Make security meetings and briefings more accessible
- Meet informally with stakeholders to gain trust and familiarity
- Facilitate security committees composed of airport stakeholders
- Offer additional training to badge holders and stakeholders
- Recognize those occasions where information sharing was shown to have successfully worked to create a good security result (e.g., a security breach foiled or a crime solved)

3.1 Cultivate a Need-to-Share Culture

Airports have varying information-sharing philosophies on the scale of need-to-know to need-to-share, often shifting depending on the situation. Airports universally agreed that ensuring all stakeholders have necessary information was important, but questions like what information was necessary for whom and how to achieve proper distribution of information were always concerns.

Many airports interviewed for this research stressed the importance of the need-to-share perspective, believing that it is critical for them to disseminate security information to operational teams as quickly as possible to inform their decision making and actions. Further, they believe educating the airport community enhances the airport's security posture by fostering engagement and creating a two-way feedback loop.

Some airports indicated that the need-to-share philosophy has to be tempered by need-to-know requirements. In those cases, strategies have to be developed to share portions of the information they can while respecting need-to-know constraints. Section 4 highlights methods to respect these constraints.

Airports reported varying strategies addressing how much information to share. Some airports reported sharing all information they received as soon as they received it with the appropriate audience. Other airports expressed concern with unintentionally sharing information inappropriately based on the various federal information classifications and designations, or disseminating information without appropriate vetting.

Research findings from airports and government interviewees identified the institutional proclivity toward the need-to-know philosophy versus the need-to-share philosophy. However, these interviews also identified “invisible” barriers that exist within the aviation industry, both internally among the airport departments and tenants, and between the aviation industry and federal and law enforcement agencies. These barriers are rarely based on law or policy prohibitions and typically stem from a fear of inappropriately sharing security information or an unwillingness to share security information with others outside of their familiar network.

Agencies or individuals may hoard information under the guise of protecting and securing, but it can have detrimental effects on information-sharing strategies and practices. This dynamic is frequently referred to as “knowledge is power,” meaning that the information holder has more status or importance if they possess knowledge that no one else has or that others need.

3.2 Improve Timeliness of Sharing Information

One of the most common hurdles in information sharing reported by airports and airport stakeholders was the timeliness of the information. Often, airports will receive information from their stakeholders after it has graduated from a nuisance or minor issue to a security concern.

One CAT I airport was informed of reports of homeless individuals in the terminal making customers and crew members uncomfortable weeks after the first report. The airport believes they would have done more to mitigate the issue if they had known earlier.

Airports should look at their current information-sharing processes to determine if and why delays exist. For example, the approval process to release information may be an unnecessarily cumbersome, or stakeholder leadership may not be relaying messages to the frontline employees. Regardless, identifying and minimizing these barriers will improve the information-sharing processes. The solutions may require more frequent stakeholder meetings, visits with frontline workers to discuss issues, or the implementation of automated technology to push relevant information to stakeholders.

3.3 Conduct Robust Meetings

Conducting meetings is the universally preferred method for security information sharing in airports. This strategy is consistent with the goals of building trust and reinforcing security culture. Airports reported hosting a variety of meeting types with a range of frequencies.

INTERNAL AIRPORT STAFF MEETINGS AND BRIEFINGS

Internal communication is just as important to an airport’s security posture as communication with the airport’s stakeholders. Many airports host regularly scheduled department meetings. These meetings can be held on a weekly, bimonthly, or monthly basis depending on the airport’s size. Some airports indicated that they also hold internal department meetings at the beginning of the first shift every day and encourage the meeting participants to spread the information to their employees and other airport workers. It is common at airports of all sizes for the duty managers to share relevant, daily information during shift changes. This solution may work better in smaller airports and is less scalable to larger, more complex, airport operations. Most airport law enforcement agencies and operations staff routinely have roll call and operations briefings at the beginning of each shift.

While most these meetings focus on matters other than security, the security department, typically represented by the ASC, gives security reports and provides relevant airport security information. These meetings enable airports to demonstrate that security is a common responsibility within airports.

A small number of airports indicated that they hold short briefings with executive management to discuss relevant intelligence. These meetings are opportunities for security leaders to justify necessary security measures to the airport leaders.

STAKEHOLDER MEETINGS

The most common information-sharing strategy across all airport sizes is a regularly scheduled stakeholder meeting, either in-person or via a conference call or a virtual meeting. These are often referred to as tenant meetings. All airports interviewed hold at least one weekly, monthly, or quarterly meeting with their tenant stakeholders to discuss relevant topics, including security. It is common for the airport to host several of these meetings with different entities in order to share different levels of security information. For instance, meetings with all stakeholders will only discuss unclassified or non-SBU information, while a meeting with tenant airlines and TSA may include SSI topics. Sometimes these focused meetings are held before or after the larger stakeholder meeting. The airport should consider the time commitments of each option to ensure the stakeholders' time is being respected.

Stakeholder meetings should encourage participation of all appropriate stakeholder personnel, including frontline staff. This will help promote the overall security posture and culture at the airport. It is also a good tool to build stakeholder trust and sense of inclusion.

SECURITY MEETINGS

Some airports host narrowly focused meetings that specifically address security information, often referred to as security consortium meetings. At the core, they generally involve the airport's security department (usually represented by the ASC), the TSA, an FBI liaison, and the airport's dedicated or local law enforcement agency. In larger airports where there is a greater federal presence, these meetings can also involve FAA, CBP, ICE, US Department of Agriculture, DOS Diplomatic Security Service, US Secret Service, and the US Postal Service.

In one CAT X airport, the FBI agents assigned to the airport—rather than the ASC—hosts the security consortium meeting. The airport believes that this helps to ensure better federal participation in the meeting and access to a wider array of security information.

Consortium meetings offer the airport an opportunity to include other stakeholders, such as airport badge holders. Involving badge holders in security committees reinforces their role and responsibilities in securing the airport. Airports may consider including airport leadership in these meetings to show that the decision makers are participating in the community and listening to stakeholder concerns.

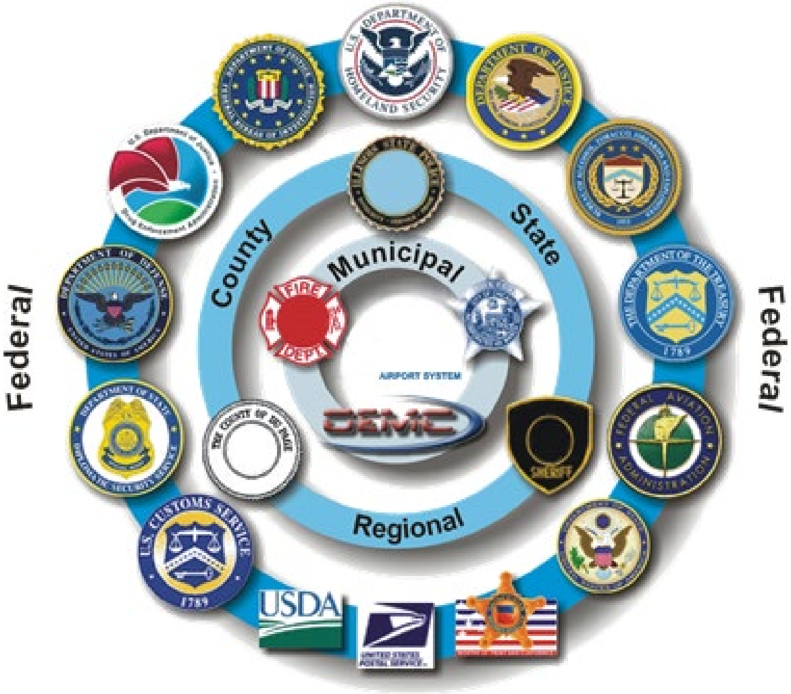
Consortium meetings typically discuss and establish security roles and responsibilities, along with processes and programs for information sharing. In many cases, the meeting participants form the basis for the operational structure that will be activated during an event.

One CAT X airport has created a security awareness consortium consisting of badge holders and LEOs. The security department encourages all badge holders to join. Typically, fifty to seventy participants join the meeting. Topics can include recurrent security violations, such as tailgating and piggybacking, failure to secure gates and portals, new security policies and measures, regulatory developments, and crime trends and threat information.

Several airports indicated that it was not uncommon for airline tenants to initiate meetings to address security challenges. These types of meetings more frequently occurred at airports reporting strong security cultures. In general, airports found that attending those meetings provided significant benefits, especially in viewing security from the tenants' perspective. In some cases, airports have not been invited to tenant-hosted meeting because the tenants did not think the airport would find the topics useful. Airports are encouraged to reach out to tenants hosting security meetings and request an invitation.

Ad hoc security committees are occasionally created when an airport has to manage a large event, for example the Superbowl, World Series, March Madness, Air Force One, or a national convention. In these instances, a meeting schedule is usually established for information sharing. Figure 3-1 depicts a security consortium for a major event at a CAT X airport.

Figure 3-1. Security Consortium for a CAT X Airport Event



Source: Chicago Department of Aviation

Some airports indicated hosting monthly meetings with their security consortiums. When the meeting involves a smaller core group, they are often scheduled immediately before or after the larger stakeholder meetings since the consortium members participate in the larger meetings as well. In cases where the security consortium is larger, they hold their meeting on a different day to promote more participation.

One CAT X airport has created the Insider Mitigation Assessment Program (IMAP) that includes a security consortium consisting of TSA, security personnel, police chiefs, airport directors, and federal partners. The IMAP consortium meets twice a year to discuss local, state, federal, and global threats.

INFORMAL MEET-AND-GREETS

Frontline workers have excellent information to share about daily operations and behaviors in airport terminals and restricted areas. However, airports do not include most frontline workers in stakeholder meetings, and many airports do not have strategies in place to regularly collect information from them. This often results in the frontline workers not knowing how to report suspicious activity.

One CAT X airport's ASC frequently walks through the terminal to introduce themselves to tenant employees. The ASC answers any security questions and encourages the employees to report any unusual activities or behaviors in the areas they work. The airport has seen increased participation in the reporting programs and fewer security violations. The airport also uses this as a training opportunity to answer security questions and reinforce security measures.

Meet-and-greets like these foster a positive security culture. Frontline employees have the highest turnover rates in the airport badged population. As employees leave, they are replaced with new individuals who need to know the proper channels to report concerns and other security matters. Regular meet-and-greets through the terminal and airfield by security leadership and personnel will continue to reinforce the airport's commitment to security and encourage participation from the airport workers.

3.3.1 Enhance Meeting Practices

Given the importance of meetings to the information-sharing process at airports, review of meeting practices is advisable. The suggestions below discuss some of the main concerns airports should examine as they attempt to address the effectiveness of meetings.

MEETING SCHEDULING

Most airports host weekly, monthly, or quarterly stakeholder meetings to discuss relevant security and operational matters. However, if airports notice trends of information not being received or delivered in a timely manner, airports may find value in more frequent meetings with agenda time allocated for stakeholders to discuss any security concerns they may have.

An added benefit to hosting more frequent meetings is that the agenda can be more tightly controlled with fewer topics, and the meetings can be shortened.

VIRTUAL MEETINGS

After COVID-19, many airports moved their stakeholder meetings to virtual platforms, which allow more individuals to participate, including personnel not on the same shift and those working from home.

Many video conferencing platforms offer options to secure the meetings and prevent unauthorized access or recording. For example, Zoom has a Government Federal Level III option that federal agencies use to discuss regulations, threats, and common security violations. However, this level of security is unnecessary for most airport communication. A more appropriate option may be a disclaimer or warning statement that requires acceptance before being allowed to join the meeting.

Some airports concluded that while attendance increased as a result of virtual meetings, they are uncertain as to the quality of attendee participation. Some airports reported that they require attendees to remain on camera and to ask or respond to questions during meetings to enhance participation. Tools that are typically included with virtual conference call systems, such as voting polls and chats, can also be used during the meeting to increase participation.

MEETING DURATION

The length of the meeting can have a significant bearing on the engagement of the meeting's participants. Studies have shown that shorter meetings result in more engagement.[21] Meetings that are less than 15 minutes long keep about 90 percent of the participants' full attention, while meetings longer than 45 minutes drop that attention down to 60 percent.[22]

ADIAC hosts daily ten-minute secure phone calls to update members on current threats and trends. The organization keeps the meetings short and focused on the topic to encourage its members to participate. ADIAC reports excellent engagement with its members.

While a 10-minute meeting may not be enough time to discuss all the relevant topics at a stakeholder meeting, a 25 to 30-minute meeting may be more appropriate, and could easily be broken down into a focused agenda.

MEETING AGENDAS AND MATERIALS

Using agendas to manage meetings is an excellent and simple method to keep discussions focused on the topic at hand and keep the meeting on time. Examples of agendas from airport tenant meetings are presented in Appendix C.

The inclusion of take-away materials, such as briefing slides and reminder notices, can help reinforce critical points made during meetings. They can also be provided to individuals who were unable to attend to review important information.

One CAT I airport reported creating and distributing a PowerPoint presentation in connection with their monthly briefing. They believe this approach reinforces and strengthens their communication with stakeholders.

Using handouts requires careful planning to ensure that security information is not improperly disseminated. Many airports specifically use the verbal meeting format to avoid that risk. Additionally, caution should be exercised to ensure that handouts do not become a substitute for meeting attendance.

3.4 Minimize Knowledge Loss

Loss of institutional knowledge is a significant concern for many airports, especially with the large number of industry retirements and layoffs during the COVID-19 pandemic. Creating programs designed to capture the experience of security personnel, including relevant stakeholder contacts, maintenance schedules, informal processes and procedures, and any other relevant information may minimize this loss in the future.

In addition, a lack of written procedures and policies can create confusion and miscommunication that can result in critical failures, particularly during high-stress emergency situations. Documenting SOPs and Post Orders ensures a consistency of knowledge, understanding, and application of the policy/procedure among stakeholders. This provides uniformity and compliance in operations and workflows, and allows stakeholders to reference proper protocols easily and quickly. These documents

[21] https://www.trollandre.com/blog/2019/06/the-meeting-rules-of-engagement/

[22] Roy-Andre Tollefsen, 2019, *The Meeting Rules of Engagement*

require review and updating at least annually to ensure they still meet the current procedures and regulations.

Ensuring policy documents and SOPs are accessible will enable stakeholders to access relevant documents to refresh their understanding or clarify questions they may have about policies and procedures. Airports have done this in a variety of ways, such as maintaining hard copy briefing books of SOPs in security offices or storing digital copies on local networks or in the cloud. Allowing for SOP retrieval and review from mobile devices would be valuable to dispatch and field personnel.

One CAT X airport is in the process of developing a mobile application to provide field officers with access to a range of SOPs and other reference documents. This would allow the officers to pull up relevant security procedures and processes when needed. The airport anticipates this tool will eventually be used for field reporting. Establishment of this technology as a two-way communication platform is expected to greatly strengthen information sharing at the airport. An example of this type of application is discussed in Section 3.6.2.

Another CAT X airport created a pocket-sized manual covering security procedures and violations. The airport provides the manual to all frontline workers and requests they carry the document with them. The airport's badge holders have provided positive feedback, and the airport reported a reduction in security violations. However, the airport must reprint the document for all badge holders when policies or regulations change.

As materials are made more easily available, both physically and digitally, frontline workers should be aware of the requirements to safeguard those materials. This can be accomplished with security markings on the materials themselves as well as reinforcement of training on information security. Disclaimer messages, NDAs, and language in the user agreement of mobile or web-based applications can also help protect the information.

Technology is also available to assist with knowledge retention and reinforcement of critical information. Machine learning and predictive analytics tools can measure, reinforce, and predict the knowledge base of the organization's employees.

One such tool, Blank Slate, is a peer-reviewed, app-based knowledge retention solution that can reinforce SOPs and maintain retention of job-based knowledge, which is essential to mitigate the effects of high turnover rates in airport workers, training challenges, and liability exposure. Blank Slate Technologies' machine learning tools continuously measure and improve employees' ability to retain and recall information, leading to better performance and reduced risk.

National Safe Skies Alliance evaluated this application with a segment of the security workforce at FLL. Similar applications are deployed in defense, law enforcement, and a variety of other industry sectors.

3.5 Train and Educate Stakeholders

Training and education are the foundation of strong and stable security postures at airports. Badge holders are required to be given training covering their security responsibilities, federal requirements, and consequences for security violations, but many training programs include additional security training. Airports can consider the appropriate level of training based on an assessment of their security culture and level of stakeholder engagement.

Onboarding new personnel in security positions may provide an opportunity for airports to institute new programs and training modules to influence the direction of the airport security culture and security posture.

Airports implementing any new security programs (e.g., incentive programs, consortiums, mobile applications, etc.) should develop relevant and documented SOPs and policies. If necessary, training modules for the new programs should be assigned to appropriate stakeholders, including current and new airport workers. Adding the training modules to new badge holders' training requirements introduces the new population to the programs early on. This will strengthen the airports' security culture and posture, and the new badge holders will be able to help reinforce the new programs and policy changes.

> One CAT X airport took advantage of the high attrition rate in airline employees to implement new training programs focused on the employee's role in airport security. This program was introduced to the new airline employees, which allowed the airport to start to build and change their security culture and knowledge base starting with the new badge holders.

SSI TRAINING

Nearly all airports provide at least a basic level of SSI training to all their badge holders, frequently incorporating it into their SIDA training. Recurrent training, especially for those who do not handle SSI often, will help reduce errors and potential litigation by reminding the individual of their role in protecting the airport's sensitive information and methods for managing SSI.

Many airports require contractors handling security information for projects to develop SSI protection programs and train their employees on the handling of SSI. It is also common to have the contractor or the contractor's employees execute an NDA and confirm that training has been completed.

Authorized signatories are typically required to take SSI training with the expectation that they will train the company's other employees on managing SSI. This also helps to remind the company representatives and leadership that the company is responsible for their employees' compliance with all regulations, including those applied to the protection of SSI. Failure to comply may result in penalties for both the employee and the company.

OPERATIONAL TRAINING

Most interviewed airports, airlines, and industry associations indicated that one of the barriers to information sharing is the fact that most stakeholders do not understand the complete breadth of operations being performed at the airport. As a result, stakeholders do not understand how their information could be relevant to the airport, or they do not know which department or individual to report information.

> One CAT X airport trained airport LEOs on day-to-day airport operations after discovering that the LEOs were unfamiliar with the ASC's responsibilities. By educating the LEOs on security responsibilities and policies, the airport was able to break down some of the communication barriers that had been limiting their information-sharing capabilities.

Providing stakeholders with relevant information on how the airport operates and which roles are responsible for managing security information gives them the tools and knowledge they need to better communicate security concerns and report relevant security information.

TRAINING METHODS

Most badge holder training is provided via computer-based training with some instructor-led sessions. Some airports have created security-based roadshows hosted by a security expert to discuss airport security fundamentals. This also allows the participants to build relationships and trust that can carry over into information-sharing relationships.

Several federal and local partners offer classroom training sessions, including for security awareness. TSA's internal regulations require them to improve airport engagement by offering training to educate airport partners. An example of this is classroom training as part of TSA's See Something, Say Something program. Many airports ask local or airport police or TSA to present before stakeholders on topics such as inspection policies or recent security trends.

3.6 Encourage Reporting of Security Incidents

Reporting of security incidents is an essential form of information sharing in an airport. Airport and stakeholder personnel should be incentivized to report security incidents and suspicious activity, and be aware of the available reporting methods.

3.6.1 Provide Education and Incentives

Airports can encourage personnel to share information by educating them on the underlying reasons for the security requirements or policies in place. Many individuals are hesitant to report security incidents or suspicious behaviors because they fear the social stigma, they believe someone else is responsible for reporting, or that they are too busy with operational responsibilities to report. By identifying and explaining the regulations and giving examples of the consequences of security incidents, airports can illustrate and emphasize the importance of following security rules and policies, and reporting suspicious activities and behaviors. The more individuals who understand the "why" of the security, the more likely they are to actively participate in information-sharing programs.

Another method is to share real-life examples of identified threats or vulnerabilities, including the reports and information generated by tenants and frontline workers, which result in the creation of policies.

One CAT I airport received feedback from their tenants indicating that security incidents were being reported, but it did not seem as though law enforcement was responding. This was discouraging for the tenants because they did not feel that their concerns were being heard. The airport, in turn, could see that it was affecting the security culture. The airport began collecting and tracking reports from tenants and sharing them with all the stakeholders so that everyone was aware of the current trends. The stakeholders could also see that their reporting activity had value and that the information being provided had a positive benefit. Implementing the feedback loop proved to be a positive development, and the airport management also believes this practice helps maintain and strengthen their security culture.

Publicizing success stories is another method to encourage participation in information-sharing programs. Identifying and recognizing incidents where the sharing of information resulted in addressing a threat or minimizing a vulnerability can encourage individuals to participate in implementing security measures. This kind of conduct could be incentivized through a range of activities, such as the creation of a formal reward programs or an acknowledgment of exemplary behavior during stakeholder meetings or through a note from a senior executive.

3.6.2 Provide Reporting Channels

Not having or not knowing the proper reporting channel is a significant barrier for stakeholders to report information. Many airports identified instances of frontline workers reporting suspicious activities to their direct supervisor and that supervisor never passing the information along to the security department. Often, the supervisor does not know how to share the information with the airport. Airports that have worked to create simple processes for reporting believe their information-sharing programs have become more successful as a result.

HOTLINES AND TEXT MESSAGING

Most airports use hotlines as their main reporting channel. Hotlines allow dispatchers to have conversations with callers to gather details and provide feedback on situations in real-time. Some airports provide special phones in their terminals that connect directly to the airport's security department or dispatchers.

Some technologies enable security departments to respond to reports via text messages. Communication through text may be a good addition to a call-in number for reporters who would rather not, or cannot, speak over the phone. Providing a text number for the public and badge holders to send information, photos, and videos directly to the security department eliminates the need for the caller to download a mobile application or find a supervisor.

APPLICATION-BASED SOLUTIONS

Some airports have adopted application-based platforms to enhance their ability to receive operational and security information. These solutions allow badge holders and the public to report suspicious activities quickly and easily without the need to pass the information directly on to supervisors or hunt for phone numbers.

Most of these reporting applications allow users to upload photographs and videos, which can be useful for forensic and investigative purposes. These applications also allow for anonymous submissions of information or the ability to text chat directly with dispatchers.

Mobile solutions enable LEOs to receive information in the field, transmit data, and prepare and submit reports from their phones. These applications are rapidly gaining acceptance in many law enforcement settings outside of the aviation sector.

Gatwick Airport offers an airport community mobile application that provides employees and other badged personnel access to a wide range of resources, such as SOPs, rules and regulations, relevant contact information, employee bus schedules, and an airport calendar of events. It also includes information commonly asked by passengers, such as flight information, on time performance, and arrival and departure passenger flow information. This has significantly improved customer service levels.

The app also enables the airport to push relevant messages to app users and to receive information from its user base. This information flow can include photographs in addition to text, which has allowed the airport to eliminate the previous text messaging platform, saving the airport money.

The app was launched in 2016 and was reported to have over 12,000 users within 2 years (out of an eligible badged population of 20,000). Badge holders are incentivized to use the app through coupons and discount offers from airport concessionaires.

Several transit agencies in the US, including commuter trains and light rails, have mobile application solutions in cities across the country that are available for the public to use. They provide a means for the transit agencies to receive real-time information on security concerns.

One CAT X airport was experiencing challenges in coordinating the actions of security officers across the airport campus, so they issued smartphones to the 150-person security force. At the start of their work shift, security personnel log in to an application installed on the phone that assigns them a range of work tasks or “missions.” Those missions can include staffing fixed posts or conducting mobile assignments such as security checks.

Once the user accepts a mission, they must report to the mission location to begin their task. The app tracks the mission start time and records progress information. Users can file reports through the app, which can include supporting photographs and video files. The user then logs the completion of the mission.

The user’s supervisor is able to immediately review security reports submitted by field personnel to quickly address security concerns. The app allows users to quickly find and view these reports, which is especially useful when TSA requests information on security compliance. The digitization of these reports has replaced a cumbersome paper process.

The app also provides resources that can help users with their missions, such as digital copies of post orders and SOPs. Report templates are provided to assist with report creation. When conducting badge checks, the app can scan badges using the phone’s camera.

The app monitors the activity of the users in real time through geographic information system functionality. This allows the phone to relay information about the user’s movements while on the airport campus.

EMAIL-BASED SYSTEMS

Some airports provide a dedicated reporting email address for badge holders and the public to send information, images, and videos. Although this does not appear to be common practice, it could provide resource-restricted airports with another reporting channel that shares many of the benefits of a mobile application without the additional resource costs. This method requires a commitment to continuous monitoring.

WEBSITES

Contact forms on websites allow the airport to receive information from the public. A process should be in place to send form submissions to the appropriate individual. This can be an automatic function of the website, or the airport can assign a contact form manager to forward information to the relevant individual.

3.7 Improve Messaging

Information overload greatly impairs an individual’s ability to retain and act upon information. When there is too much to look at and take in, some people may ignore the message completely. Airports can help prevent message fatigue and information overload by carefully curating messages in tone, appearance, and delivery method so that it targets the appropriate audience.

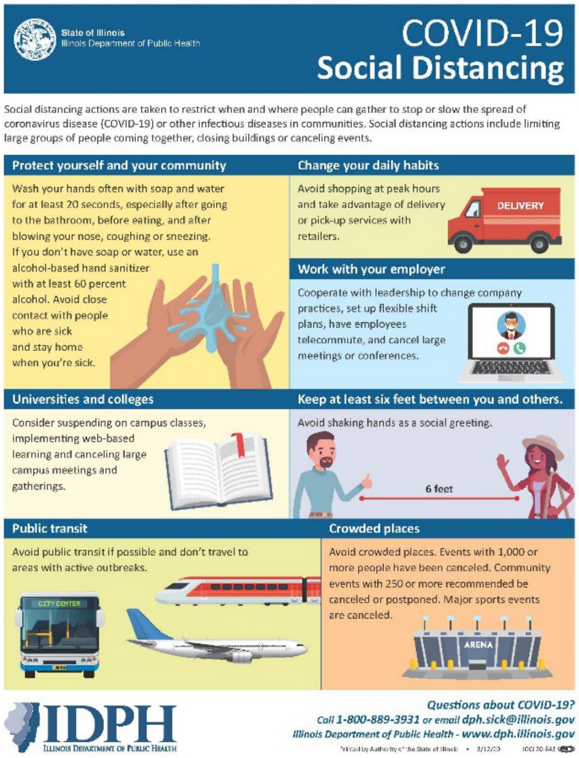
3.7.1 Printed Materials

Many airports create and share posters, handouts, fliers, and other printable communications with stakeholders. These materials are designed to be printed by the company or department representative and posted in employee areas. They can include documents highlighting important phone numbers or common security violations at the airport. Documents created for this purpose should follow good design practices, (e.g., easily readable font, not too cluttered) and should focus on a single topic. Links to relevant and important webpages and documents can be created using quick response (QR) codes. Individuals can scan the code with their mobile device camera to open the webpage or document.

Occasionally, airports need to create messages that go against the typical good practices for printed materials in order to provide sufficient information on a single, focused topic. Press releases and factsheets, such as the social distancing poster in Figure 3-2, are good examples of this.

Information of this type is most effective when located in areas where individuals will be waiting long enough to review the information.

Figure 3-2. Example of a Single Focus Poster



State of Illinois
Illinois Department of Public Health

COVID-19
Social Distancing

Social distancing actions are taken to restrict when and where people can gather to stop or slow the spread of coronavirus disease (COVID-19) or other infectious diseases in communities. Social distancing actions include limiting large groups of people coming together, closing buildings or canceling events.

Protect yourself and your community

Wash your hands often with soap and water for at least 20 seconds, especially after going to the bathroom, before eating, and after blowing your nose, coughing or sneezing. If you don't have soap or water, use an alcohol-based hand sanitizer with at least 60 percent alcohol. Avoid close contact with people who are sick and stay home when you're sick.

Change your daily habits

Avoid shopping at peak hours and take advantage of delivery or pick-up services with retailers.

Work with your employer

Cooperate with leadership to change company practices, set up flexible shift plans, have employees telecommute, and cancel large meetings or conferences.

Universities and colleges

Consider suspending on campus classes, implementing web-based learning and canceling large campus meetings and gatherings.

Keep at least six feet between you and others.

Avoid shaking hands as a social greeting.

Public transit

Avoid public transit if possible and don't travel to areas with active outbreaks.

Crowded places

Avoid crowded places. Events with 1,000 or more people have been canceled. Community events with 250 or more recommended be canceled or postponed. Major sports events are canceled.

IDPH
Illinois Department of Public Health

Questions about COVID-19?
Call 1-800-889-3931 or email dph.sick@illinois.gov
Illinois Department of Public Health - www.dph.illinois.gov

Printed by Authority of the State of Illinois • 3/12/20 IOCI 20-643

Source: Illinois Department of Public Health

In general, single-focus materials are only posted temporarily to address specific issues, such as new compliance information, and are meant to be removed and replaced with updated information as needed.

3.7.2 Digital Messages

Airports will often share links through email with their stakeholders and receive links from their federal and industry association partners to information on HSIN, SAGE, SharePoint, and other platforms. Sharing links instead of sharing documents offers two document security benefits. First, links to other platforms often require the user to sign in to authorize access; this acts as the second half of a two-factor authentication process, with receiving the email being the first. Second, documents shared over email, even when password-protected or encrypted, could be shared without permission through message forwarding or hacking. Airports using links to share information should ensure that their target audience has access to those external platforms.

Multiple airports reported interest in having an internal, web-based security forum or blackboard where the airport and its stakeholders can post information or discuss security topics. This type of system would require a software investment, but may have significant advantages in fostering communication and enhancing security awareness. A web forum or blackboard would enable the airport and its stakeholders to address current challenges and also reference back to older discussions as necessary. Further, these tools often enable targeted communications, allowing the airport or stakeholder to reach out to specific audiences.

3.7.2.1 Distribution Lists

Distribution lists are useful tools for quickly sending information to large groups of individuals. These lists save time and reduce the risk of sending messages to the wrong email addresses or omitting email addresses.

Airports may create multiple distribution lists to make sending messages to groups with focused interests simple and quick. Security-centric distribution lists can assist airports in ensuring that messages are only sent to authorized individuals.

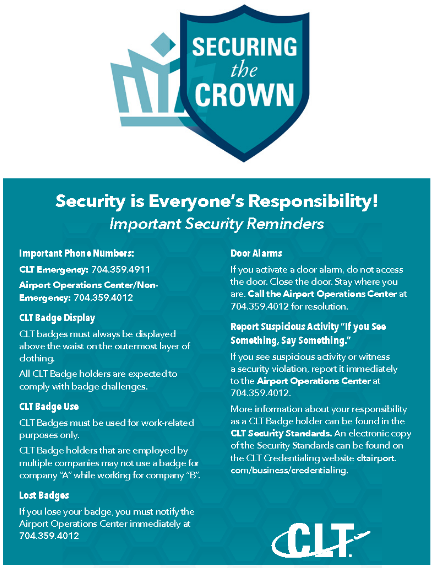
Distribution lists require frequent curation to account for turnover and changing roles and responsibilities. Distribution policies and workflows should be in place to ensure that sensitive information is not being released without authorization.

3.7.2.2 Newsletters

A security-focused newsletter may help strengthen the security awareness and posture at the airport. This could be a multipage document sent out biannually or quarterly that covers several security topics, such as known events at the airport or new access portals. Alternatively, it could be a single-page document published monthly that covers one or two topics of relevance, such as new security leadership or new processes. The frequency of the newsletters should be carefully considered to ensure that stakeholders are reading the information; newsletters arriving too often may be deleted before opening.

Regardless of who authors the newsletter, the airport should assign one or two individuals to be responsible for reviewing and editing the document before it is published. This helps to create a well-written and designed newsletter. An individual from the security department or police department should review security-focused articles to ensure no unauthorized security information is released. The PIO could also be included in the process to ensure the newsletter reflects the airport's brand.

Figure 3-3. Example of a Single Focus Newsletter



SECURING *the* CROWN

Security is Everyone's Responsibility!

Important Security Reminders

Important Phone Numbers:

CLT Emergency: 704.359.4911

Airport Operations Center/Non-Emergency: 704.359.4012

CLT Badge Display

CLT badges must always be displayed above the waist on the outermost layer of clothing.

All CLT Badge holders are expected to comply with badge challenges.

CLT Badge Use

CLT Badges must be used for work-related purposes only.

CLT Badge holders that are employed by multiple companies may not use a badge for company "A" while working for company "B".

Lost Badges

If you lose your badge, you must notify the Airport Operations Center immediately at 704.359.4012

Door Alarms

If you activate a door alarm, do not access the door. Close the door. Stay where you are. **Call the Airport Operations Center** at 704.359.4012 for resolution.

Report Suspicious Activity "If you See Something, Say Something."

If you see suspicious activity or witness a security violation, report it immediately to the **Airport Operations Center** at 704.359.4012.

More information about your responsibility as a CLT Badge holder can be found in the **CLT Security Standards.** An electronic copy of the Security Standards can be found on the CLT Credentialing website **cltairport.com/business/credentialing.**

CLT

Source: CLT Security Awareness Bulletin, July 2021

Charlotte International Airport (CLT) publishes a quarterly security newsletter for their stakeholders. This multipage document covers security topics of relevance to the airport stakeholders and is written by the airport tenant security directors. Topics include construction projects, evacuation plans, credentialing processes, and severe weather planning.

Figure 3-3 shows the final page of one of the airport's security newsletters. The airport intended for this page to be printed and posted in employee areas to provide a quick reference for security numbers and common security issues.

For newsletters containing a large amount of information, it may be better to summarize the topic and link to the full document or article instead of including the full text in the newsletter body. This will allow the reader to choose what is relevant or of interest to them. Linking to an external platform that requires user authentication could also be a method of controlling access to the information as needed.

Some email distribution services are able to track the number of times links in an email have been clicked. This allows the airport to determine the level of engagement and the appropriate frequency for publication.

3.8 Leverage Technology for Awareness and Information Distribution

Most airports already have systems and processes in place to share information during emergencies or other security events. These communication channels are critical to the success of emergency events but often remain unused when no event is occurring. However, many airports leverage these existing channels to push operational and compliance information to their stakeholders.

AUTOMATED NOTIFICATION SYSTEMS

Many airports report the use of or an interest in adopting automated notification systems to better ensure information sharing in the event of an emergency or security incident. Airports use these systems to push emergency or incident notifications, digitize response plans, and send out regular security reports. The leading vendor selling these solutions has about 400 different airport and aviation sector clients using their software, with over one billion users worldwide.

Automated notification systems enhance incident response and action by:

- Sending messages to key individuals or to other systems using distribution lists that can be adjusted based on the nature of the incident
- Offering features to create and store scripted messages, and to adjust the timing and content of messages for each stakeholder group for various situations
- Using multiple communication channels, such as text messages, email, phone messages, public address notifications, and social media posts to ensure a wide distribution of information
- Setting up action and notification workflows that reflect the airport's response plans

Airports with an existing notification system can leverage it to send critical security information to relevant stakeholders outside of emergency events to familiarize themselves with the system and run tests. This allows the airport community to ensure reliable information flow during incidents and events.

Utilizing automated notification systems for proactive messaging lets stakeholders know that the airport is aware of an issue and is taking corrective actions, while minimizing cascading calls for service that can clog or disable communication channels and lead to slower incident response and action times.

Deploying an automated notification system will have associated costs and time commitments, but airports using these systems have seen benefits to their information sharing programs and improved feedback from their stakeholders.

PARAS 0013: *Minimizing Congestion in Public Areas to Mitigate Security Vulnerabilities*[23] provides more information on automated notification systems.

INTEGRATED PUBLIC ALERT AND WARNING SYSTEM (IPAWS)

FEMA's IPAWS distributes Wireless Emergency Alerts (WEA) to smartphones within designated areas. Authorized alerting authorities, such as cities and counties, are permitted to send WEAs on behalf of airports during emergency events, but the approval channels required may cause a delay in relaying the

[23] **PARAS 0013:** https://www.sskies.org/images/uploads/subpage/PARAS_0013.MinimizingCongestion.FinalReport-Final.pdf

information. Airports may apply to become an alerting authority, which would allow them to eliminate steps to send a WEA and make the information more timely and actionable. Currently, eight airports and airport authorities have IPAWS alerting authority.

There is no cost to become a WEA alerting authority, but the software required to send the alerts must meet IPAWS requirements. More information on becoming an alerting authority is available on the FEMA website.[24]

SOCIAL MEDIA

Social media also offers some information-sharing benefits. First, during emergency events, an airport's social media pages offer a direct source for the public to get information in real time. Second, social media forums allow one-on-one messaging or group discussions in real time. This feature also allows the public to provide feedback and report directly to airports.

This is not the most reliable means of sharing information, because only a small percentage of an airport's customers will follow the airport's social media page. However, social media is inexpensive and can be used to supplement more reliable channels.

Airports should implement appropriate policies and procedures, and provide training to their social media account managers regarding forwarding potential security-related information to the appropriate airport personnel. The ASC, legal team, and PIO should be consulted when drafting any posts or materials being posted to the social media account to ensure it does not share SSI and that the message appropriately reflects the airport's brand.

SAFETY/SECURITY MANAGEMENT SYSTEMS

Some airports accept reports about safety concerns as part of the airport's safety management system (SMS). These airports could adapt their existing infrastructure and processes in the SMS to also enable security reporting.

> The SMS program at Frankfurt Airport actively encourages employee reporting of safety concerns and helps to ensure airport safety is a focus of the community. The airport's website includes forms and instructions for reporting that are sent directly to the SMS or the safety office. The website emphasizes that reports will be treated as confidential and "not used to the detriment" of the reporting employee, and offers an option to report anonymously.

An SMS employee reporting system could be readily adapted into a Security Management System (SeMS). SeMS encourages airport worker participation in security improvement. The engagement of staff through training and the SeMS focus on continual improvement are examples of the importance of two-way information sharing. The SeMS model has not been widely adopted in the US, but at least one CAT I airport is utilizing the SeMS approach. More information on SeMS can be found in PARAS 0009: *Guidance for Security Management Systems (SeMS)*.[25]

[24] **IPAWS signup:** https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/sign-up

[25] **PARAS 0009:** https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf

3.9 Leverage Lessons from Emergency Management Practices

Communication and preparation are key to successfully managed emergency events. These practices focus on information sharing necessary for collaborative problem solving. Both elements require airports to familiarize themselves and build relationships with their stakeholders prior to an incident or emergency. These are the individuals who will sit next to them in their EOCs during emergency events.

> One CAT I airport with a multi-tenant terminal had a designated airline representative who acted as liaison for all the airlines in the terminal. The airport did not have enough space in the EOC for a representative of each airline. Instead, the representative had a seat assigned in the EOC, and during an event would relay the information from the airport to the airlines' points of contact.

Establishing processes to share information is essential for emergency response. The lessons learned from those experiences have great relevance to the practices established for day-to-day information sharing. Where that day-to-day sharing is strong, emergency response practices are greatly enhanced. Airports should use lessons from their emergency response exercises and practices to enhance their non-emergency practices.

TABLETOP EXERCISES

Regular tabletop exercises for emergency scenarios are federally mandated, and they can serve as excellent training and team-building opportunities. Cultivating information-sharing relationships during these regular exercises may lead to more open dialogue during non-emergency scenarios.

META-LEADERSHIP FRAMEWORK

The Meta-leadership framework and practice method was created based on insights from the Boston Marathon Bombing in April 2013, lessons learned from other crisis situations, and research on how leaders respond to high-stress situations. Meta-leadership's focus is organizational framework, categorizing activity, and improving community function and performance.

The Meta-leadership framework was developed by faculty at Harvard's National Preparedness Leadership Initiative,[26] a joint program between the Harvard T.H. Chan School of Public Health and the Kennedy School of Government, Center for Public Leadership.

The researchers determined that the first responders in the Boston Marathon Bombing were able to effectively lead within their own organization and collaborate with other organizations because of pre-existing relationships and an ability to communicate effectively with multiple internal and external stakeholders, which facilitated faster information flow, more informed decision making, and more effective response. These factors enabled leadership and first responders to know who was in charge of which responsibilities, and to contact those individuals directly instead of navigating dispatch channels. Although Boston did not have roles perfectly detailed, first responder organizations from local, state, and federal agencies were able to execute tasks and collaborate successfully.

The important takeaway from Meta-leadership is the importance of information sharing at appropriate levels, and managing relationships to ensure individuals are ready to act cohesively in emergency situations.

[26] https://npli.sph.harvard.edu/

SECTION 4: MINIMIZING UNAUTHORIZED INFORMATION ACCESS

Preventing the unauthorized further dissemination of information was the principal legal concern identified in the research. This included concerns over compelled disclosure of information through mechanisms such as Open Records requests. See Appendix F for more information on responding to Open Records requests.

The practices put in place for securing shared information generally involve ensuring that documents are properly marked with appropriate security notices (e.g., headers and footers required by 49 CFR §1520), and disseminated using recognized protocols (e.g., utilizing password protections). Typically, airports will impose additional security measures when sharing highly sensitive documents, such as the ASP, or when potentially sensitive information is given to parties generally unknown to the airports, such as contract bidders.

Typically, unauthorized access to information occurs due to negligence or misuse by authorized individuals. This has become an even larger concern as more airport personnel are working from home and accessing information in non-secure environments. This vulnerability can be reduced and managed by creating well-defined user rights access controls, choosing secure solutions to store files and documents, utilizing existing information sharing platforms, and establishing policies for sharing information.

For more in-depth discussions on cybersecurity at airports, please refer to PARAS 0007: *Quick Guide for Airport Cybersecurity*[27] and ACRP Report 140: *Guidebook on Best Practices for Airport Cybersecurity*.[28]

4.1 Measures to Limit Dissemination

Airports commonly use a range of measures to limit further dissemination of security sensitive information. These measures can include NDAs, MOUs, tenant security programs, lease agreements, and airport rules and regulations. Some airports have developed programs to manage the sharing process, particularly when sensitive information is provided to individuals outside the airport community, such as Open Records requesters and bidders on security procurement projects. These measures supplement the federal and state requirements protecting the security information.

4.1.1 Non-Disclosure Agreements

Airports do not often share SSI, but when it is necessary the most common practice is to require the individual recipients of the SSI to sign an NDA. Other airports manage SSI compliance by requiring the company's leadership to execute an NDA on behalf of the company's employees, and the company representative is responsible for enforcing the security requirements outlined in the agreement. An example of an NDA with language for both corporate entities and individual employees is presented in Appendix D.

NDAs are usually tailored to address specific sensitive information of concern, such as sharing the ASP or systems data, but may be more generally constructed.

[27] **PARAS 0007:** https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf
[28] **ACRP Report 140:** https://www.trb.org/Publications/Blurbs/172854.aspx

One CAT I airport utilizes a general NDA form to protect information provided to companies supplying goods or services to the airport. The form extends beyond SBU information to include information that the airport deems sensitive, including proprietary information. This form notes that restrictions on dissemination include unauthorized reproduction of the provided materials, and requires the company executing the document to ensure employee compliance with SSI requirements. Appendix D presents a redacted version of this NDA.

One CAT III airport requires all badged personnel to execute a DHS NDA to protect sensitive information shared or learned while employed at the airport. The agreement follows the format utilized by DHS to cover SSI, PCII, and other SBU information. The NDA details the limits on disclosure of the sensitive information and the potential penalties for individuals who violate the agreement. This measure emphasizes the importance the airport places on properly safeguarding sensitive information.

A copy of the DHS NDA template can be found in Appendix D. A fillable PDF version can be downloaded at https://www.dhs.gov/publication/ndagsa-forms.

More general NDAs have been utilized to protect a range of other information not addressed in the DHS form. They are limited in their enforceability, incurring civil action rather than criminal penalties and fines. Enforcing the provisions of the NDA would require the airport to initiate a lawsuit, which would likely be time consuming. However, it is important to note that if the information is covered as SBU (e.g., SSI or PII) and is properly marked, fines and criminal penalties could be applied at the discretion of the federal government. Additionally, it should be noted that in jurisdictions with fewer Open Records exemptions, stakeholders may have more access to information without the protections of an NDA to limit subsequent dissemination.

A properly drafted NDA should alert the recipient to the importance of the information, the requirements for securing the information, and the penalty for failing to meet those requirements. NDA language can address the following:

- Definition of information deemed as “Confidential Information” covered by the NDA, such as SBU and proprietary information
- Acknowledgement that the information is owned by the airport
- Required protection measures, such as passwords or secure servers
- Restriction on the use of information, especially if limited to a specific purpose, such as providing services or preparing a proposal bid
- Requirements to inform or train employees and subcontractors of the necessary protection measures and the penalties for non-compliance, as well as any requirements for these individuals to sign an NDA
- Requirements to notify the airport if the information is lost, stolen, or otherwise improperly disseminated
- Requirements to notify the airport of any court order or public process compelling disclosure of the information
- Requirements to return or destroy the information upon completion of services or the project, upon demand by the airport, or after a designated time period (e.g., two years after receipt)
- Remedies available to the airport in the event of a breach of the NDA terms in addition to state and federal penalties

- Disclaimers of warranties and limitation of liability related to the information
- Acknowledgement that the recipient has received the information

Airports should collaborate with their legal counsel to draft NDA language to address these issues and determine when the NDAs should be served. The examples shown in Appendix D can serve as templates to be customized for the airport's needs.

4.1.2 Memoranda of Understanding/Agreement

Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA) are used to protect all types of information being shared, but are most often used by airports to outline the access to and dissemination of CCTV data. These agreements define the ownership, operation, and access restrictions for use of CCTV systems and its generated images.

Entities that conduct investigations for compliance and criminal activities, such as TSA and law enforcement agencies, are often afforded routine download access by airports. MOUs are in sometimes used to support that access. In the case of TSA, the MOUs are frequently drafted in connection with TSA funding for the airport's procurement of the CCTV system.

Below is a sample of an MOU agreement between an airport and the TSA for TSA-funded projects. The form is redacted to protect the identity of the airport. The language in Figure 4-1 requires TSA/DHS review of video before dissemination, even for Open Records requests. These types of provisions are generally applied to review of images from cameras monitoring checkpoints, and the airport must clarify a process for release of information with TSA. That process needs to account for the airport's legal requirements for response to requests, which may come from the Open Records request policy, such as response timeframes in a subpoena or court order, or they may be set by a statute or regulation.

Figure 4-1. Sample from a CAT X Airport's MOU with TSA

> "Any and all third-party requests, including [*state information request law*] requests, for CCTV media generated by the CCTV system that are received by the [*airport authority*] shall be forwarded to the FSD or designee, or TSA Technical Representative for a [SSI] review […].
>
> "The [*airport authority*] shall be the owner and custodian of the CCTV system as well as any video media generated from the CCTV system and will secure all such CCTV media at all times […]. Immediate access to all CCTV system data output will be limited to the [*airport authority*], law enforcement agencies, and TSA or DHS personnel in order to operate the CCTV system or for law enforcement and security purposes. **No part of this provision shall be constructed to limit the ability of the [*airport authority*] and TSA or DHS personnel to access the above-referenced media for the purpose of conducting any administrative or criminal investigation. […]** Any requests, including FOIA requests, received by the [*airport authority*] for the data produced by the CCTV system must be handled in accordance with [the above paragraph]. Upon written request, TSA or DHS will be provided copies of the data produced for law enforcement investigations, national security investigations, other administrative investigations, training, or for quality control purposes."

The key takeaway from the MOU arrangement is the clarification of system ownership, including ownership of the infrastructure and the images generated by the system. This applies to sharing with TSA and other stakeholders who may have CCTV infrastructure on a common system or who seek access to an airport-owned system. At some airports, the issue of access is governed by a regulatory structure.

At a minimum, written governance of the CCTV system or any sensor data through an MOU or airport regulation should address the following issues:

- Who owns the system and who will develop and operate it; this should include proprietary rights of the equipment, such as:
    - Cameras, biometric equipment, etc.
    - The physical and virtual data-sharing infrastructure
    - The physical and virtual storage infrastructure
- Who maintains the system and makes determinations on modification and/or expansion
- Who owns the images in the system
- What access rights are given to stakeholders
- How long to retain sensor data
- What the is process to request review, download, or copy sensor data
- Under what circumstances a stakeholder can review sensor data
- Whether data can be downloaded or copied
- What information can be generated based on the shared data, including copies
- What the are restrictions on further dissemination of the shared sensor data

For more in-depth discussions and examples of legal measures to ensure security compliance, refer to PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.[29]

4.1.3 Tenant Security Programs

Some airports include the tenants' responsibilities and requirements to protect information in the tenant security program, often with requirements for the tenants to provide training on information security and treatment of SSI. These security programs may also include a requirement for reporting of suspicious activities. More detailed information can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.

4.1.4 Lease Agreements and Airport Regulations

Several airports have lease agreements or airport regulations that govern the release of information to stakeholders. Airports adding clauses regarding information sharing in these agreements should consult the airport's legal counsel. Many airports include indemnity and hold harmless language in their lease agreements for actions that violate federal, state, or local laws. This includes reimbursement of the airport for any fine or penalty levied against the airport as result of the conduct of a tenant or tenant employee. Examples of lease agreements and regulatory language with indemnity and hold harmless language can be found in PARAS 0025: *Security Regulatory Compliance at Tenant Facilities*.

Some subscription agreements, such as those used to access the FBI's InfraGard program and DHS' HISN, include indemnity and hold harmless language specifically tailored to information sharing.

[29] **PARAS 0025:** https://www.sskies.org/images/uploads/subpage/PARAS_0025.SecurityComplianceTenantFacilities_.FinalReport_.pdf

Applicants to the FBI's InfraGard program are required to agree to the indemnity and hold harmless language shown in Figure 4-2.[30]

Figure 4-2. FBI Indemnity and Hold Harmless Language

> "**Agreement to Hold Harmless the U.S.:** The applicant agrees not to institute, initiate, prosecute, or in any way aid in any demand, action, suit, or other claim, legal or otherwise, against the FBI, the Department of Justice, or the United States, or the officers, employees, agents, representatives, task force members, contractors/subcontractors, consultants, or advisors thereof, on account of any damage, loss, injury, or expectation arising from, in connection with, or in any way pertaining to the reporting, non-reporting, or use of information in accordance with this agreement.
>
> **Agreement to Hold Harmless Other InfraGard Members:** The applicant agrees not to institute, initiate, prosecute, or in any way aid in any demand, action, suit, or other claim, legal or otherwise, against any other InfraGard member on account of any damage, loss, injury, or expectation arising from, in connection with, or in any way pertaining to the reporting, non-reporting, or use of information in accordance with this agreement, and the member further expressly agrees to hold harmless and indemnify the same against loss from any and all claims that may hereafter be brought against the same by applicant arising out of the reporting, non-reporting, or use of information."

Source: FBI's InfraGard Application

Airports may decide that this type of language is relevant to reduce airport liability when sharing information. These clauses could be used in conjunction with a lease agreement, as well as with more limited agreements, such as NDAs and MOU/MOAs.

4.2 Create a User Rights Management Program

A user rights management program controls users' accesses to digital and printed files, and what actions can be performed with those files. Nearly every industry uses some level of user rights management to keep sensitive information behind a secure wall. Digital access requires users to input their unique login and password or PIN, and is typically assigned based on the user's role within the airport community and their daily responsibilities. Physical files require access codes or keys to access.

4.2.1 Limiting Access to Digital Files

Most user rights management programs closely reflect airports' physical access control programs. In general, individuals with greater security responsibilities (e.g., ASCs and tenant security directors) are given more access to security files and systems and more authority to download, share, and edit in order to complete their daily responsibilities. For example, authorized signatories are considered by some airports as the security representatives of tenant companies. As a result, those authorized signatories often have the most access to security documentation in their tenant company. If the airport intends to treat the authorized signatory as a company's security representative, that fact should be clearly conveyed to the company.

User access and authority to modify security files should be limited to only the files necessary for the user to perform their duties. Typically, access control management is highly configurable, allowing

[30] U.S. Office of Management and Budget, *Form UnNumbered InfraGard Application*, OMB 1110-0049, (2014)

airports to create levels of access based on an individual's role, identifications, clearance level, or other criteria. This access can be attached to databases and applications as well as folders and files.

However, even though access is based on role, the authority granted is tied to the user, meaning that when an individual changes roles, they may retain their access permissions from their previous role. Regular audits should be performed on user access permissions to ensure they are valid and limited to only the necessary files and systems.

Airport IT departments is usually responsible for managing user access to files within the airport's servers. The ASC or security department typically defines the permissions for each role in each company. This often looks like a decision flow chart that helps determine the user's necessary access, and enables the IT department to assign access permissions to new users without needing to consult the ASC each time.

Managing and auditing the access permissions of potentially hundreds or thousands of users is a significant task. Third-party software is available to manage the database of users and their access permissions. After initial setup, the software can automatically assign permissions to new users and modify permissions based on changes to the users' role in the company.

4.2.2 Monitoring User Activity

In general, airports do not track or account for information once it has been released. The only audits or inspections identified by airports were audits of the ASP or documents released to contractors or bidders for procurement or contract work.

Some airports only allow access on an as-needed basis as a means of monitoring activity. In practice, this requires security personnel, typically the ASC, to manually approve requests for access to specific security files. Most airports utilizing this strategy only apply these restrictions to the most secure documents, such as the ASP, so the workload is not significant. The benefit to being able to identify users' activity in real time has helped these airports feel more secure sharing such sensitive documents. This practice may prove difficult in larger airports with large numbers of stakeholders unless the security department is well staffed.

Tracking users accessing the secured files and systems can help with forensic investigations in the event of a breach, but it may also help the security department to identify unusual access activity. Multiple attempts to access restricted information or multiple attempts to download or copy the information may indicate insider threat behavior. It may also indicate a lack of knowledge on the part of the user that could be considered for additional training.

Some airport IT departments already log users' access to documents. This can also be done using third-party software.

4.3 Choose a Secure Storage Option

The popularity of cloud-based storage has slowly grown in nearly all industries due to its highly scalable architecture. Collaboration tools, email, and IDMS are commonly hosted on cloud platforms, and many financial institutions, government agencies, and military branches use and trust cloud-based storage solutions. However, some airports are concerned about the potential for data and privacy breaches on cloud-based platforms, and the risk to critical infrastructure and the public that such a breach may cause.

4.3.1 On-Premises Solutions

Most airports currently host their data on premises. Airports use server rooms or dedicated data centers either on- or off-site, or they lease storage at third-party data centers. However, for a range of reasons (technical, fiscal, and security-based) there is growing interest in cloud-based solutions for data storage.

On-premises solutions allow the airports to maintain direct control of their data. This means that airports can be confident in the access, control, and destruction of their data. There is also greater confidence in the creation of network isolation, virtual environments, and backups. However, this option may cost more in the long term. On-premises solutions require the purchase of physical hardware (hard drives, servers, etc.) and, potentially, physical security measures. If the airport owns a data center or is housing servers onsite, costs may include utilities, security personnel, and city/state/federal permits and compliance certifications in addition to the physical hardware. If leasing at a data center, these costs are often passed on to the airport in the leasing fees.

Scalability can also be a challenge with on-site solutions. The hardware takes up physical space, which is already at a premium for most airports. There may not be room for additional server racks or computers to increase storage space. Additionally, the scaling of the systems themselves may limit their utility. If the on-premises system is built and scaled only for routine operations, it may not have the capacity to handle peaks or spikes in demand that may occur in emergency situations. However, if the system is built to handle peaks and spikes, it will routinely operate under capacity.

4.3.2 Cloud Storage Solutions

Very few airports currently use cloud solutions for their data storage. Some airports indicated that their ASP was stored in an online platform with access control management policies in place, and a few airports host their IDMS and emergency notification systems on cloud-based platforms. Many airports believe that cloud-based systems have too much risk associated with them, or their IT departments believe they will have less control over the data.

Certified platforms with well-designed access control configurations can significantly reduce the risk of data breach. The Cybersecurity Maturity Model Certification and the Federal Risk and Authorization Management Program Certification are useful in helping airports determine whether vendors demonstrate compliance with federal regulations. Federal agencies, financial institutions, military branches, and other high-security, high-risk industries consider vendors with these certifications acceptable risks.

When using cloud solutions, it is important to configure environments to meet security needs. This may include multifactor authentication for access, IP address allow lists, and Virtual Private Network allow lists. A cloud solutions expert is recommended to assist in this configuration. It should also be noted that changes to vendor systems may break some configurations, so frequent tests should be performed to identify any errors.

Scalability and associated costs are the greatest benefits of cloud storage. Increasing storage capacity does not require new hardware or space to house the hardware. Maintenance of this equipment and physical security costs are left to the cloud vendor. Additionally, clouds solutions may permit the use of applications that are unavailable for on-premises solutions due to lack of computational power.

Use of cloud services requires a lot of trust in the vendor and their ability to protect and maintain the security information and the physical hardware where it is stored. The data is held within the vendor's infrastructure, which has the risk of being breached or failing. This lack of implicit control over the data is often cited for airport IT departments' reluctance to use cloud solutions. Conducting thorough research on the vendors, prioritizing those with federal-level certifications, and creating clear and well-defined contracts and agreements can help reduce the security risks of using cloud solutions. Additionally, as technology improves, so too will data security measures.

Another consideration is that cloud storage providers will not have the same sense of urgency for disaster recovery as the airport would with an on-premises solution. In the event of a data center breach or failure, priority will be given to customers with higher subscription fees using more storage space. At the same time, a large cloud vendor may have more assets and expertise available than the average airport. The service-level agreement with the cloud provider will determine the provider's responsibilities for recovery services.

TRANSITIONING TO CLOUD OR HYBRID SOLUTIONS

Many organizations, including airports, are currently working in a hybrid state, with programs such as Microsoft Office 365 running and backing up data in the cloud. Some companies operate their primary systems in an on-premises environment with backups saved to the cloud. This allows for sustainability, reliability, and redundancy of the organization's data.

When transitioning to cloud solutions, functionality to work with current workflows and compliance with city, state, or federal requirements are the most important qualities to look for. A cloud expert should configure the cloud solution to ensure the proper security measures are applied.

If the airport plans to retire physical hardware after the transition to cloud-based services, all storage devices need to be wiped digitally, using a special software, and physically, using special equipment destruction machines or services. Storage devices should never leave an airport's possession without being securely wiped.

4.4 Leverage Information-Sharing Platforms

Numerous electronic information-sharing platforms exist to support information operations in the aviation industry. US government agencies manage many of these platforms. Access to the information typically requires a username and password which must be granted. This provides some level of vetting to protect the information.

Many airports and airport stakeholders leverage these platforms to prevent unauthorized access to security information. Links to the relevant articles or document are typically sent to stakeholders via email. Since the information is secured behind access controls, only those with the appropriate vetting can view the information.

4.4.1 Linking to Federal and National Platforms

All interviewed airports indicated that they utilize federal information-sharing platforms, such as HSIN, as a means to review security intelligence and compliance information. Airlines and aviation industry associations also access these platforms, although their security clearances often give them greater access to information.

The existing federal information-sharing platforms are largely one-way sharing channels; the communication stream is almost exclusively outbound.

Some of the federal information-sharing platforms commonly used by airports and their stakeholders are described below.

HSIN

DHS's primary information-sharing platform, HSIN, is a web-based platform designed to facilitate SBU information sharing and collaboration between federal, state, local, tribal, and private-sector entities. The HSIN network contains a number of subgroups that may have entry restricted to certain groups or individuals. This allows access to certain information to be subject to further restriction. Users will require a HSIN login and, once obtained, can set up alerts and notifications when a new document of interest has been posted. HSIN contains a wide range of security information beyond aviation-specific information, but it is not intended to be the only source of intelligence products.

Many interviewed airports and airport stakeholders commented on the difficulty of navigating HSIN. Airports wishing to share information on HSIN should consider sending direct links. That way, the recipient will not need to search for the document once logged into the system. Some airports have also indicated that the registration process can be an impediment, and there is some concern about the difficulty in receiving and maintaining access permissions.

TSA'S AVIATION WEB BOARDS

These web boards provide real-time access to aviation security-related information. The web boards are hosted on HSIN and include posts of regulatory and policy documents for airports, passenger airlines, and air cargo carriers. Users will require a HSIN login to access the information.

SAGE

SAGE is a secure sharing portal operated by ODNI. Users receive notifications of newly posted information on topics that interest them. Multiple agencies post SBU information to SAGE, including FOUO and LES; SSI is not posted here, as it is almost exclusively posted on HSIN. However, SAGE does not always host the information on their platform; often, the posted information will include a link to the official report and access would be managed through usernames and password on the third-party site. Many airports and their stakeholders indicated that SAGE is more user-friendly than HSIN.

HOMELAND SECURE DATA NETWORK (HSDN)

HSDN is a Secret level and above intelligence-sharing platform hosted on the DOD's SIPRNet. SIPRNet terminals are required to access the information. No airports indicated having a SIPRNet terminal on site, and only a small number of airlines have one available. Typically, ADIAC will send an email to the TSA FIOs assigned to some airports informing them of new classified products. If the airport or airline does not have access to a SIPRNet terminal, ADIAC can host a secure phone call to read the intelligence to cleared personnel.

4.4.2 Utilizing Web Portals and Applications

The major industry associations (Section 2.2) maintain robust programs for information sharing. Association members can access online platforms, such as forums and discussion groups, which offer an opportunity for interactive communication with peers on a range of security and operations-related topics. These sources offer near real-time opportunities for security professionals to receive information and get answers to questions from other security professionals and colleagues.

Membership costs are a minor barrier to entry and access to information. The most significant limitation is the open-source nature of the communication that limits the depth in which security information can be shared; SSI is not shared on these platforms. These platforms are used as bulletins for information or emerging issues that may serve as introductions for follow-up discussions in more controlled conditions.

Daily email newsletters also provide information to the association members. The newsletters and links to articles or forums can be shared with stakeholders. Recipients will require a login to access forums or articles hosted on secured platforms.

Some CAT I and II airports share a large portion of their security information through authorized signatory web-based portals. Many airports feel comfortable sending this information to the authorized signatory using the portal, but some believe the signatory is not a high enough level of authority to communicate important or significant security information. It is not always clear if an individual who is empowered to represent a company with respect to badge issuance is also empowered to act on security-related information. Even the airports that indicated they use the authorized signatory portals to push security information do not utilize these systems to share sensitive information or SSI.

Additionally, web-based portal systems are typically not designed for two-way communication. This creates a significant lack of feedback on security information or understanding of the information's further dissemination.

One CAT II airport uses a commercial, web-based information-sharing system to provide their stakeholders with airport operations information. The system was built to share operational issues and management of the airfield and terminal facilities, but also allows for sharing of limited security information.

The users are given different levels of access, which grants them permission to view certain folders and files. However, the system does not provide any sort of notification that the intended user received the information. Additionally, although access to the system is limited and can be controlled by the airport, the system is not used to communicate highly sensitive information. This type of portal, which is open to a wide number of stakeholder users, is a good way to share general security information.

One CAT X airport is developing a collaborative information-sharing application, similar to WebEOC, for real-time security information sharing. WebEOC is an emergency information management application used by FEMA and a number of state and local governmental entities, including airports, to share informational products in emergency situations. The application allows participants to remotely access and input information addressing security problems, and would allow for access to a range of sensor information, such as camera images and access control logs, to enhance effectiveness of response.

4.4.3 Sharing the ASP

In most airports, access to the ASP is highly restricted and only key members of an airport's security staff or executive personnel can view the document. Airports that do not share their ASPs indicated that the relevant parts of the document are shared verbally in one-on-one meetings with the tenant's representative, or to multiple individuals in various staff, stakeholder, and consortium meetings. The airlines interviewed also indicated that conversations, rather than document exchanges, is the preferred method of communicating security-related information with the airports.

At most of these airports, if a tenant has questions or concerns about the specific terms of the ASP that cannot be answered verbally, they are afforded an opportunity to inspect relevant portions of the ASP. In these cases, the stakeholders visit the office of the ASC or some other secured location and are supervised while they review the information.

However, some airports share all or portions of the ASPs with tenants either physically or digitally. These airports felt that it was difficult to hold critical security partners accountable for compliance with ASP requirements if the tenants could not access the requirements. This practice requires significant trust between the airports and the tenants.

Sharing the entire physical ASP document is a practice in some smaller airports, including CAT IIs and IIIs. In these cases, the ASP is generally restricted to regulated parties such as airlines and cargo carriers, or in one circumstance a fixed-base operator FBO. As a prerequisite to receiving the ASPs, the recipients execute receipts and often sign NDAs. The receipt points to the recipients' responsibilities for securing the document in accordance with 49 CFR § 1520. Examples of receipt documents are attached as Appendix E.

One CAT II airport requires security measures to protect the ASP when they provide it to their tenants, and they inspect to ensure those measures are appropriately applied. When the ASP is updated, the ASC physically delivers the new document to the tenants and at that time inspects and audits for compliance with 49 CFR § 1520. This process presents some challenges in scalability, as larger airports tend to have many more tenants than smaller airports.

Electronic ASPs are stored in either on-premises or cloud-based storage platforms. These platforms allow the airports to control access to the documents by sharing links to the document's location and creating password or other login requirements.

One CAT I airport uses a digital information-sharing program that accesses data stored on a file transfer protocol (FTP) server. The airport uses this program, in part, to share the ASP with various departments and individuals who need access to the document.

The airport uses a folder structure organized by file type with ASP as the top folder and a subfolder containing relevant sections of the ASP for each tenant or airport department needing access. Each account is given a username and password that grants them access to their authorized folders. Certain accounts, such as security personnel, are given administrator access to all folders so that they can manage and upload the relevant chapters of the ASP to the appropriate folders. This system has been approved for use at the airport by the local FSD.

The airport reported that some external stakeholders were denied access to the airport's system. Those affected worked with their company's corporate IT to make the necessary modifications to access the airport's secure network. However, the airport's IT department is researching secure FTP (sFTP) servers, which would provide a more secure platform and would enable external stakeholders to access information for specific periods of time.

Some airports have created access levels in online storage platforms (such as SharePoint) that allow access to specific and relevant sections of the airport's ASP. Sending links to access-controlled documents or folders is more secure than sending a password-protected document, and may offer the airport the ability to review who has tried to access the file.

Leveraging access control mechanisms on sharing systems and platforms allows the airport's stakeholders access to the portions of the ASP that are relevant to their operations while the airport maintains full control of access permissions.

Some of these systems notify users of changes to folders, and many systems are capable of collecting metadata to track who has accessed the folders and files, but not all are capable of these types of auditing. The system described in the example above is not capable of pushing automatic notifications or tracking access to the files.

Another CAT I airport is planning to deploy a cloud-based storage platform to host the chapters of the ASP as individual files. The airport will send links to the file locations to relevant users, who will need the file's password to access the content. The system will create each ASP chapter as an encrypted PDF to protect it from unauthorized download and copying. The system under consideration is not capable of pushing automatic notifications or auditing access to the files, and it will share the same external access issues as the example above. At the time of this guidance was prepared, the airport's TSA FSD had not approved the system for use.

A third CAT I airport uses a large sFTP server to host their ASP. The user must request permission from the ASC to view individual sections of the ASP. This provides the airport with more control over access to the file and provides an audit trail if necessary.

4.5 Establish a Records Management Program

Establishing a records management program may help airports protect their digital files and physical documents from unauthorized access. This may require the airport to create and/or formalize file management practices through SOPs that cover the program objectives, roles and responsibilities, and administrative authorities. The SOPs should also describe the airport's policies and requirements for creating backup files, document retention schedules, and data destruction procedures. Creating a training briefing for new personnel would be beneficial to maintaining a standardized program.

As airports collect information, they should be mindful that the information may be the subject of laws requiring release in response to public request. Those requests come from a variety of sources and may concern non-security requests (e.g., lost property in the terminal or slip and fall cases). While security information is almost universally protected from disclosure, the laws will still require airports to review the information, redact it where appropriate, and produce it. See Appendix F for more information about responding to Open Records requests.

4.5.1 Protecting Digital Files

Access to digital storage, regardless of whether it is cloud-based or on-premises, should be password protected. The password can be unique for each folder or document or tied to an individual's unique login access. If the file is protected by a unique password, it is good practice to follow SSI guidance and send the password in a separate email, unconnected to the file. If the airport uses unique logins, it is good practice to create access control policies to prevent unauthorized access to protected files and folders. These can be global policies based on several factors, including:

- Clearance level
- Organization or organization type (concessionaire, airline, FBO, etc.)
- Department
- Role and responsibilities
- Completion of certain training modules
- Signing of an NDA

Access can also be granted temporarily or on an as-needed basis, such as for a contractor needing sensitive blueprint files.

Well-designed access-control policies should make adding or removing access to individuals or groups simple. Airport IT departments are well-suited to assisting airports with creating these policies. If using a third-party platform, their support may be required during the initial deployment and software updates.

4.5.1.1 Dual-Factor and Multifactor Authentication Protocols

The greater the sensitivity of the information, the greater the need for security and corresponding protocols to ensure information is not shared without authorization. Requirements such as dual-factor (2FA) or multifactor authentication (MFA) enhance security by requiring identification based on more than just entering the correct username and password, which could be brute forced or stolen.

Many organizations require individuals to regularly change their password as a means to increase security, but the cybersecurity industry no longer recommends this practice as people tend to write down new passwords or simply add a single character to change the password. 2FA and MFA can help eliminate these password management vulnerabilities.

Implementing 2FA or MFA may require the IT department’s assistance or a third-party application.

4.5.1.2 Folder Structure

Folder structures should be clear and standardized across all folders and files to simplify file retrieval and minimize duplicate documents. There are several conventional methods for organizing folder structures within an enterprise. One common method is organizing by department/division with subfolders for document types. An example is shown in Figure 4-3. Another method is organizing by document type first, then by department/division, as shown in Figure 4-4. A third option is to organize by project followed by the relevant folders for that project, as shown in Figure 4-5.

Figure 4-3. Folder Organization by Department/Division

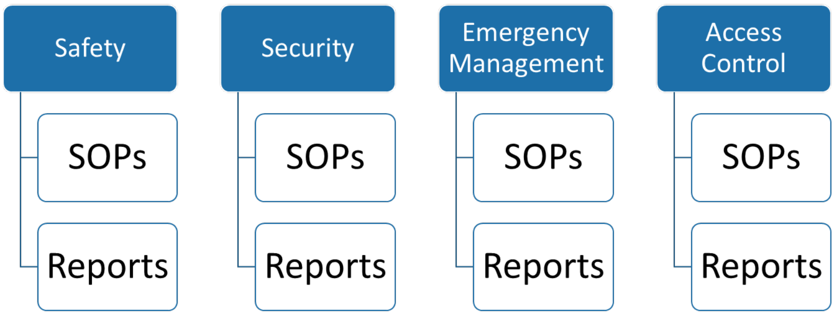


Figure 4-4. Folder Organization by Document Type

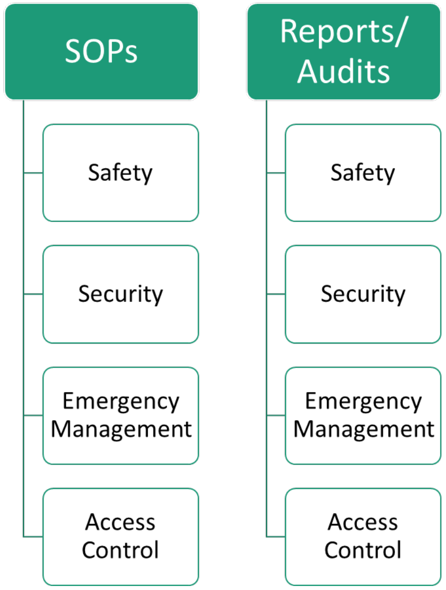
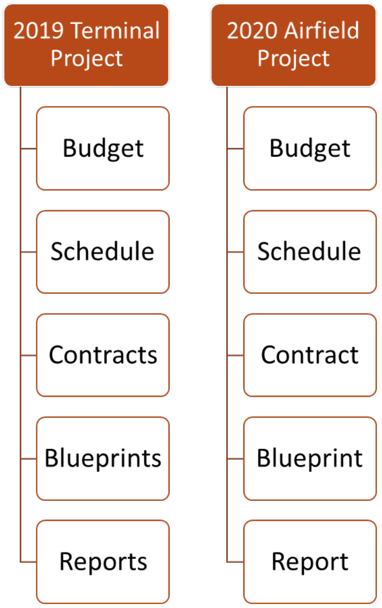


Figure 4-5 Folder Organization by Project



A system set up by department or division may allow the airport to better authorize individuals' access based on the department they work under. However, organization by document type may allow the airport to grant access to folders based on the individual's role or responsibility. Organization by project may allow the airport to grant access to individuals based on their assignment to a particular project. None of these organization methods is best. As long as the folder organization is standardized and consistent, it only matters that it works for the airport's needs.

4.5.1.3 File Naming Conventions

File naming conventions should also be standardized and consistent across the airport's network. This helps with file retrieval and minimizes duplicate documents.

It is good practice to use short but descriptive file names. Adding headers, such as "BP-" for blueprints or "ASP-" for different sections of the ASP, will alphabetically group the files together in the folder listing, allowing for a more organized folder.

Some document-sharing platforms have version control features that could help airports when they update their SOPs or other documents. Airports storing their documents on premises may not have the ability to automatically track changes to documents or files. In that situation, use of version control in the file name (e.g., ASP 05.16.22 or ASP 4.2) or use of "Archive" folders may be necessary to conform to the airport's retention requirements.

4.5.2 Securing Physical Documents

Protecting documents' storage locations and maintaining a strict filing system are necessary to secure hard copies of documents.

4.5.2.1 Locked Storage

Physical records and server storage locations should be kept secure with locks and alarms. Airports with an electronic ACS could deploy access control equipment to use authorized airport badges to open the secure room. The access control lock may work better for high traffic areas, but will have a cost associated with the equipment and installation. Keys or codes can be given to those with access authorization, but should be changed any time a key is lost or a code is unintentionally released.

It is much more secure to give out keys/codes and badge access to a small number of individuals, such as the file management staff, instead of every individual with access authority. The authorized personnel would be able to retrieve the information for individuals requesting a folder or document. This practice provides another factor of authentication, but it requires a personnel resource to retrieve the requested materials.

Airports could implement an access log system to track individuals entering the secured file storage location. This can be done with a paper login sheet and a policy requiring all individuals to sign in before entry. This may work best for areas with little to no regular traffic, but may require a staff member to ensure compliance with the policy.

4.5.2.2 Filing Systems

Standardizing the filing and storage system is especially important with physical documents and folders, since there is no digital search option to find a particular item. There is no optimal method for filing physical records. Airports should create a system which works best for their demands.

Airports may choose to file documents based on the year they were created with sub folders used to separate the documents based on the department responsible for them. This could help during audits and destroying files past their retention period, but would likely require the filing cabinets or document boxes to be stored in a single location. Airports could use this opportunity to secure the entire document storage room instead of locking individual filing cabinets.

The opposite strategy is also a viable option, with the main folders consisting of the departments responsible for the documents and subfolders separated by years. The main benefit to this is that filing cabinets or boxes can be stored in or near their appropriate department, making the documents easy to reference. However, without a centralized storage room, each department would need to secure the cabinets or boxes in some way. Additionally, arrangements would need to be made to ensure all departments are properly disposing of the documents after their retention period is complete.

4.5.3 Retention Schedules

Each record maintained by a government entity, including airports, is subject to a data retention schedule, which is usually determined by the entity’s state or local governments. Airports setting retention schedules should ensure they account for legal requirements, such as the state’s claim period for legal actions, or operational demands, such as project or service timeframes.

CCTV images make up a huge portion of the data maintained by airports. In many circumstances, data retention timeframes for archived images are set by external forces. For example, airports that received federal funding under TSA’s Advanced Surveillance Project must retain CCTV images for at least 30 days. Special rules apply to footage from LEO-worn body cameras.

In general, airports only keep information for the minimum amount of time required, usually destroying the information once the retention period is over. This allows the airport to free up storage space. The longer information is stored, especially in the case of video data, the more it will cost to store it.

Additionally, Open Records requests can become more of an administrative burden when there is more data to review and produce.

Airports should consult their legal counsel to determine local requirements for retention schedules and regularly review the schedules to ensure they continue to comply with applicable laws and ordinances.

4.5.4 Data Destruction Procedures

Security data should be properly destroyed when it reaches the end of its retention period. Typically, the information's classification or designation specifies the destruction requirements, but some state statutes specify the methods of destruction. PII, in particular, should be completely destroyed to prevent fraud and identity theft.[31]

Methods of destruction can include burning, pulverizing, or shredding of paper records and certain storage media (e.g., CDs and hard drives), and the erasure of digital records using the IT department's systems or special software. All storage devices should be digitally wiped before the equipment is physically destroyed with special machines.

Table 4-1 shows DHS-approved destruction methods for different categories of records.

Table 4-1. DHS-Approved Destruction Methods

Type of Media	Approved Destruction Methods
Paper	Shred or burn
Electronic File	Delete and empty recycle bin
Magnetic Media	Degauss or shred
Compact Discs	Shred and grind
Thumb Drives/Memory Sticks	Wipe and erase data
Microfiche: Audio/Video Tapes	Chemical (e.g., acetone bath) or shred
System Backups	Contact the PCII Program Manager
Other (e.g., databases or hard drives)	

Source: DHS, Protected Critical Infrastructure Information Program Procedures Manual, 2009

Many airports utilize a vendor to shred and dispose of records for a service fee. These companies provide shred bins for paper records, and often offer services to dispose of storage devices. Airports utilizing these service providers should perform due diligence to ensure the company complies with destruction requirements. This may include independent audits, an analysis of their performance record, and a review of the company's security policies.

Airports should consult with their legal counsel to establish their data destruction practices and ensure they comply with federal, state, and local requirements.

[31] The National Conference of State Legislatures has created a reference of state laws governing the destruction of PII: https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

4.6 Redact/Sanitize Information

In general, airports prefer to not redact or sanitize information that was not authored by the airport. They believe that it is the responsibility of the authoring body to release the information at the appropriate clearance levels. This is fairly common with federal documents, which often feature tear lines.

When airports need to share information at a lower clearance level (e.g., sharing SSI with frontline workers), many airports rely on their Chief of Police or legal department to redact the sensitive information. This helps ease concerns over unauthorized sharing of information, as the Chief and airport lawyers understand the legal requirements and often have experience redacting information.

It is common for airports to collect local intelligence based on observations, trends, and assessments of local and national events. Given that the airports collected and produced these analyses, they are the authority to appropriately assess how to share it. Even if the analyses discuss issues related to federal classified briefings, the results of the analyses are the work product of the airport and not subject to the federal classification.

Below are some examples of common documents and reports that airports may need to redact in order to share with their stakeholders:

- Security incident reports
- Police reports
- Badge office reports
- Security violations (financial and personal information)
- Airport access control schematics (maps of restricted areas)
- Security training materials
- Training records
- ASP
- Security staffing schedules
- TSA Vulnerability Assessments
- Security violation hearing decisions (written)

These reports often contain SSI and PII, which must be removed before sharing. Badge holders' names, social security numbers, dates of birth, and financial/account numbers (both bank and credit card) are examples of PII that may need to be redacted before further distribution. Airports should consult their legal department for state and local requirements governing PII protections, as they are different across the nation. Examples of information which may need to be redacted from reports include:

- Name/badge number
- Vehicle permit information
- Aviation security audit findings
- TSA regulatory inspection results
- Reference to TSA SDs or ICs
- Security equipment specifications

There are several methods to redact information from digital and physical documents. Redaction should ensure that the information cannot be read when held up to light, and that no part of the text is visible (i.e., top, bottom, or ends of the font).

Redactions made to physical documents should be photocopied and the photocopied version provided to the requester. Methods of redaction to physical documents include:

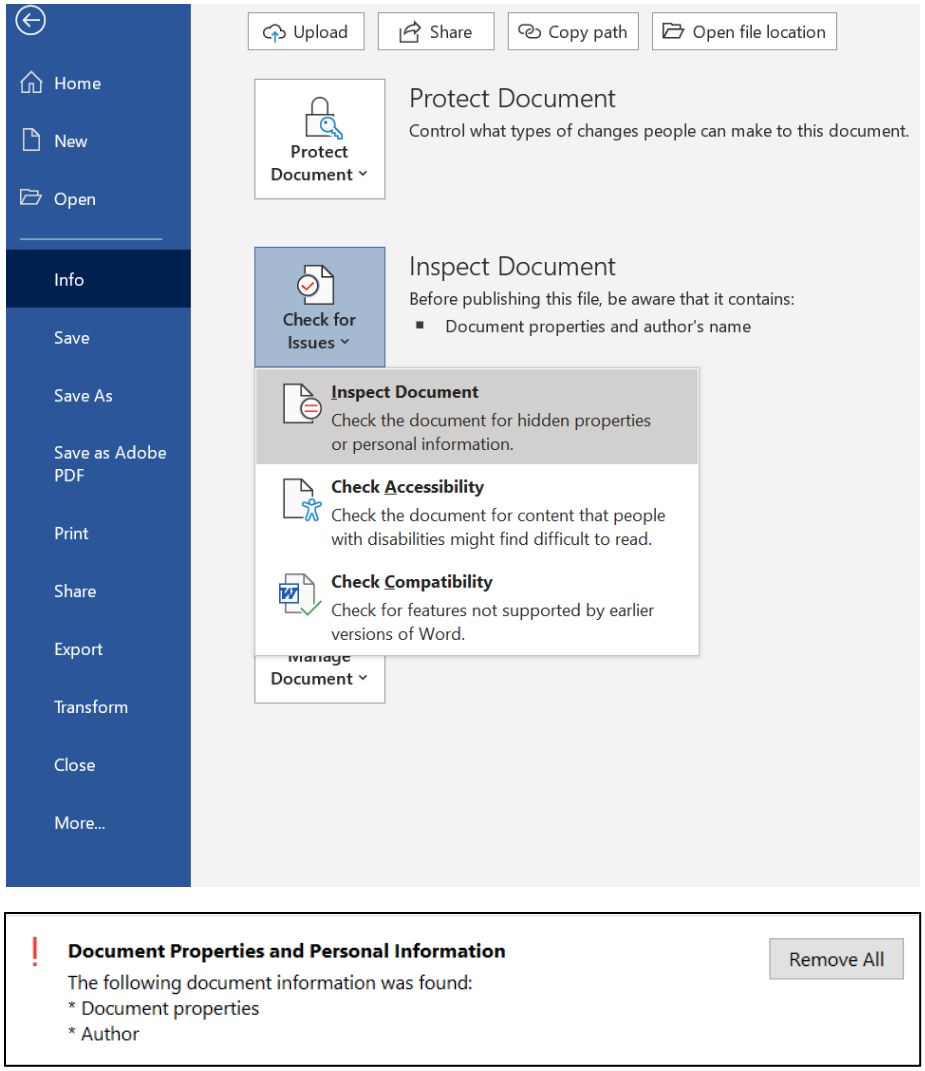
- Cover-up tape – can be used multiple times
- Black out/white out – use a black marker or correction tape
- Scalpel – cut the redacted information out of the sheet of paper

However, physical documents require extra effort and costs to print and ship to the requestor. Digital files can be more challenging to redact than physical documents because word processor and spreadsheet files contain metadata (information about the document and its authors), which often needs to be removed in addition to the actual text.

All redaction activities should be made to a copy of the file and never to the original. The National Archives and Records Administration recommends that digital information be converted to a plain text file before release to remove any metadata in the file. This can be done with programs such as NotePad on Windows machines and TextEdit on Apple machines.

Microsoft Word offers the ability to remove metadata as well through its Inspect Document feature. To access this feature, choose File, then Info, then Check for Issues, and finally Inspect Document, as shown in Figure 4-6. A pop-up message will ask you to choose which options to search for in the file. All options remove metadata in the file, but the most important option is Document Properties and Personal Information. Click Inspect and another pop-up will indicate the types of metadata in the document. Click Remove All to clear the metadata and then close the pop-up window.

Figure 4-6. Removing Metadata in Microsoft Word



Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware that it contains:

- Document properties and author's name

Inspect Document
Check the document for hidden properties or personal information.

Check Accessibility
Check the document for content that people with disabilities might find difficult to read.

Check Compatibility
Check for features not supported by earlier versions of Word.

Document Properties and Personal Information
The following document information was found:
* Document properties
* Author

There are a few options to redact documents using word processors, such as Microsoft Word, iWorks Pages, and WordPerfect. One option is to delete the restricted information and replace it with [redacted]. Another option is to highlight the restricted text using a black highlight color so that it appears as: [redacted]. After redaction with either option, the document should be stripped of metadata and converted to a PDF to preserve the document's formatting.

PDF is the preferred file type for transmitting digital files because it is more difficult to edit and modify. Some PDF programs, such as Adobe Acrobat, have tools and features to redact information and remove metadata as well as edit text. In this case, the restricted information could be deleted and replaced with [redacted].

Spreadsheets, such as files created in Microsoft Excel, iWorks Numbers, and Google Sheets, are redacted in a similar manner to a word document with [redacted] or black bars covering the information. These files should only be converted to PDF after removing the metadata, and not into TXT files as this will destroy the table format. If the spreadsheet contains multiple sheets, the relevant material should be exported as an individual sheet before redaction. If the spreadsheet contains equations, graphs, or other added content, these should also be reviewed during the redaction process to ensure they do not contain exempt information.

Airports should maintain a record of the information that has been redacted, especially if provided as an Open Records request. Maintaining a copy of the redacted material for future reference is considered good practice and may be useful if there are multiple requests for the same information or required audits.

No airport indicated that they redact video data for dissemination. However, the growing use of body cameras by LEOs may require airports to address policies for redaction. Without the proper systems and SOPs in place, redaction of video data will likely be an expensive and time-consuming process. Airports with LEOs using body cameras should consult their legal counsel to identify any state or local laws specifying body camera footage requirements, including redaction.

4.7 Use Tear Lines

A tear line is the point in a report where information that follows has been sanitized so that it may be disseminated at a lower security classification. The federal government frequently uses tear lines to share information between various departments, agencies, and individuals. The most common method is through a tear-line report with the more restrictive content in the body of the report and other versions of the information appropriate for a lower classification or designation in appendices.

Airports receive information at multiple clearance and designation levels from many sources. When the airport needs to pass this information on to other stakeholders, it may be difficult to share due to its classification or designation. Use of the tear-line approach may help airports share important information to more stakeholders.

In general, airports choose not to alter information shared from an outside entity (e.g., TSA). Most airports and airlines believe that it is the responsibility of the authoring body to create versions of the information at different tear-lines to make it easier and more appropriate to share. However, this could prevent stakeholders from learning information that could preempt a security incident.

A good practice for airports creating tear-line or lower security reports is to seek review and approval from the issuing entity. This will help alleviate potential concerns about oversharing. A small number of airports collaborate with their LEOs to review the information and remove any parts considered SSI or other SBU designation. This allows them to share information with the relevant stakeholders without sharing regulated security information. These airports also indicated that this is an infrequent practice, only used in special circumstances, and the new document is always vetted by TSA to ensure no SSI remains.

One CAT X airport creates their own internal security directives by sanitizing and converting SSI-related direction from TSA into operational instructions for relevant stakeholders. This has the advantage of tailoring the security guidance to the needs and requirements of specific stakeholder groups. The airport's directives are generally provided to stakeholders at stakeholder meetings where the guidance can be further explained if necessary.

The airport recognized that crafting documents to avoid including SSI material is often difficult and stressful. However, the airport concluded that tailoring guidance to specific needs and challenges achieved better security. The airport also has a dedicated compliance division that can focus the time and attention necessary to create the security directives in a way that clearly outlines the essential requirements without compromising the security of the information.

Airports can also apply tear lines to meetings. For example, an airport can host a security meeting consisting of stakeholders of all need-to-know levels (e.g., frontline workers up to law enforcement). The beginning of the meeting would discuss relevant non-SSI information. As the meeting progresses, individuals with lower levels of clearance can be dismissed so that more sensitive information can be shared.

4.8 Records Request Formats

Some airports require tenants and other stakeholders to request information through formal request processes, which allows them to define what information can be shared, to whom it can be shared, methods to share, and required protections. These often require the stakeholder to indicate a security reason to request the information. This is a particularly useful practice because it allows the airport to understand the security basis for the request and determine whether the stakeholder has a need to know the information requested.

Some airports require the stakeholder to request information through their state Open Records request process (see Appendix F). This could be detrimental to building trusting relationships, as information marked SSI is exempt from Open Records requests and must be redacted. It also removes the airport's ability to determine need to know, as Open Records requests do not require a reason for the request. Some airlines observed that requiring a security reason for the request could be a hindrance to information sharing between the two parties. However, failure to establish the need to know may expose the airport and the stakeholder to liability for improper sharing of SSI.

One CAT X airport provides a form for companies to request ACS data and reports. Information submitted on the form allows the airport to determine if the company has a legitimate security need for the information. The airport limits the types of ACS data that can be requested and outlines procedures for the stakeholders to receive the data. The airport uses the process to track the requests for auditing purposes, determine access authority for the system, and develop or negotiate additional processes or procedures.

Some airports expressed concern over receiving broad data requests from stakeholders, such as requests for ACS data. Those airports indicated that they sometimes needed to deny the requests because they lacked the resources to pull the information together into an acceptable format.

Another CAT X airport indicated it would only provide ACS data that has been interpreted for the requester by the airport; the airport never gives out the original ACS logs. This places a substantial resource burden on the airport, but allows the airport to remove any SSI or PII that is not required for the request.

4.9 Procurement and Construction Documents

Procurement documents and construction documents, such as ACS data and terminal blueprints, may include sensitive information. However, in order to complete projects, airports often have to share this information with companies and individuals that are often unknown to the airport.

One CAT I airport created a project procedures manual that contains requirements for protecting SSI during an airport project. The manual outlines several processes that must be implemented for each project, including:

- Assessing the need for SSI access
- Identifying the information to be accessed

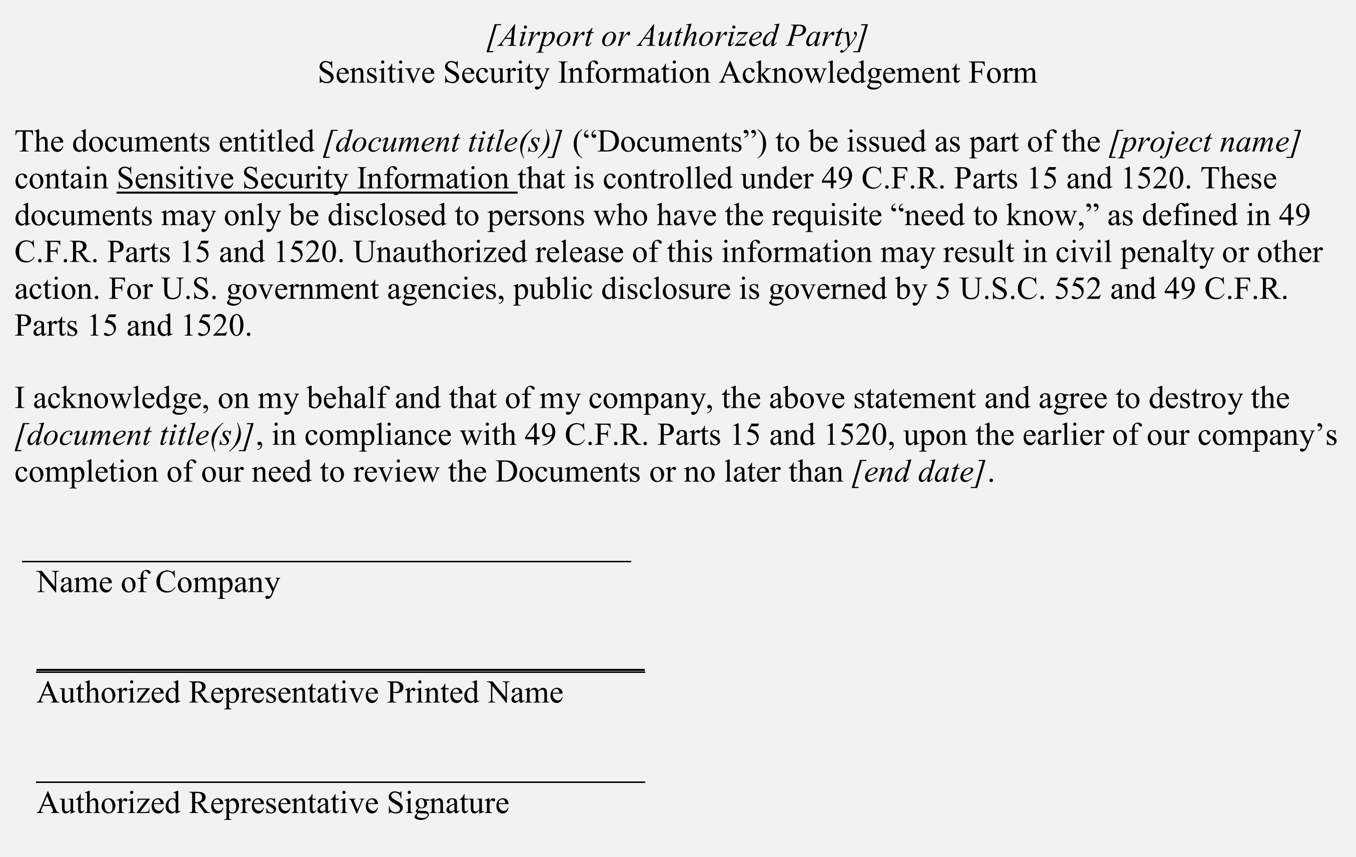
- Marking SSI by following the correct procedures
- Arranging for proper storage and transmission
- Performing background check requirements for anyone accessing SSI
- Documenting control measures, including stamping with control numbers and maintaining document control logs
- Executing transmittal memos for shared materials

The manual also outlines the steps to return or destroy SSI materials, includes timeframes for access to the SSI, and describes the correct procedures for marking and sharing SSI. This manual is primarily used to identify how information is being shared with contractors during security-related projects, such as ACS or physical security projects. Appendix G provides a redacted version of the airport's program to manage SSI during construction projects.

Procurement processes may require the release of SSI to bidders in order for them to accurately propose budgets and schedules. Most airports choose to only send sensitive information to bidders who have demonstrated that they are qualified to propose on the project. This is done through required pre-proposal meetings or Request for Information/Qualifications processes, which limit the number of individuals who need access to the sensitive information. Some airports may require the bidders to sign NDAs as well.

In some cases, airports simply require bidders to execute an acknowledgment form indicating they understand their obligations to control the information they receive. Acknowledgement forms do not offer the same level of protection as an NDA, but should be considered the minimum protection for information shared with bidders. Figure 4-7 shows an example of an Acknowledgement Form.

Figure 4-7. Sample of a CAT X Airport SSI Acknowledgement Form



[Airport or Authorized Party]
Sensitive Security Information Acknowledgement Form

The documents entitled *[document title(s)]* ("Documents") to be issued as part of the *[project name]* contain Sensitive Security Information that is controlled under 49 C.F.R. Parts 15 and 1520. These documents may only be disclosed to persons who have the requisite "need to know," as defined in 49 C.F.R. Parts 15 and 1520. Unauthorized release of this information may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. Parts 15 and 1520.

I acknowledge, on my behalf and that of my company, the above statement and agree to destroy the *[document title(s)]*, in compliance with 49 C.F.R. Parts 15 and 1520, upon the earlier of our company's completion of our need to review the Documents or no later than *[end date]*.

____
Name of Company

____
Authorized Representative Printed Name

____
Authorized Representative Signature

____________________ Title	____________________________________ Phone Number

____

Address, City, State, and Zip Code

Depending on the scope or sensitivity of the documents provided, an NDA or non-disclosure clause in procurement contracts may be more appropriate than an Acknowledgement Form. Figure 4-8 shows an example construction clause in an NDA.

Figure 4-8. Example Construction Document Clause from an NDA

"The *[airport]* is only willing to disclose and the Recipient may only use the SSI for the purpose of construction and any subsequent contracts relating to it. Recipient may only use the SSI for the purpose and may not use the SSI for its benefit or the benefit of others. The Recipient shall immediately upon the written demand of the *[airport]* return all documents and other materials and any and all copies thereof in the Recipients power and control, which constitutes the SSI."

Ideally, the airport's procurement department will cooperate with the airport's security department to determine if there are sensitive documents or information that the bidders require to create a detailed proposal. This not only protects the airport by creating a quality control process to check for SSI, but it also builds relationships between the airport departments and encourages participation in the airport's security culture.

A few airports require contractors and even contract bidders to complete SSI training to address responsibilities of individuals handling SSI or working in sensitive systems, such as the ACS or building systems. This provides the airports additional liability protection. Contractors working with systems handling PII are usually given simulated data for use in the system's testing environments.

One CAT X airport requires prospective bidders to review the documents in a secure room at the airport. The bidder is not permitted to take images of the documents (typically blueprints), but they are permitted to take notes. The airport has chosen to do this to narrow the number of bidders and protect the sensitive documents. The airport logs the individuals who view the document; only bidders who appear in the log may be eligible for the selection process. A log of everyone who viewed the documents is also helpful for investigation purposes if the information is ever made public.

REFERENCES

This reference section divides the literature resources reviewed during the research into seven sections:

- Federal and State Requirements – These documents discuss the federal classification schema and relevant information sharing state laws
- Federal Practices – These documents discuss federal recommendations and best practices for information sharing, as well as federal programs to facilitate that sharing
- International Practices – These documents discuss recommendations and best practices for information sharing from international organizations
- Non-Aviation Industry Practices – These documents discuss information sharing practices in non-aviation industries
- Digital Sharing and Cybersecurity – These documents discuss practices for sharing and protecting digital information
- Stakeholder Engagement – These documents discuss strategies for improving stakeholder engagement in information sharing programs
- Emergency Information Sharing – These documents discuss strategies for sharing information and building relationships during emergency situations

FEDERAL AND STATE REQUIREMENTS

Aviation and Transportation Security Act of 2001, Pub. L. 107-71, 115 Stat. 597.

> The Aviation and Transportation Security Act (ATSA) created the TSA. The agency is responsible for receiving, assessing, and distributing intelligence information related to transportation security.

Bureau of Justice Assistance. (n.d.). *Privacy and civil liberties policy development guide and implementation templates overview.* Bureau of Justice Assistance. Retrieved from https://bja.ojp.gov/program/it/privacy206 .

> This article provides guidelines on how organizations can develop a privacy and civil liberties policy.

Critical Infrastructure Information Act (CIIA) of 2002, codified at 6 USC §§ 131–134.

> The CIIA establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS.

Department of Defense. (2019). *DOD Freedom of Information Act (FOIA) Program*. (DOD Directive 5400.07).

> This document establishes policy and assigns responsibilities for the DOD FOIA Program.

Department of Homeland Security. (2009). *Protected Critical Infrastructure Information Program Procedures Manual.*

> This document discusses the DHS program to protect PCII, including methods for destroying physical and electronic information.

Federal Records Act of 1950, as amended, codified at 44 USC chapters 21, 29, 31, and 33.

> This Act requires each federal agency to manage the creation, maintenance, use, and disposition of records in order to achieve adequate and proper documentation of the policies and transactions of the federal government.

Freedom of Information Act (FOIA), codified at 5 USC § 552.

> FOIA allows for the full or partial disclosure of previously unreleased information and documents controlled by the U.S. government. The Act defines agency records subject to disclosure, outlines mandatory disclosures procedures, and grants nine exemptions to the statute.

National Conference of State Legislatures. "Data Security Laws." https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx.

This webpage provides links to each state's data security laws.

National Defense Authorization Act for Fiscal Year 2022, codified at Pub. L. 117–81.

Section 6423 of this act describes TSA's responsibility to create a formalized program for designating materials as SSI. This act also requires the TSA to make efforts to collect and document feedback from aviation stakeholders.

Presidential and Federal Records Act Amendments of 2014, Pub. L. 113–187, 128 Stat. 2003.

Amends the Federal Records Act of 1950 regarding the preservation, storage, and management of federal records to include the definition and management of electronic records. It also clarifies the Archivist's role as the final determinant of whether certain materials qualify as a federal record.

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

This book presents a detailed history of managing and handling sensitive and classified information within the federal government. It provides summaries of relevant laws, discussion of government agencies and offices dedicated to securing classified and controlled information , and considers some long-standing difficulties attending the management of security classified information.

Reporters Committee. "Open Government Guide." https://www.rcfp.org/open-government-guide/.

This webpage provides links to the Open Record laws in each state.

Winkler, Sophie. (2010). *Open Records Laws: A State by State Report.* National Association of Counties.

This report summarizes the Open Record laws in each state.

Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. (2011). Exec. Order No. 13587, 76 Fed. Reg. 198.

This Executive Order seeks to improve the governance of classified systems and reduce network vulnerabilities to ensure that the sharing of information between departments and agencies continues.

FEDERAL PRACTICES

Aviation ISAC. (2021). *Annual Cyber Risk Survey of Aviation Cybersecurity Leaders* 2021 Edition.

An annual survey of Chief Information Security Officers (CISO) to identify their most pressing cybersecurity risks and challenges. In 2021, the top five priorities for A-ISAC Member Company CISOs were identified as security operations center, identify and access management, culture and organizational security shift, network transformation, and asset/vulnerability management.

Department of Homeland Security. "Fusion Center Locations and Contact Information." https://www.dhs.gov/fusion-center-locations-and-contact-information.

This webpage provides links to each fusion center in the United States.

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

The Handbook provides guidelines to help DHS employees, contractors, interns, and consultants safeguard physical and electronic PII. It provides step-by-step guidance on identifying PII and simple instructions on encrypting, securing, and disposing of PII.

Domestic Security Alliance Council. https://www.dsac.gov/.

The DSAC website describes the Council's purpose and provides resources to industry stakeholders.

Federal Aviation Administration. (2010). *Airport Emergency Plan*. (AC 150/5200-31C).

This Advisory Circular provides guidance to airports on the development and implementation of an Airport Emergency Plan.

Francy, Faye. (2015). "The Aviation Information Sharing and Analysis Center (A-ISAC)."

This presentation presents the scope of the A-ISAC and progress to-date on meeting goals. The presentation briefly discusses strategies implemented to share information and forward documents to stakeholders.

Federal Bureau of Investigation. "Joint Terrorism Task Forces." https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces.

This FBI webpage discusses the purpose of JTTFs.

Office of Management and Budget. *Form UnNumbered InfraGard Application.* (OMB 1110-0049)

This agreement outlines the member's legal obligations to access the InfraGard program.

Lehocky, Stephen, Gloria Bender, and Jessica Gafford. (2008). *PARAS 0008 Synthesis: Findings and Practices in Sharing Sensitive Information.* National Safe Skies Alliance.

This report identifies successful practices at airports to share privileged information not classified by the federal government. The document provides findings and practices on effective ways that airports administer access, as well as control and recover information after it is no longer needed.

Overseas Security Advisory Council. https://www.osac.gov/.

The OSAC website offers resources for security information sharing.

Russell, W. W. (2020). *TSA and Airport Stakeholders Have Enhanced Airport Public Area Security, but a Plan Is Needed for Future Collaboration*. GAO-20-278.

This report describes actions the TSA has taken to enhance the safety and security of screening personnel and the security of airport public areas in response to the 2013 LAX shooting and the Gerardo Hernandez Act. The report discusses methods that airports, airport stakeholders, and the TSA have implemented to improve information sharing.

The National Archives. (2021). *Redaction toolkit: Editing exempt information from paper and electronic documents prior to release.*

This report discusses multiple methods to redact information from physical and electronic documents.

Transportation Security Administration. (2020). *2020 Biennial National Strategy for Transportation Security*.

This report highlights the TSA's efforts to improve information-sharing practices with its stakeholders.

Transportation Security Administration. *Sensitive Security Information: SSI Quick Reference Guide for DHS Employees and Contractors.*

This handout provides best practices for DHS government employees and contractors for handling SSI. This guidance is required of all DHS and component organization employees and contractors.

Transportation Security Administration. *Sensitive Security Information: Best Practices Guide for Non-DHS Employees and Contractors.*

This handout provides best practices for handling SSI for stakeholders and non-DHS government employees and contractors. Airports use these guidelines when handling SSI and sensitive information.

Transportation Security Administration. (2015). *SSI Policies & Procedures Handbook*, v2.0.

This handbook outlines requirements and recommendations for handling SSI.

INTERNATIONAL PRACTICES

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

The Aviation Security Manual was developed to assist states in promoting safety and security in civil aviation. Section 2.3 discusses general principles on managing and handling sensitive aviation security information.

United Nations. Archives and Records Management Section. *Records and Information Management Guidance: How do I protect sensitive information?*

This is a quick-reference guide for United Nations personnel to understand sensitivity classifications and seven tips for protecting sensitive documents.

NON-AVIATION INDUSTRY PRACTICES

Crosbie, W. L. (2008). *Public-Private Sector Passenger Rail Intelligence and Terrorism Information Sharing.* Monterey; Naval Postgraduate School.

This article provides methodologies on how a private passenger railroad can share intelligence and terrorism information with its external public partners.

Miller, P. E. (2005). *How Can We Improve Information Sharing Among Local Law Enforcement Agencies?* Monterey; Naval Postgraduate School.

This article highlights the benefits of information sharing to identify a series of events that could indicate criminal activity. Without information sharing, an incident may seem isolated, but by utilizing information sharing across agencies, law enforcement can have a more complete picture of what is occurring.

Sanchez, P. L. (2009). *Increasing Information Sharing Among Independent Police Departments*. Monterey; Naval Postgraduate School.

This article examines information-sharing networks and provides methods that can be utilized to improve information-sharing capabilities. The need for accurate information sharing in a timely manner is critical, especially in large urban areas such as Los Angeles County.

DIGITAL SHARING AND CYBERSECURITY

Cybersecurity & Infrastructure Security Agency. "CISA Services Catalog." https://www.cisa.gov/publication/cisa-services-catalog.

The CISA Catalog provides a list of all the services offered by CISA to support cybersecurity efforts.

Department of Agriculture (USDA). (2005). DM 3550-002. *Cyber Security Manual: Sensitive but Unclassified (SBU) Information Protection.* Chapter 10, Part 2.

This manual addresses the needs of cybersecurity professionals and other technical specialists useful in the protection of IT assets. It is designed to be both a policy roadmap and an operational document.

Harwood, D. I. (2014). *Barriers to Cyber Information Sharing*. Monterey; Naval Postgraduate School.

Cyber-information sharing is critical to defend digital networks, especially given their interconnectivity. This article outlines the barriers that private and public organizations face in information sharing, while providing solutions to overcome them.

Information Commissioner's Office. (2016). *The Guide to Data Protection*.

This guide was created for those who have day-to-day responsibility for data protection. It explains the purpose and effect of several guiding principles, gives practical examples, and answers frequently asked questions about data management.

PricewaterhouseCoopers. (2010). *Protect your organization's sensitive information and reputation with high-risk data discovery.*

This document is designed to sell PricewaterhouseCoopers' high-risk data discovery management services. However, it gives several examples of high-risk information and suggestions for IT services that would manage that information.

Riccardi, C. (2013). *Social Media Principals Applied to Critical Infrastructure Information Sharing*. Monterey; Naval Postgraduate School.

This article outlines how social media principles (e.g., the quick dissemination of information) can be utilized to share CII.

"Working Group 5: Cyber security information sharing June". (n.d.). Retrieved December 5, 2021, from https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf.

This article assesses the difficulties of cyber threat–information sharing. One of the biggest challenges is the variety of organizations that information needs to be shared with given overlapping responsibilities. Challenges can be organizational, operational, technical, consumer/market, financial, and legal/policy.

STAKEHOLDER ENGAGEMENT

Diana, T. (2021). "Improving messaging to airport community residents: An application of sentiment analysis to community engagement". Journal of Airport Management, 15(3), 304–312.

This article discusses strategies and methods to engage nearby airport communities in airport information. These strategies can be used to increase the security culture at and near airports.

Dulin, J. M. (2009). *The Components Necessary for Successful Information Sharing*. Monterey; Naval Postgraduate School.

This article highlights key elements of a successful information-sharing network, such as trust, leadership, and relationships. While law enforcement has fusion centers for information-sharing purposes, there are other non-law enforcement agencies (i.e., fire, EMS, and public health) that also need this information.

"How long should a board meeting last?" *Explainer*. Retrieved 25 March 2022. https://boardmaps.com/how-long-should-a-board-meeting-last.

This article discusses the science behind attention spans and offers strategies for creating a meeting that will engage participants.

Peacock, Cheryl. *Sign Blindness: A big risk to health and safety.* Seton

This report discusses sign blindness in safety and several good practices to mitigate this challenge.

Regnier, P. (2018). "Beyond the lease: True partnerships between airports and concessionaires." Journal of Airport Management, 12(2), 157–168.

This article identifies strategies to strengthen relationships and deliver results, including creating programs that build relationships within an airport, defining programs, firm scheduled meetings, measuring results, identifying stakeholder problem solving, and always celebrating success.

Rodriguez, L. de, et. al. (2017). *Guidebook for Preparing Public Notification Programs at Airports* (ACRP Report 170). Transportation Research Board.

This research outlines methods for notifying the public of important information. It offers considerations to reach individuals with disabilities and non-English speakers.

Rieder, R., et. al. (2018). *PARAS 0009: Guidance for Security Management Systems (SeMS)*. National Safe Skies Alliance.

This research focuses on SeMS practices at airports. These systems may have additional benefit by pushing important security messages to stakeholders during non-emergency situations.

Sanchez, D. (2019). “Innovative ideas for improving airport community relations.” Journal of Airport Management, 13(2), 174–185.

This paper focuses on airport strategies for creating a culture of trust, collaboration, and security with local leaders, organizations, and communities.

Seton. *10 ways to Combat Sign Blindness*.

This infographic summarizes ten good practices for mitigating sign blindness in safety.

Tansey, M. (2019). *Data Sharing in airports*: Mike Tansey: Accenture. WordPressBlog. Retrieved December 5, 2021, from https://www.accenture.com/us-en/blogs/compass-travel-blog/how-data-sharing-in-airports-can-transform-the-passenger-experience.

This blog highlights that if airports improve information sharing methods, then it will be the customer who benefits the most. It addresses some positive measures that some foreign airports have implemented to improve the travel experience for customers.

The 9/11 Commission Report - University of North Texas. (n.d.). Retrieved December 5, 2021, from https://govinfo.library.unt.edu/911/report/911Report.pdf.

This report identifies six problems recognized pre- and post-9/11: Structural barriers to performing joint intelligence work, lack of common standards and practices across the foreign-domestic divide, divided management of national intelligence capabilities, weak capacity to set priorities and move resources, too many jobs, and too complex and too secret.

Tollefsen, Roy-Andre. (2019). “The Meeting Rules of Engagement.” Trollandre. Retrieved 25 March 2022. https://www.trollandre.com/blog/2019/06/the-meeting-rules-of-engagement/.

This blog post discusses methods for creating the most efficient and effective meetings.

EMERGENCY INFORMATION SHARING

Fort Lauderdale-Hollywood International Airport. (2017). *Active Shooter Incident and Post-Event Response January 6, 2017: After-Action Report*.

This after-action report outlines the events of the January 2017 shooting at FLL. The report highlights the lack of communication and recommended that FLL improve relationships with their emergency partners.

Harrison, K. P. (2018). *Improving Information Sharing in the New York City Homeland Security Community*. Monterey; Naval Postgraduate School.

This article puts forward a conceptual model for multi-agency information sharing needs during a large-scale emergency. It is a case study of the 2017 Hurricane Maria response by NYC agencies.

Kipp, David and Dominic Nessi. (2017). *ACRP Report 182: Guidance for Planning, Design, and Operations of Airport Communications Centers*. Transportation Research Board.

This research offers guidance to airports planning or running a communication center. The guidance highlights the facility’s function in emergency situations as well as normal operations. Several successful examples are presented.

Krebs, C. (2018). “In an Interconnected World, We Stand and Fall Together.” Electric Perspectives, 43(5), 34–40.

This article discusses strategies and methods for organizations to work together and communicate before an emergency requires all participants to collaborate quickly.

Marcus, Leonard, Eric McNulty, Barry Dom, Joseph Henderson, and Lisa Flynn. (2018). *Meta-Leadership Lessons from the Response to the Boston Marathon Bombing*. The President and Fellows of Harvard University.

This case study examines the response to the Boston Marathon Bombings in 2013. The document identifies strategies and methods using the Meta-leadership framework to create a task force of government leadership, law enforcement, the public, and private organizations.

National Preparedness Leadership Initiative. https://npli.sph.harvard.edu/.

The NPLI website offers resources to incorporate a Meta-leadership into an organization's existing operational framework.

Southeast Airports Disaster Operations Group. https://seadogops.com/.

The SEADOG website provides resources to assist airports with recovery efforts.

Smith, James, Ken Kenville, John Sawyer. (2015). *Airport Emergency Post-Event Recovery Practices*. (ACRP Synthesis 60).

This document discusses airport practices for post-event recovery. Of note is the discussion of communication centers.

APPENDIX A: MOU WITH TSA OR AIRLINE FOR ACCESS TO CCTV IMAGES

MEMORANDUM OF UNDERSTANDING

TO:
FROM:
DATE:

SUBJECT: PERMITTING LIMITED ACCESS TO THE *[AIRPORT]* CLOSED CIRCUIT TELEVISION SYSTEM

THIS MEMORANDUM OF UNDERSTANDING TO PERMIT LIMITED ACCESS TO THE *[AIRPORT]* CLOSED CIRCUIT TELEVISION SYSTEM (the "MOU") is entered into by and between the *[Airport]* (the "Airport") and Department of Homeland Security, Transportation Security Administration ("TSA") / *[Airline]* (the "Airline") and shall be effective as of the date on which it is fully executed by the authorized representatives of both parties.

WHEREAS TSA/the Airline desires to obtain access to certain real-time video feeds from the Closed Circuit Television ("CCTV") system maintained by the Airport to allow TSA/the Airline to view areas in which it conducts operation; and

WHEREAS the Airport, pursuant to the terms and conditions set forth herein, is willing to provide TSA/the Airline with certain video feeds from the Airport CCTV system showing views of TSA's/the Airline's areas of operation;

NOW, THEREFORE, the Airport and TSA/the Airline agree as follows:

1. The initial term of this MOU shall be two years from the date of execution, unless earlier terminated by the parties pursuant to paragraph 9 below or extended by mutual agreement pursuant to paragraph 8. Upon the expiration of the initial term, the MOU shall be automatically renewed for a two-year period unless either party gives the other party written notice of its intent not to continue pursuant to paragraph 9 below. During any renewal term, the terms, conditions and provisions set forth in this MOU shall remain in effect unless modified in accordance with paragraph 8.

2. TSA/The Airline will purchase the equipment necessary to enable the viewing of the video feeds provided under this MOU, including *[describe equipment]*. The Airport will provide TSA/the Airline with credentials to enable the operation of the foregoing *[equipment]* to access the real time Airport CCTV video feeds described in the attached Exhibit A.

3. The Airport will assist TSA/the Airline with technical support necessary to enable the use of the *[equipment]* operated hereunder to access the real time Airport CCTV video feeds described in Exhibit A.

4. TSA/The Airline agrees that the *[equipment]* operated hereunder shall be used only on premises leased by TSA/the Airline at the Airport, only to access the video feeds provided to TSA/the Airline under this MOU and shall not at any time be connected to a network not provided by the Airport. One monitor, keyboard, and mouse (to be provided by TSA/the Airline) may be connected to each *[equipment]* operated under authority of this MOU. No other devices or media (including, but not limited to, WiFi, Internet, Intranet, thumb drives, external drives, or printers) shall be connected to the *[equipment]* operated under this MOU, or the feeds therefrom. TSA/The Airline shall not engage in, or permit any other person or entity to engage in, wireless monitoring, recording, copying, photographing, or any other means of

electronic reproduction of the video feeds provided hereunder. The Airport shall at all times retain ownership of the video images provided to TSA/the Airline pursuant to this MOU. Failure to comply with the terms and conditions contained in this Section 4 shall be grounds for immediate termination of this MOU without notice or opportunity to cure.

5. The Airport will use its best efforts to maintain the Airport CCTV system to consistently provide to TSA/the Airline the video feeds identified in Exhibit A. However, the Airport does not guarantee the continuity or quality of the video images provided under this MOU and reserves the right to modify or eliminate the fields of vision available under this MOU, as may be necessitated by changes in technology and equipment or the Airport's determinations regarding airport development or operations.

6. TSA/The Airline shall be responsible for all costs of labor and material associated with the installation and maintenance of any cabling, wiring, connections, and jacks needed to facilitate location of the *[equipment]* on TSA's/the Airline's leased premises and shall bear all costs related to the connection of the *[equipment]* to the Airport CCTV system. All installation and maintenance performed by or for TSA must be in compliance with the Airport Standards of Network, and as approved in advance by the Airport Electronic Systems Manager.

7. Presently, motion tagged video from the Airport's CCTV system is saved for 90 days. Upon request, the Airport Security Coordinator will provide TSA/the Airline with the policy for requesting a copy of a video recording obtained from the Airport's CCTV system.

8. Changes and modifications to this MOU shall be in writing executed by the authorized representatives of the Airport and TSA/the Airline. Any modification shall state the exact nature of the change or modification. No oral statement by any person shall be interpreted as modifying or otherwise affecting the terms of this MOU.

9. Either party may terminate this MOU at any time prior to its expiration date without incurring any liability or obligation by giving the other party at least thirty (30) days prior written notice of termination.

10. The Airport reserves the right to install on its equipment any security software or group policy it deems necessary or desirable to ensure the security of the Airport's platform.

IN WITNESS WHEREOF, and with the intent to be bound hereby, the parties have executed this MOU on the dates indicated below.

APPENDIX B: CASE STUDY: TECHNOLOGY-ENHANCED INFORMATION SHARING CENTER

This case study of an Airport Communication Center (ACC) at one CAT X airport offers a good example of technology-supported information sharing. It demonstrates the potential integration and interoperability with systems of external users, including local police and the TSA. The ACC offers an example of how the systems deployed in the ACC, which are common to many airports, can help collect and distribute a wide range of security information to internal and external stakeholders

ACC FUNCTION

The ACC collects and disseminates information for a wide range of sources, addressing several airport requirements. It uses a blend of technologies and sensors, such as:

- Cameras and alarms
- Communications systems – radio, telephone, paging, public address, and mass notification
- ACS
- Computer-aided dispatch (CAD)

These technologies provide situational awareness concerning critical operational areas inside the airport and along the perimeter, allow for evaluation of activity in the terminals and on the airfield, and provide logs of badge-holder activity throughout the airport. The ACC brings the sensor information into a single location for decision and action.

TECHNOLOGY SYSTEMS FOR INFORMATION SHARING

The following are descriptions of the major technology systems deployed in the ACC:

Telephony – The ACC communicates within and outside the airport using preset telephone talk groups to quickly connect stakeholders, such as airport operators and first responders, during emergencies. The system also includes 9-1-1 dispatch, public information lines, a direct phone line to the FAA tower, and employee call-in lines.

Radio Communication – The ACC has the capability to monitor and communicate up to six radio channels simultaneously, if needed. The radios connect to public safety personnel, including local and airport police and airport operations.

CAD – The ACC dispatches police and fire resources utilizing a CAD system. The airport is researching a move to a new CAD system that would align with the system utilized by their supporting police agency.

VMS – The ACC has access to camera views throughout the airport, which are collected and managed by a VMS. Intentionally designed and categorized camera workspaces provide quick review of most incidents by ACC personnel.

Physical Access Control System (PACS) – The airport uses a PACS with centralized control of all alarmed portals and gates to restricted areas of the airport. The system allows the airport to monitor the movement of badge holders and dispatch response personnel to investigate alarms.

Life Safety Alarms – The ACC monitors a number of life safety alarm systems, such as fire alarms, duress alarms, Automatic External Defibrillator cabinets, airport parking area alarms (blue light stations and a 911 emergency call line), and critical building systems across the airport campus. The ACC dispatches law enforcement or security to respond to and investigate the alarms.

Notification Systems – The ACC manages an automated notification system to send phone, text, and email notifications to airport stakeholders. Workflows and distribution lists allow dispatchers to quickly send messages to specific stakeholders.

Paging and Public Address – The ACC has the capability to make emergency notifications, public health advisories, or other public announcements using paging speakers deployed throughout the airport.

Lightning Detection/Monitoring System – The airport uses a lightning monitoring system to warn airport stakeholders to seek shelter, as well as initiate and terminate cease-fuel protocols.

Airport Transit Monitoring System – The ACC has a system for monitoring movements of the airport's tram system. This allows them to track the tram's movement throughout its journey and identify any potential mechanical issues.

OPERATIONAL FACTORS FOR TECHNOLOGY SUPPORTED INFORMATION SHARING

The ACC is located in a secure area of the terminal and is staffed 24/7. There are twelve operator workstations and two supervisory stations in the ACC. Typically, each shift staffs five dispatch personnel, two or three personnel to manage the public address, and one floor supervisor.

The workstation positions are numbered 1–12 and have the following principal responsibilities:

- Positions 1 and 2 are expansion positions that can be activated to expand ACC capacity in response to a major event or incident.
- Positions 3 and 4 are utilized to dispatch police; one position serves as a call operator and enters information into the CAD and the other position acts as the dispatcher.
- Positions 5 and 6 monitor radio traffic and dispatch other non-public safety resources, such as maintenance, and answer and log employee call-ins.
- Positions 7 and 8 are spillover positions that can be utilized for additional dispatch.
- Positions 9 and 10 are dedicated to tasks such as paging, public address, and answering non-emergency inquiries from the public.
- Position 11 monitors the tram movements and activities in the terminal areas.
- Position 12 monitors all access control alarms and handles incoming calls.
- The two supervisory positions monitor ACC functions and develop summary reports to assist upper management with decision making.

Redundancy is built into the positions to configure staffing to meet operational needs. The ability to handle calls for service or to address incidents and access cameras can be shifted among positions as required. The dispatch personnel are cross trained to work in any dispatch position.

The workstations are equipped with multiple monitors to display dashboard information and CCTV images.

TECHNOLOGY ENHANCED INFORMATION SHARING IN ACTION

The ACC receives and disseminates information from both internal and external stakeholders to maintain airport operations. The technology deployed in the center allows the staff to turn disparate information from multiple sources into actionable operations information.

The ACC monitors dispatch operations for city police operating in the vicinity of the airport. In one instance, ACC staff learned of a security incident off airport property. Though the incident itself did not affect the airport, the location of the incident was in the flight path of aircraft landing at the airport. The ACC contacted the FAA tower to warn them of the incident, and approaching aircraft were rerouted to an alternate runway. The ability to proactively monitor the dispatch activity adjacent to the airport helped to mitigate potential issues.

APPENDIX C: AIRPORT TENANT MEETING AGENDAS

Airport Tenant Meeting Agenda

[Date]

NOTE: This meeting takes place using the Microsoft Teams platform. The Teams meeting link will be distributed with the agenda prior to each meeting.

Airport Tenant Meeting at 10:00 a.m.

1) New Members or Guests
2) Airline Manager Council New Business
3) Airport Departmental Reports

Department	Representative
Airport Director's Office	
Airport Emergency Management	
Airport Operations	
Airport Planning & Compliance	
Air Service Development	
Buildings and Grounds	
Concession and Properties	
Engineering	
Environmental	
Fire / ARFF	
Marketing/PR	
Safety / Risk Management	

4) Miscellaneous and Follow-up Items
5) Closing Comments

Security Consortia Meeting 10:30 a.m.

6) Airport Security Report (Included)

EXAMPLE OF A TENANT MANAGER'S MEETING AGENDA

Tenant Manager's Meeting Agenda

[Date]

1. Welcome
2. Previous Meeting Debrief
3. Updates
4. Snow Removal Season Debrief
5. Parking Lot Management
6. Rental Car Agency Concession Agreement Extension
7. Terminal Art Rotation
8. Misc. Airport Updates
   a. Manager
   b. Operations
   c. Security
   d. Administration
9. Around the Room
   a. Air carriers
   b. Atlantic
   c. TSA
   d. Hangar tenants
   e. The Car Park
   f. Hertz
   g. Enterprise
   h. Avis

APPENDIX D: EXAMPLE NON-DISCLOSURE AGREEMENTS

EXAMPLE NDA FOR CORPORATE ENTITIES AND INDIVIDUALS

NONDISCLOSURE AGREEMENTS

FOR CORPORATE ENTITIES

THIS NONDISCLOSURE AGREEMENT (NDA) is entered into as of this _ day of _____ 20__ (the "Effective Date"), by ____ a corporation with a principal place of business at ____________________________________ ("Recipient"), concerning Confidential Information to be provided by the *[City]* ("City"), a municipal corporation, acting by and through its Airport Commission, the owner and operator of the *[Airport]* (the "Airport" or "Discloser").

FOR INDIVIDUALS

THIS NONDISCLOSURE AGREEMENT (NDA) is entered into as of this _ day of _____ 20__ (the "Effective Date"), by ____ an individual employee of ____________________________________ ("Recipient"), concerning Confidential Information to be provided by the *[City]* ("City"), a municipal corporation, acting by and through its Airport Commission, the owner and operator of the *[Airport]* (the "Airport" or "Discloser").

RECIPIENT hereby agrees as follows:

1. CONFIDENTIAL INFORMATION. The Airport will provide certain Confidential Information (as defined in this paragraph 1) to Recipient in order for Recipient to perform services for the Airport as specified under *[Airport Project]*. The Discloser and the Recipient intend that the furnishing of Confidential Information to Recipient will not render such information subject to public disclosure or disclosure to any third party. **"Confidential Information"** means any and all nonpublic information, written, electronic, or oral, relating to Airport technology, computer, or data systems, processes, or procedures, including but not limited to Private Information as defined under *[Local Administrative Code XXX]*, and Critical Infrastructure Information or Protected Critical Infrastructure Information as defined under the Homeland Security Act of 2002 and 6 CFR §29.2, which information or access to such information is supplied by the Airport or on behalf of the Airport to the Recipient or otherwise acquired by the Recipient during the course of dealings with the Airport and regardless of whether such information is in its original form, a copy, or a derivative product. **"Derivative"** means written or electronic material created from or with, or based on Confidential Information (i.e., a report analyzing Confidential Information shall also be considered Confidential Information). Confidential Information shall also mean proprietary, trade secret or other protected information, identified as Confidential Information by the Discloser. This NDA shall govern all Confidential Information provided to Recipient during the term of this NDA that Discloser has provided either directly, indirectly, or through access to Airport systems or data.
The Confidential Information furnished by Airport consists of: *[description of information]*

2. USE OF CONFIDENTIAL INFORMATION. Recipient agrees to accept Discloser's Confidential Information solely for use in connection with Recipient's duties in performing services for the Airport. Recipient shall not disclose, publish, or disseminate Confidential Information to anyone other than certain individuals on a need-to-know basis, as reviewed by the Airport. Recipient shall inform individuals having access to Discloser's Confidential Information of the confidential nature of this information and the restrictions on its use, dissemination, duplication and disclosure, and shall assume the responsibility that such employees, agents and contractors will preserve the confidentiality of such information as to third parties. Each employee, agent, and contractor of Recipient identified as having a need-to-know in connection with the receipt, review or evaluation of the Confidential Information shall be required to execute a Non-Disclosure Agreement under the same terms as stated in this NDA. Recipient shall provide Discloser with a copy of the executed Non-Disclosure Agreements and a master list of the employees, agents, and contractors and their respective duties in connection with the services involving Confidential Information.

3. **PROTECTION OF CONFIDENTIAL INFORMATION.** Recipient shall handle and safeguard Confidential Information in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information. The Airport has placed special confidence and trust in Recipient and Recipient is obligated to protect Confidential Information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which Recipient is granted access. Recipient understands that the Airport or other governmental entities may conduct inspections, at any time or place, for the purpose of ensuring compliance with the condition for access, dissemination, handling and safeguarding information under this Agreement. Recipient shall promptly report to the Discloser any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation Recipient has knowledge of, whether or not Recipient has direct involvement in such circumstances. Recipient's anonymity will be kept to the extent possible when reporting security violations.

4. **RETURN OF CONFIDENTIAL INFORMATION.** Recipient shall return or, with the express permission of the Discloser, destroy all tangible information obtained during the term of this NDA upon the earlier of **(a)** request of the Airport; **(b)** the completion of services to the Airport; or **(c)** two years from the date of this Agreement.

5. **OWNERSHIP OF CONFIDENTIAL INFORMATION.** The City owns all Confidential Information under this NDA. Recipient shall have no right, title, or interest in any Confidential Information. Nothing contained in this Agreement shall be construed as granting or conferring any rights by license or otherwise in any Confidential Information. This Agreement shall be binding upon the Recipient and its officers, directors, governing board, parent corporations, subsidiaries, affiliates, successors and assigns. In addition, all Confidential Information shall remain the exclusive property of Discloser, and Recipient shall have no rights, by license or otherwise, to have access to or use the Confidential Information except as expressly provided under this Agreement. No patent, copyright, trademark, trade secret, service mark or other legally protected proprietary right is licensed, granted or otherwise conveyed by this Agreement with respect to the Confidential Information.

6. **COMPLIANCE WITH COURT ORDER OR PUBLIC DISCLOSURE LAWS**. In the event that disclosure of Confidential Information is mandated by a court order or express governmental directive, Recipient shall immediately notify Discloser and shall take all reasonable steps to enable and permit Discloser to seek a protective order or take other appropriate action. Recipient will also, at no cost or expense to Discloser, cooperate in Discloser's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be afforded the Confidential Information. If, in the absence of a protective order, Recipient is required as a matter of law to disclose the Confidential Information, it may disclose to the party compelling the disclosure only the part of the Confidential Information required by law to be disclosed (in which case, where possible prior to such disclosure, Recipient will advise and consult with Discloser and its counsel as to such disclosure). Nothing in this Agreement shall require Recipient to take any action, or to refuse to release information where to do so would violate applicable law.

7. REMEDIES. Recipient acknowledges and agrees that violation of this NDA shall constitute a material breach of this NDA and may be grounds for termination of this and any underlying or related contract for services involving the use of Confidential Information. Violation of this NDA may be grounds for denying further access to any Airport Confidential Information. Violation of this NDA may also result in administrative debarment and/or civil or criminal action. Discloser shall be entitled to specific performance and injunctive and other equitable relief, in addition to any other remedies or money damages available at law or in equity.

8. INDEPENDENT KNOWLEDGE. This NDA imposes no obligation upon Recipient with respect to information which: **(a)** was in Recipient's possession before receipt from Discloser; or **(b)** becomes a matter of public knowledge through no fault of Recipient; or **(c)** is received by Recipient from a third party without a duty of confidentiality; or **(d)** is disclosed by Recipient with Discloser's prior written approval; or **(e)** is developed by Recipient without reference to Confidential Information.

9. NO REPRESENTATIONS AND WARRANTIES. Discloser makes no representation or warranty as to the accuracy or completeness of the Confidential Information and Recipient agrees that Discloser and its employees and agents shall have no liability to Recipient resulting from any access to or use of the Confidential Information.

10. NO WAIVER. If the Discloser fails to enforce any right or remedy under this Agreement, that failure is not a waiver of the right or remedy for any other breach or failure by the Recipient.

11. AGREEMENT MADE IN [STATE]; VENUE. This NDA shall be governed by and construed in conformance with the laws of the State of *[State]*. Venue for all litigation relative to the formation, interpretation, and performance of this NDA shall be in *[City*].

12. AUTHORITY. The undersigned representative of Recipient represents and warrants he/she has the requisite power and authority to enter into this Agreement on behalf of the Recipient corporate entity.

13. ENTIRE AGREEMENT. This Agreement: **(a)** represents the entire NDA with respect to the Confidential Information; **(b)** may be modified only by written amendment signed by the Recipient's officers or authorized designees; and (**c**) contains headings for reference only; these headings have no effect on any provision's meaning.

14. SEVERABILITY. Should the application of any provision of this NDA to any particular facts or circumstances be found by a court of competent jurisdiction to be invalid or unenforceable, then **(a)** the validity of other provisions of this NDA shall not be affected or impaired thereby, and **(b)** such provision shall be enforced to the maximum extent possible so as to effect the intent of the Discloser and Recipient and shall be reformed without further action by the Discloser or the Recipient to the extent necessary to make such provision valid and enforceable

EXAMPLE OF AN NDA PROTECTING SBU INFORMATION

NON-DISCLOSURE AGREEMENT (NDA)

[Airport]

NON-DISCLOSURE AGREEMENT (NDA)

CONDITIONAL ACCESS TO SENSITIVE SECURITY INFORMATION (SSI)

AND/OR PROPRIETARY INFORMATION

WHEREAS the undersigned (the Recipient) will be receiving from *[Airport],* Confidential Information, providing a product or service to *[Airport]* that involves or requires access to *[Airport]* designated sensitive security information and/or airport operational security systems, must execute this Non-Disclosure Agreement (NDA).

NOW THEREFORE in consideration of receiving the Sensitive Security Information (SSI) and/or *[Airport]* Confidential and Proprietary Information from *[Airport]* the Recipient agrees as follows:

1. Proprietary Information, Confidential Information and/or Sensitive Security Information (SSI) means all information disclosed, whether disclosed on or before the date hereof or upon any subsequent date in connection with the Purpose and whether disclosed orally, visually or in any tangible or electronic form.
2. SSI is protected from disclosure by state and /or federal law and is information that if released, may pose a threat to transportation security. SSI includes, but is not limited to, information about transportation security measures and requirements, security vulnerabilities and vulnerability assessments, the technical specifications of certain *[specify type]* equipment, and other information pertinent to aviation security that the Recipient may be granted access to in performance of its obligations and duties with *[Airport]*. On behalf of the Recipient and its employees:
    a. As used in this Agreement, SSI includes that information defined in 49 CFR Part 1520 but also includes any information not specifically mentioned in Part 1520 but marked as “sensitive security information” or “SSI”.
    b. The Recipient understands that by being granted access to SSI, the Recipient is obligated to protect this information from unauthorized disclosure, in accordance with the terms of this agreement and all applicable laws.
3. The Proprietary Information, Confidential Information and/or Sensitive Security Information (SSI) which has been or will be provided to the Recipient will be held by the Recipient in strict confidence, will not be disclosed, directly or indirectly, to any third party, except with the prior written consent of *[Airport]* or unless required by lawful order of a court or regulation authority having jurisdiction over the parties to be disclosed (Lawful Order).
4. Where disclosure of any of the Proprietary Information, Confidential Information is required by Lawful Order, the Recipient shall promptly inform *[Airport]* thereof and shall use all reasonable efforts to minimize such disclosure and to obtain an undertaking from the receiving party to maintain the confidentiality of such. Except with the written permission of the Administrator of the Transportation Security Administration (TSA) unauthorized release of information may result in civil penalties or other actions, therefore, requests for SSI information must be referred to the TSA.
5. The Recipient may disclose the SSI to those of its representatives, consultants, and employees who have a need-to-know the SSI for the Purpose provided that prior to disclosure the Recipient will

inform each such recipient of the confidential nature of the information and cause such a third party to enter into a written Non-Disclosure Agreement with respect to such SSI substantially the same as the obligations set out herein. The Recipient will not make notes of, copy or reproduce any Proprietary Information, Confidential Information and/or SSI in any form except as previously agreed upon in writing by *[AIRPORT]*.

6. The obligations of the Recipient set out herein shall commence effect at the time which Recipient first receives or received any SSI and shall continue in full force and effect for a term expiring *[term limit]* from the date hereof.
7. Nothing contained herein derogates, diminishes or otherwise displaces the common law duty of the confidentiality vested in the undersigned concerning the Proprietary Information, Confidential Information and/or SSI received from *[Airport]*.
8. This Acknowledgement of Non-Disclosure and confidentiality is binding upon the Recipient’s successors is not assignable and shall be governed by the laws of the *[State]*.
9. The invalidity or unenforceability of any provision of this Agreement or of any covenant herein contained shall not affect the validity or enforceability of any other provision or covenant shall be deemed to be severable.

The corporate agreement is entitled, Non-Disclosure Agreement, Conditional Access to Proprietary Information, Confidential Information and/or Sensitive Security Information. The corporate agreement shall be signed by the President or Chief Executive Officer of the Recipient.

DATED this day of ___________________________, 20___

I have the express authority to sign this agreement and hereby consent to all of the conditions stated herein, in consideration of my being granted conditional access to certain information that may contain *[Airport]* Confidential and/or Proprietary Information and/or Sensitive Security Information (SSI) that is owned by, produced by, or in the possession of *[Airport]*.

Company Name ____

Company Address ____

Company Phone ____

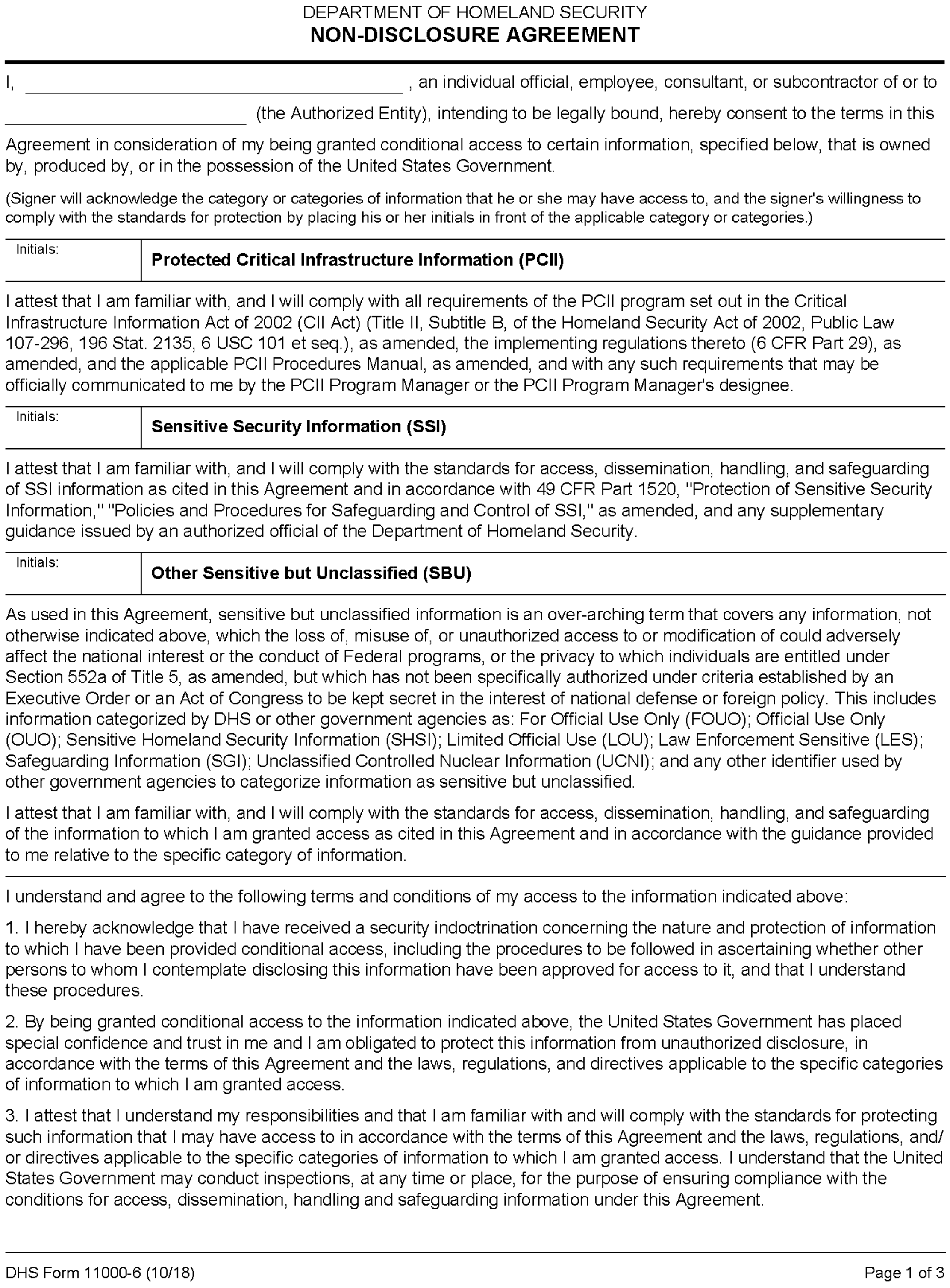
Title of Recipient ____

Print Name ____

Signature ____

WITNESS (Print & Sign) ____

DEPARTMENT OF HOMELAND SECURITY NDA TEMPLATE



DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

I, ______________________________________ , an individual official, employee, consultant, or subcontractor of or to ________________________ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

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

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

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

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

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

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

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

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

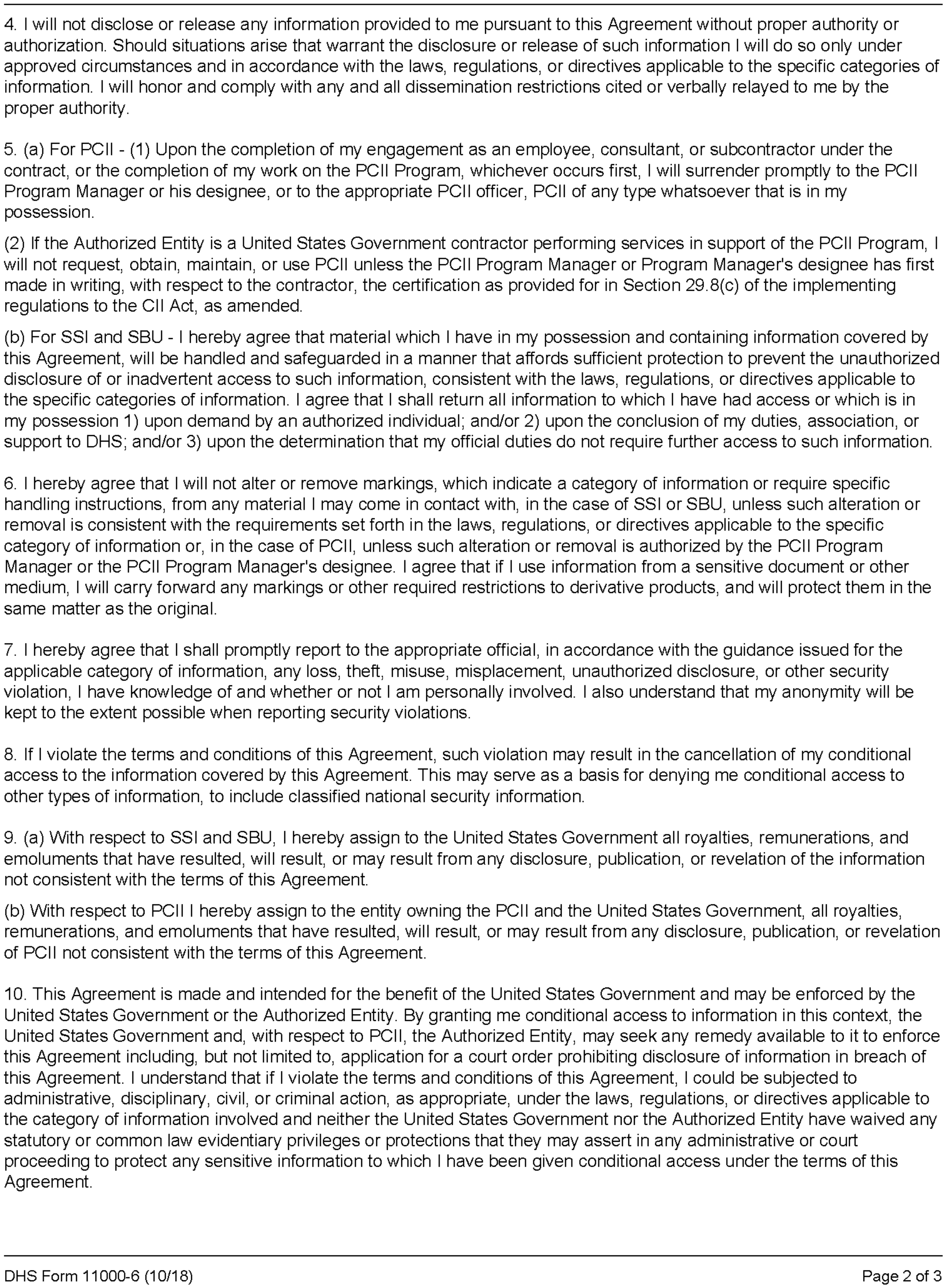
I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

DHS Form 11000-6 (10/18) Page 1 of 3



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

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

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

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

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

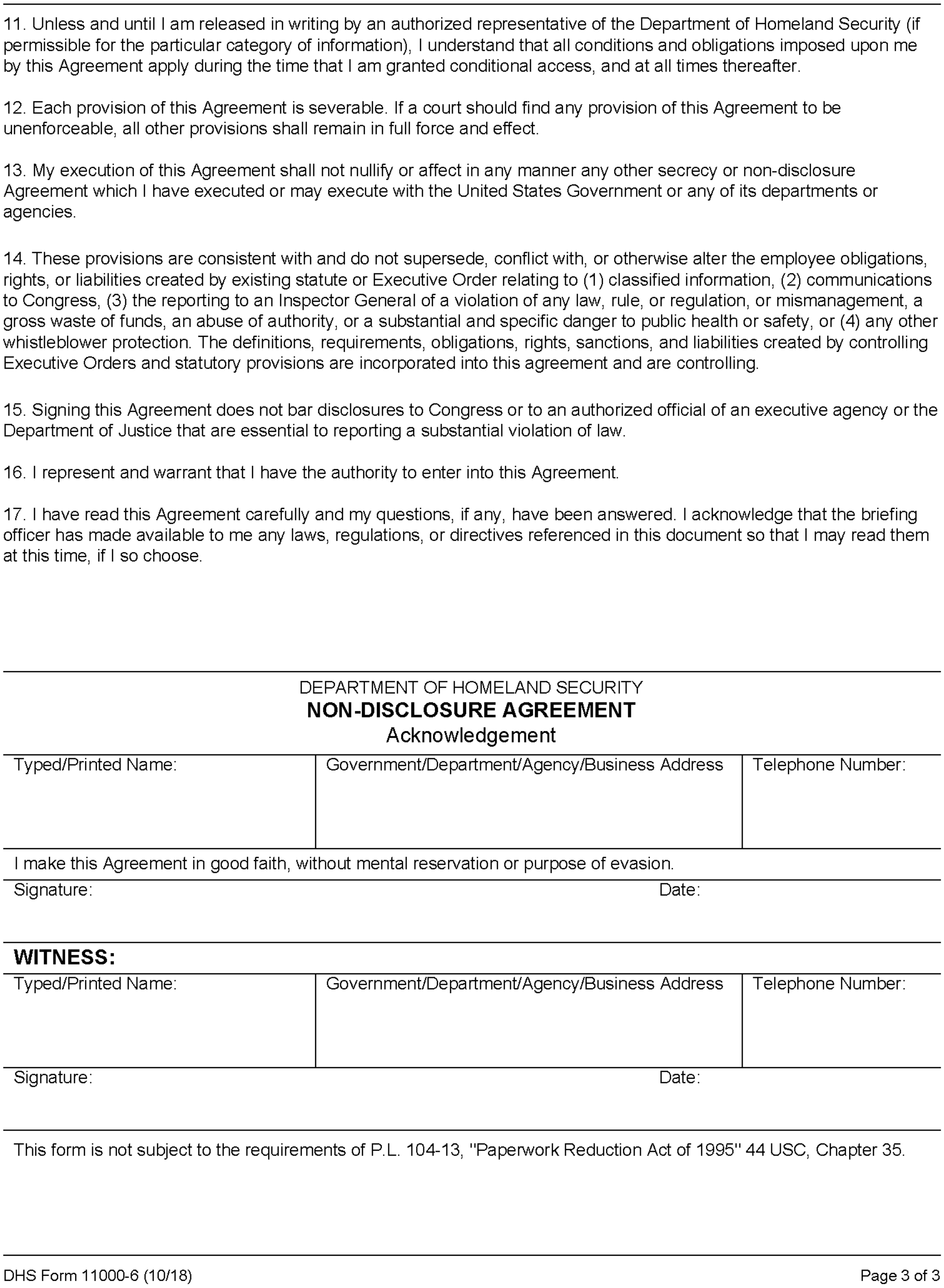
7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

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

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

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

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



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

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

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

14. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive Order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive Orders and statutory provisions are incorporated into this agreement and are controlling.

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

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

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

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Acknowledgement

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:
I make this Agreement in good faith, without mental reservation or purpose of evasion.		
Signature:	Date:	

WITNESS:

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

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.

APPENDIX E: EXAMPLES OF INFORMATION RECEIPT FORMS

[Airport] Tenant ASP Acceptance Acknowledgement Form

I hereby certify that the following individual has received the *[Airport]* Airport Security Program (ASP).

Printed Name: ______________________________ Date: __________

Authorized Signatory
or Manager Signature: ____

□ Tenant (Authorized Signatory or Manager) is responsible for updating their copy of the ASP with any and all changes the airport provides via electronic or paper format (print and replace in the ASP binder)

□ The ASP is considered SSI (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 the 49 CFR parts 15 and 15820, except with the written permissions of the Administrator of the Transportation Security Administration, or the Secretary of Transportation. Unauthorized disclosure may result in civil penalty or other action. For U.S. Government agencies, public release is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Authorized Airport Signature: ___________________________ Date: ______________

Airport Security Program Distribution

Date _______________

Airport Security Program (ASP)

I (Print Full Name) ____ acknowledge receipt of the *[Airport]*, Airport Security Program. Information contained within the ASP will only be distributed to those persons with an operational need-to-know. While not in use the ASP will be stored in a secured/locked location.

ASP Volume Number: ____

Organization/Employer: ____

Print Name: ____

Signature: ____ Date: __________________

Return of ASP

Airport Security
Coordinator Signature: ____ Date: __________________

APPENDIX F: RESPONDING TO OPEN RECORDS REQUESTS

Since the passage of the Freedom of Information Act (FOIA),[32] there has been a great expansion of public access to governmental records. Currently, all fifty states and the District of Columbia have some form of legislation that governs the public's access to records. Many of those laws are modeled after the federal FOIA statute. In 2010, the National Association of Counties (NACo) created a comprehensive summary of state laws in the *Open Records Laws: A State by State Report* (the 2010 NACo Report).[33] The report offers an excellent summary of state statutes that control disclosure requirements for airports in their respective states.

The 2010 NACo Report notes that the general structure of state FOIA provisions contain the following features:

- Designation of who may request records and reasons for which requests can be made
- Identification of the records protected under the law (including specification of the particular entities covered)
- Fees and costs that can be assessed to requestors
- Enforcement and sanction provisions to ensure compliance
- Designation of records that are exempt from disclosure
- Provisions respecting production of digital records
- Limitation on profit in connection with providing requested data

The 2010 NACo Report includes excellent summary charts outlining the general requirements of each state's FOIA provisions.

The extent of records and type of data that can be obtained by Open Records requests can vary greatly from state to state. However, all jurisdictions have exemptions from the requirement to produce records, including protected categories such as national security information, certain categories of law enforcement information, trade secret information, and information that if released would constitute a violation of personal privacy. The federal SBU designations were designed to help protect this type of information from state Open Records and FOIA requests. While the exact parameters of any exemption may vary between states, those statutes will likely protect most security or law enforcement information from disclosure, as well as most PII.

Accordingly, airports should carefully evaluate the legal environment around Open Records in their respective state and locality. Helpful resources include the 2010 NACo Report and the airport's legal department. The Open Government Guide, maintained by the Reporters Committee for Freedom of the Press, is also a comprehensive resource for airports to view state-by-state analyses on Open Records laws.[34]

It is important that airports be mindful of the Open Records requirements in their state, which may specify the length of time that data must be retained, types of data that must be provided, time limits for

[32] 5 U.S.C. § 552

[33] **Open Records Laws: A State by State Report:** https://irp.cdn-website.com/4365c51b/files/uploaded/Open%20Records%20Laws.pdf

[34] **Open Government Guide:** https://www.rcfp.org/open-government-guide/

responding to requests, and whether associated costs can be transferred to the person or entity making the request.

49 CFR § 1520.9 (a)(3) requires airports to report third-party requests for SSI through Open Records processes to the TSA.[35] This may be relatively simple for documents marked SSI, but can be much more difficult for unmarked data, such as CCTV images. Airports should coordinate with TSA to make determinations on how to handle unmarked data that may be SSI.

REQUEST REQUIREMENTS

Most airports respond to Open Records requests submitted through their local or city government records department. However, some airports have policies that outline the requirements and processes for requesting various types of airport data. This practice allows the airport to clearly define the requirements of the requestor when filling out the form, as well as define limitations to the types of information that can be provided.

In general, requiring requesters to be very specific about what data they need and why will make it easier for the airport to fulfill requests. Under most state Open Records laws, burdensomeness can be an exemption to production of records, though in many states this objection is viewed with skepticism by the courts. Better framing of requests may help address these types of challenges. Seeking additional detail from the requester might also reduce the number of requests in addition to making responses more manageable.

It should be noted that, in jurisdictions with fewer Open Records exemptions, stakeholders may have more access to information without the protections of an NDA to limit subsequent dissemination. This may result in airport stakeholders using those processes to circumvent official procedures to obtain information. Legally, there are very few methods to deny Open Records requests for non-exempt information. Airports should consult with their legal counsel about security concerns over Open Records disclosures.

DIGITAL RECORDS

When most Open Records laws were created, record keeping was typically done through paper systems, and production generally involved physical photocopying of records. With the development of digital record-keeping systems and growing collections of digital sensor data, such as video, responding to Open Records requests has become more complex. As the 2010 NACo Report discusses, most states include digital records and items, such as video recordings, as requestable information. There is also a growing body of state law requiring the production of metadata that is associated with digital information.

CCTV Images

Airports will likely receive requests for access to and copies of recorded images. Most airports have an administrative process in place for airport stakeholders and the public to request, view, and download images on a need-to-know basis. Exemptions for disclosure can be asserted if the information is security sensitive.

If the information is not security sensitive, some airports have had success in reducing their Open Records burdens by bring requesters into the security office to view the images under supervision. The data never leaves the airport's possession. This may work for smaller airports with less expansive CCTV

[35] *SSI Policies and Procedures Handbook*, (2015)

systems, but such a system might prove unmanageable at larger airports. However, if the images are non-exempt, in most circumstances the requester will be entitled to receive a copy.

Producing digital records can be time consuming and costly. The administrative burden and costs of producing copies of video data and fulfilling records requests should be considered if the airport is allowed to set data retention limits. The longer data is retained, the higher the cost to the airport for storing the data and processing requests.

Access Control Data
In some jurisdictions, ACS data can be the subject of Open Records requests. However, the almost exclusive security nature of the ACS and its integration with PII provide grounds to object to a request for that data.

Data Review
The administrative burden to respond to Open Records requests has also grown significantly and has placed pressure on airport security departments that must process those requests. In general, a response for digital information requires the ASC and airport legal personnel to review the information requested. Depending on the area of the airport where the information is focused, or the general policy set by the local TSA, the TSA may need to review the information as well. If an Open Records request involves video of a checkpoint or other TSA operational area, TSA will almost certainly insist on conducting a review.

At one CAT X airport, the TSA requires review and approval of requests for any video images from security cameras inside the airport before the images may be released. This is due in part to the security risk of the requester identifying camera locations and blind spots.

Technology Considerations
The existence of Open Records requirements may shape how an airport operates its information collection and sharing systems. Airports procuring new technology that will interface with sensitive data may consider what features would be helpful to respond to common Open Records requests.

For example, because video footage takes up a large amount of data storage space, it is in the airport's best interest to retain the minimum amount of data required. It also serves to mitigate the administrative burden for Open Records production. However, if reduced retention time is not possible, there may be other technological solutions to address capacity concerns. Airports may choose features in their video surveillance system that can help with this, such as video compression software to shrink the file size or cloud-based storage to move the storage off premises. Alternatively, airports may use fewer cameras and access control sensors to reduce the cost of retaining the associated data. Also, some IDMS may allow the airport to create reports quickly and easily with unnecessary or exempt information automatically redacted.

One CAT X airport created an automated portal where requests can be made for video review and dissemination. This helps the airport meet request demand as well as track and catalog the requests. It also reduces the administrative burden of inputting information from a written form, reduces input errors, and reduces the time needed to track down missing field information.

RESPONSE PERIOD AND CONTENT

Most Open Records statutes have specified time periods for response to a request that vary from state to state. To ensure that responses are completed within this period, a process should be established for all necessary entities (legal, security, TSA) to review requests, redact information as necessary, and respond to the requester. If all or any part of a request is denied, the response should state the reason and cite the specific statutory exemption(s) that prohibit disclosure or release, and include the organization’s administrative appeals process available under a statute, if applicable.

REQUEST FEES

The assessment of fees to complete an Open Records request may help pay for the resources needed to fulfill requests as well as reduce the number of requests. However, many cities and states have restrictions on implementing fees such as this. Airports should consult their legal department to determine available options.

APPENDIX G: EXAMPLE OF SSI SHARING PROGRAM FOR CONSTRUCTION PROJECTS

Project Procedures Manual

A. OBJECTIVE

To limit the exposure of designated Sensitive Security Information to properly authorized personnel.

B. DEFINITION

Sensitive Security Information (SSI) is information and documentation designated by the Transportation Security Administration (TSA), and identified by the *[Airport]*, Aviation Security and Public Safety (AVSEC/PS), or applicable *[Airport]* Contractors, as important to the security of *[Airport]*, its employees and the public. SSI includes, but is not limited to, materials related to the Vulnerability Assessment, Blast Analysis, Passenger Screening, Baggage Screening Projects, Video Surveillance (CCTV / DVMS) and Access Control.

C. REFERENCES

1. 49 CFR Part 1520 – PROTECTION OF SENSITIVE SECURITY INFORMATION
2. 49 CFR Part 1542 – AIRPORT SECURITY
3. TSA SSI Quick Reference Guide
4. TSA SSI Best Practices Guide

D. WORK PROCESS

1. As part of Project Setup, the PROJECT TEAM makes recommendations on Sensitive Security Information (SSI). AVSEC/PS reviews and approves. If there will be SSI documentation, it is indicated on the Project Setup Form.

2. Any incoming or outgoing documentation, identified as SSI, must include the following header and footer on each page:

   Header:

   Sensitive Security Information

   Footer:

   "WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."

3. All SSI documentation in physical format is stored in locked cabinets at all times, when not in use. The procedures for distribution and control of keys are subject to audit by the Director of AVSEC/PS or designee.

4. All personnel requiring access to SSI documentation must have a ten (10)-year fingerprint background check and Security Threat Assessment (STA) on-file with AVSEC/PS, or have an alternate AVSEC/PS approved security clearance, at the time access is required.

5. If copies are required, DOCUMENT CONTROL will create the copies. DOCUMENT CONTROL stamps each copy with an assigned control number. DOCUMENT CONTROL logs the controlled copy on the SSI Control Log that includes:

   a. SSI Control Number
   b. Office of Record
   c. Project Number
   d. Date Received
   e. Sender
   f. Date Sent
   g. Recipient
   h. Description
   i. Notes
   j. Date Returned
   k. Date Destroyed

6. The Recipient must review and sign the applicable SSI Release Transmittal. This Transmittal for either internal or external recipients contains directions for proper handling of all SSI documentation. DOCUMENT CONTROL then releases the SSI documentation.

   a. Internal recipients – Airport Staff only: DOCUMENT CONTROL will create and maintain a designated SSI Folder with restricted permissions. Those granted access would receive a link to the location of the SSI documentation from DOCUMENT CONTROL.

   b. External recipients – All Non-Airport Consultants and Contractors: Unless otherwise instructed, all SSI documentation with the exception of hard copies will be provided by OneDrive and it will be password protected (following DHS password requirements) and the password noted by DOCUMENT CONTROL on the SSI Control Log. The password is emailed via Outlook to the Recipient under separate cover. If applicable, DOCUMENT CONTROL hand delivers the SSI, either digital or paper, to the Recipient. Please note prior authorization from both the Department Manager and AVSEC/PS is required to provide SSI via email.

7. Once distribution is made, the SSI Release Transmittal and all SSI documentation are maintained in a secured folder and hard copies locked in secured cabinet by DOCUMENT CONTROL, or the OFFICE OF RECORD if applicable.

8. For physical formats, the Recipient has 30 days to review and return the SSI documentation. For copies sent via OneDrive or email, it is the Recipient's responsibility to destroy. At the end of 30 days, DOCUMENT CONTROL will email a notice for any outstanding SSI documentation to be returned or destroyed. If necessary, a second email is sent with a courtesy copy to the PROGRAM MANAGER. Further failure to return/destroy the SSI documentation will be escalated to AVSEC/PS.

9. If required by the Director of AVSEC/PS or designee, audits of controlled items are conducted by DOCUMENT CONTROL for all SSI documentation, including distributed copies.

10. All SSI documentation remains in a designated locked cabinet or in a secured folder until destruction. At the time of destruction, DOCUMENT CONTROL provides SSI copies to the Authority Shredding Service, observes the shredding and notes the destruction date on the SSI Control Log. Destruction of SSI originals follows Airport guidelines in consultation with AVSEC/PS.

E. ATTACHMENTS

A SSI Control Log
B SSI Release Transmittal

ATTACHMENT A: SSI CONTROL LOG

SSI Control Number	Office of Record	Project Number	Date Received	Sender	Date Sent	Recipient	Description	Notes	Date Returned	Date Destroyed Y/N and/or Date

ATTACHMENT B: SSI RELEASE TRANSMITTAL

Sensitive Security Information (SSI) Release Transmittal

Date: (Month), (Day), (Year)

To: (Name), (Title), (Company)

From: (Name), (Title), (Company)

Control Number: (SSI Number)

Items: (Description)

You are being provided documentation as indicated below that has been identified as SSI:

- □ Hard copy
- □ Flash drive
- □ CD
- □ Email
- □ OneDrive

All documentation in electronic format is in a secured location and you will be granted access after you complete this form

Hard copy– Will be provided upon completion of this form

“WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.”

Please initial where indicated to acknowledge and confirm you will abide by the SSI requirements:

SSI documentation is for intended Recipient only Initial ____________

SSI documentation is to remain at the address sent to Initial ____________

SSI documentation is not to be shared Initial ____________

SSI documentation is not to be downloaded to any device Initial ____________

SSI documentation is not to be reproduced in any form Initial ____________

SSI documentation is to be locked in a secure location (i.e., file drawer, safe, cabinet) when not is use Initial ____________

SSI documentation is not to be taken home unless you receive approval in advance from the sender Initial ____________

SSI documentation is to be returned after 30 days Initial ____________

SSI documentation provided via email is the Recipient’s responsibility to destroy Initial ____________