PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0047 August 2023

Practices and Considerations For Centralized Revocation Database Use

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Sean Cusson
Del Ray Solutions, LLC
Alexandria, VA

Don Zoufal
CrowZnest Consulting, LLC
Chicago, IL

Michele Freadman
M. Freadman Consulting
Attleboro, MA

Jessica Gafford
Andy Entrekin
TransSolutions
Fort Worth, TX

Margaret Martin
Martin Airport Law
Nashville, TN

Kate Coleman
Arlington, VA

Mary Ann Pantle
Rochester, IL

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 0047 PROJECT PANEL

Frank Capello *Broward County Aviation Department*
Hodari Davenport *Port of Seattle*
Antonella de Filippis *Massachusetts Port Authority*
Keith Jackson *Hartsfield-Jackson Atlanta International Airport*
Abedoon Jamal *San Francisco International Airport*
Sarah Pilli *American Association of Airport Executives*
Adrienne Washington *Metropolitan Knoxville Airport Authority*

AUTHOR ACKNOWLEDGMENTS

The Project Team is thankful for all the airport operators that graciously took time out of their day to meet with our team and discuss their use of CRD. These interviews provided us with recommended practices and further direction to lead our research and writing.

CONTENTS

TABLES & FIGURES

PARAS ACRONYMS

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Office
CFR	Code of Federal Regulations
COO	Chief Operating Officer
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
IP	Internet Protocol
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

ASAC	Aviation Security Advisory Committee
ASC	Airport Security Coordinator
CHRC	Criminal History Records Check
CRD	Centralized Revocation Database
FPRD	Fingerprint Results Distribution
HSIN	Homeland Security Information Network
ID	Identification
NA	National Amendment
QRG	Quick Reference Guide
SAVE	Systematic Alien Verification for Entitlements
STA	Security Threat Assessment
USCIS	United States Citizenship and Immigration Services

SECTION 1: INTRODUCTION

Airport operators continue to implement and refine their practices related to the *Centralized Revocation Database for Individuals with Revoked Identification Media TSA-NA-21-01A*. TSA issued the National Amendment (NA) in February 2021 in response to the TSA Modernization Act. The act required that TSA, in consultation with the Aviation Security Advisory Committee (ASAC), establish a database of individuals who have had their airport credentials revoked for failure to comply with an airport's security requirements. Effective implementation of the new Centralized Revocation Database (CRD) by airport operators will provide another tool to identify and mitigate insider threats.

Airport operators have novel issues to consider in their credentialing programs as they implement CRD use practices. Credentialing programs that airports have developed to comply with 49 CFR §1542 requirements vary drastically based on an airport's security posture, governance model, business strategies, resources, size, and state and local laws. Based on the variety of factors that affect these programs and their tailored nature, airports must develop customized policies and practices for CRD use.

Objective

The objective for this research was to assist airports in making informed decisions regarding their policies and practices for CRD. This report will outline considerations and factors shown in Table 1.

Table 1. Considerations for CRD Use

Considerations	Factors
Revocation of credentials	Violation and penalty structure (defined vs. discretionary)
	Single vs. cumulative violations
	Appeals or hearing processes
	Legal considerations
Entering information into the CRD	Roles and responsibilities
	Internal coordination (e.g., between airport compliance team and credentialing office)
	Provision of adequate and consistent entry information for future decision making
Use of CRD findings	Roles and responsibilities
	Adjudication policy (initial issuance and continued eligibility)

The project team collected information from airport stakeholders regarding CRD, and has identified key trends, considerations, and findings. This work included:

- Review of publicly available, original source documents such as credentialing applications, rules and regulations, and notices to tenants or credential holders
- Review of relevant literature, regulations, and laws
- Review of the 2015 TSA ASAC Report on Access Control
- Interviews with airports and airlines
- Attendance at two aviation security industry conferences
- Discussions with airport stakeholders about CRD at those conferences
- Meetings with multiple TSA stakeholders

Document Layout

Section 2: CRD Overview
This section discusses the origination of CRD and its intended purpose.

Section 3: Revocation of Credentials
This section considers the complexities of revocation, including the permanence of revocation decisions, reasons for revocation that may or may not result in CRD entry, and due process surrounding credential revocation.

Section 4: Entering Information into the CRD
This section explores best practices for CRD data entry, including creating workflows and quick reference guides, ensuring information entered is useful and accurate, and maintaining records of CRD entries to assist in potential future inquiries.

Section 5: Use of CRD Findings
This section discusses use of CRD findings, including collecting applicant information, conducting suitability determinations, and properly documenting practices and decisions.

Section 6: CRD Fit into the Broader Airport System
This section discusses how an airport's governance, security, and business strategies may affect how it employs the CRD.

Section 7: Summary of Findings and Considerations
This section summarizes the primary research findings.

Section 8: Additional Research Needs
This section identifies potential future research topics.

SECTION 2: CRD OVERVIEW

Origination

In 2014, an airline employee was arrested for using their access privileges to smuggle hundreds of guns onto commercial aircraft.[1] In 2015, TSA's Acting Administrator requested that the ASAC conduct a comprehensive review of the incident and identify other potential vulnerabilities to determine if additional risk-based security measures, policy revisions, or resource reallocations were needed. The ASAC convened a Working Group on Airport Access Control to carry out this task.

Employee vetting was a major focus of the Working Group's 2015 *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*[2] and resulted in multiple recommendations. Specifically, the report recommended that TSA create and maintain a national database of individuals who have had their airport or airline-issued identification media revoked for cause related to security requirements. TSA approved this recommendation.[3]

Congress codified the recommendations in the FAA Reauthorization Act of 2018, where it directed TSA to establish a national centralized database containing the names of individuals who have had airport or aircraft operator–issued credentials revoked for failure to comply with aviation security requirements.[4] Further, Congress directed TSA to establish (1) a reporting mechanism for airport operators, air carriers, and foreign air carriers to submit data regarding these individuals to TSA; (2) a process to access the database; and (3) a process to allow an individual whose name was mistakenly entered into the database to correct the record by having their name expunged from the database.[5]

Purpose

The CRD was created to close an existing security vulnerability. Potential existed for an aviation worker to have their credentials revoked for violation of a security rule and then apply for a new badge at another airport or airline without their past violation being disclosed. Absent a system like the CRD, the new airport or airline would have no way of knowing about the employee's actions and credential revocation at the first airport.

The CRD provides airports with a structured information exchange regarding applicants' history of credential revocation for non-compliance with aviation security requirements. This strengthens airports' ability to conduct more thorough risk assessments of individuals and make informed suitability decisions by considering the reasons for credential revocations at other airports. The CRD platform allows the information to be accessed and disseminated quickly with limited effort on the part of airports and aircraft operators.

---

[1] "Former baggage handler sentenced for smuggling loaded firearms onto aircraft," Press Release, U.S. Attorney's Office, Northern District of Georgia, accessed August 15, 2022, https://www.justice.gov/usao-ndga/pr/former-baggage-handler-sentenced-smuggling-loaded-firearms-aircraft.
[2] See "Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control," Report, TSA ASAC, accessed August 5, 2022, https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf. (Hereinafter ASAC WG Report).
[3] TSA-NA-21-01A.
[4] FAA Reauthorizations Act of 2018 § 1934.
[5] *Id.*

Using the CRD to Evaluate Suitability and Manage Insider Threat Risk

Effective vetting is one of the most critical tools used to determine an individual's suitability and the level of risk they pose to the organization and the air transportation system. The CRD is an addition to other mandated assessment tools, such as fingerprint-based criminal history records checks (CHRC), the FBI's Rap Back program, and security threat assessments (STA) performed by the TSA. Other tools are employed by airports within their individual jurisdictions. For example, some airports may conduct name-based criminal history checks, as not all fingerprints of individuals who are arrested or arraigned are submitted to the FBI. Additionally, airports can use the US Citizenship and Immigration Service Systematic Alien Verification for Entitlements (SAVE) database, which provides an individual's immigration status.

In assessing the risk of an individual to hold credentials granting access to airport SIDA and Sterile Areas, it is prudent to think of it as a risk continuum. Airports begin their suitability assessments with the mandated regulatory baseline of CHRC, Rap Back enrollment, and STA, as mentioned above, and can deploy additional checks based on their risk assessments. The risk continuum uses various data points to assess and determine risk based on available and legally permissible information. The CRD represents an additional datapoint on this continuum. Additional information regarding aviation workers' prior conduct or other relevant background information allows for more informed risk-based access suitability decisions.

SECTION 3: REVOCATION OF CREDENTIALS

The NA's definitions for revocation and surrounding processes do not align with many airport's existing penalty structures. This has created ambiguity regarding the permanence of actions taken, what types of enforcement actions require entry into the CRD, and how appeals processes may affect CRD entry. Regarding each of these issues, airport operators should work with their legal counsel to determine how their penalty structures harmonize with federal regulatory requirements.

Permanence

The term Final Cancellation used in the NA's definition of revocation has been interpreted by many airports to mean permanent. Determining the permanence of credential revocation decisions of an airport may be best understood by evaluating the difference between suspension and revocation. Many airports' penalty provisions distinguish between suspensions for a limited period and complete revocations of unescorted access rights without a right to a reinstatement. In this respect, the penalties are like the point system used for driver's licenses in many states. When a license is suspended, the privileges are automatically restored or are eligible to be restored at the conclusion of the suspension period. When the license is revoked, the former license holder does not have any expectation that privileges will be restored. That is not to say they could not subsequently apply for the privileges again, but there is no guarantee they will be granted. Additionally, the prior revocation may be considered in the determination to grant future privileges.

The essential question airport operators should ask in assessing permanence of revocation is whether the individual has any legal expectation that their unescorted access privileges will be restored. Given that there are fixed periods associated with the issuance of credentials for unescorted access privileges (up to a maximum of two years), any termination of those access privileges beyond the expiration date might be fairly characterized as a revocation. If an airport operator chooses to follow this approach, it would be advisable to seek review by counsel and input from the TSA.

For CRD purposes, an airport may want to consider changes to its rules and regulations, penalty structures, or suitability determinations to match CRD requirements and language. For example, some airports define the requirements for credential revocations while some only suspend credentials for short periods of time. Others may focus on monetary fines as opposed to access-based penalties, and some allow airport managers enforcement discretion on a case-by-case basis. Appropriate changes will assist airports in better using the CRD in the manner they choose while maintaining compliance. Where that approach cannot be taken, airports should develop adjudication processes that harmonize their rules on revocation with CRD requirements.

Security Violations

Some airports expressed concern when assessing whether actions were directly related to a security violation, since it is rare that credentials are revoked based on a single event. This concern manifests itself in two different ways: in instances where revocation penalties were imposed for multiple reasons, and in cases where the penalty might result from an evaluation of multiple offenses over time. Similarly, airport operators expressed confusion in managing the relationship between security violations and disqualifying criminal offenses.

The key to CRD reporting should be related to the underlying nature of the violation resulting in revocation. In cases where there may be multiple reasons for revocation, some of which may be reportable as a security violation and some not, the airport may consider consulting with their legal

counsel and TSA to determine if CRD entry is required and, if so, how the basis of the revocation should be worded.

Consider the following examples:

Example #1: **An employee is caught speeding on the airfield and is cited with a minor safety violation.**	The employee is also found to have a knife, which is prohibited item, in his possession. After a hearing on the offenses, his credentials are revoked.
	If the security violation (possession of a knife) is an independent basis for revocation, then a CRD would clearly be appropriate.
	If revocation is only the result of the combined security and safety violation, the airport may want to consult with counsel and even the TSA to determine whether a CRD entry is appropriate.
Example #2: **While driving on the airfield, an inidvidual intentionally commits a runway incursion by taking a shortcut across the airfield to attend a meeting.**	When the individual is stopped on the airfield, his badge is found in his jacket pocket rather than properly displayed.
	He is charged with a major safety violation (runway incursion) and a minor security violation (failure to properly display his badge). At the hearing, his credentials are revoked.
	If the minor security violation would not have ordinarily warranted a revocation, the airport might choose not to enter the revocation into the CRD because it was the major safety violation and not the minor security violation that likely informed the basis for revocation.
	As with the previous example, the airport would be well advised to confirm its decision regarding necessity for CRD entry with legal counsel and perhaps consultation with TSA.

Carefully documenting decision-making policies, processes, and standards will provide airports with justifications for their decisions in these cases. Airports should also properly document and maintain records of decisions and processes related to revocations. The documentation should include any evidence regarding the conduct that is available; analysis of the airport's considerations for revoking the credentials; and correlations to policies, processes, and standards for penalties. Any pre- and post-revocation documentation will assist in countering any challenges to the revocation, because it will be easier to show that the decisions were made within the airport's policy.

A similar problem may occur when airports' penalty structures are predicated on multiple disciplinary offenses over time. While revocations at some airports can occur after one violation of certain rules, a common approach in many airports is to look at the range of conduct over time. This may include progressive penalty models, where revocations may become a possibility after repeated violations, or three-strike models, where termination of privileges occurs after a specified number of infractions within a certain period.

Each approach presents an interesting challenge because some of the underlying conduct considered in the revocation decision may not be "security-related" misconduct, as is demonstrated by the examples above. In airports where these penalty structures exist, the airports should work with their counsel, and

possibly with TSA, to ensure that the revocation decisions can be fairly characterized as security-related violations.

Disqualifying criminal offenses, whether disclosed in a CHRC or Rap Back notification, are not a basis for a CRD entry by themselves. The CRD User Guide clearly indicates that a revocation based on either grounds should not be reported in the CRD.[6] Similarly, Rap Back notifications or other disqualifying criminal offense notices for arrests or charges that occur off airport would not qualify for CRD entry.

However, airports may need to report security violations that relate to criminal activity. If an individual violates a security rule that results in a revocation, and the conduct is charged as a crime, it is reportable in CRD. Here, the airport will have revoked the credentials based on an airport security violation and the criminal activity is tangential.

Consider the following example. A person carries a gun through a security checkpoint and is arrested, resulting in a Rap Back notification. If the airport revokes the person's credentials solely because they receive a Rap Back notification, and a security violation was not identified, entry in the CRD would be improper. However, if the airport revokes the badge based on the conduct of "carrying a gun through the checkpoint"—an independent airport security violation warranting revocation—that activity is reportable.

Similarly, if the airport gets a Rap Back notification for someone who is convicted for robbing a grocery store, a revocation based solely on those grounds would not be entered in the CRD. However, if the airport had a security rule requiring individuals to report all arrests and convictions for criminal activity, and the individual failed to report the conviction, a subsequent revocation of their credentials based on the failure to report could be entered in the CRD. While this offense is related to the Rap Back notification in that the notification evidences the existence of the unreported conviction, the revocation for failure to report the conviction qualifies for entry into the CRD.

Airports reported that individuals typically return their badge prior to enforcement when a violation occurs that would result in a credential revocation. These individuals either quit or are transferred by their company. The ability of airports to enter information into the CRD for individuals who voluntarily surrender their badge to avoid revocation action is unaddressed by the NA.

Due Process

The procedures established in the NA have created some confusion for airports trying to ensure that their internal penalty procedures meet the procedural requirements specified in the NA. There is some concern over the word "appeal" in the definition of the term "Hearing" and in the description of the "Hearing Process."[7]

Airports need to ensure that individuals whose credentials have been revoked have been given the opportunity to appeal the revocation through a hearing process prior to entry into the CRD.[8] The NA

[6] Initially some airports thought that both actions should be entered in the CRD. TSA through the CRD User Guide clarified the fact that revocations based on these grounds should not be reported. CRD User Guide at p. 6.
[7] See TSA-NA-21-01A.
[8] The U.S. Supreme Court has addressed the issue of what type of procedures meet due process requirements in many contexts. The Court has noted that those requirements vary by the interest affected by government action. Addressing those concerns in an analogous context of employment termination, the Court concluded that providing an employee with notice of

establishing the CRD was designed to ensure that federally mandated due process rights are respected. The requirements of due process apply to government actions taken against the protectible interests of individuals. Those protectible interests are often unique creations of state and local laws. The policies and procedures for issuance of credentials at any given airport may create different requirements for what revocation process is due. While this guide provides a general introduction to the concept of due process, airport operators need to consult with their legal counsel to determine how due process rights can be addressed.

The NA also includes language that has suggested to at least one airport that individuals may have some due process rights over the decision to place them in the CRD, though those procedural requirements are not well defined. One of the airports interviewed created and enacted a separate review process for the decision to place someone in the CRD. In most airports, this process was merged with the underlying decision to revoke the credentials. The decision to place the individual in the CRD is treated as a required action initiated by the decision to revoke the credentials.

Due Process

Due process rights are procedural protections afforded to individuals before a governmental entity can impose a decision affecting legal rights or privileges. With respect to the CRD, the following areas of due process are implicated:

- What process, if any, is a person entitled to before their credentials can be revoked by an airport?
- What process, if any, must be afforded to an individual to have their name removed from the CRD?
- What process, if any, must be afforded to an individual whose name is in the CRD to grant or withhold credentials?

Generally, an appeal is an action requesting higher-level review of a legal decision. Appeals occur after a determination is made in a hearing, not as part of the hearing process. Some airports have appellate review of hearing decisions on credential revocations, but others do not have any formal review beyond the hearing. The NA is clear that there is a three-day requirement for data entry after a final determination. Airports should consult with their counsel and consider implementing a policy that requires entry of qualifying revocations into the database within three days of any of the following events:

- After a decision in a hearing on revocation, unless an appellate review is requested after the hearing[9]
- After an individual chooses to forgo the request for a hearing or abandons the opportunity to have a hearing
- After the final decision in any appellate review of the revocation decision or after an abandoment of the apellate review process

The structure, detail, and formality of due process policies and procedures varies significantly among airports due to factors including local authorities, resources, business strategies, and governance models. In some cases, the processes are codified in an ordinance or regulation. In others, they are outlined in

allegations and an opportunity to be heard was adequate to meet the constitutional due process requirements. Even in that context, the Court noted that proceedings could be informal. *Cleveland Board of Education v. Loudermill*, 470 U.S. 532 (1985). This procedural requirement only applies in cases where the individual has a protectable property right or interest. In the case of the retention of unescorted access privileges or airport credentials, it is unclear whether interest held by the individual rises to the level of a protectable property interest.

[9] This exception would only apply to those airports that afforded a right to appellate review after a hearing. With respect to those circumstances, airports may need to consider the time afforded individuals to exercise appellate rights. Where no appeal is filed within the time period allotted, the hearing should be considered to be final.

employee handbooks. Some appeals are conducted in writing, and some are conducted in person. Some policies have extensive protections for credential holders, affording them the right to representation and a hearing before a hearing officer and a right to appeal. Others provide for informal proceedings before an Airport Security Coordinator (ASC). Some policies and practices include input in the decision-making process from a range of airport stakeholders, and some rely solely on the judgement of security personnel.

Many of the airports interviewed during the research indicated that their procedures for imposing penalties were not matters that could be easily addressed by the security department. Changing existing rules concerning the revocation of credentials could only be done at the highest level of governance within the airport, or required action by external organizations (e.g., city councils or county boards). This would involve legal review and other administrative actions, which would be time consuming, lengthy, and cumbersome. Outside of developing processes for data entry into the CRD, no airport indicated that they had felt the need to make changes to the existing revocation process to address the NA. In only a few cases did airports formally develop new procedures to address due process issues created by the NA. Those changes largely concerned notification of CRD entry requirements as an additional consequence of revocation but not a change in existing revocation processes.

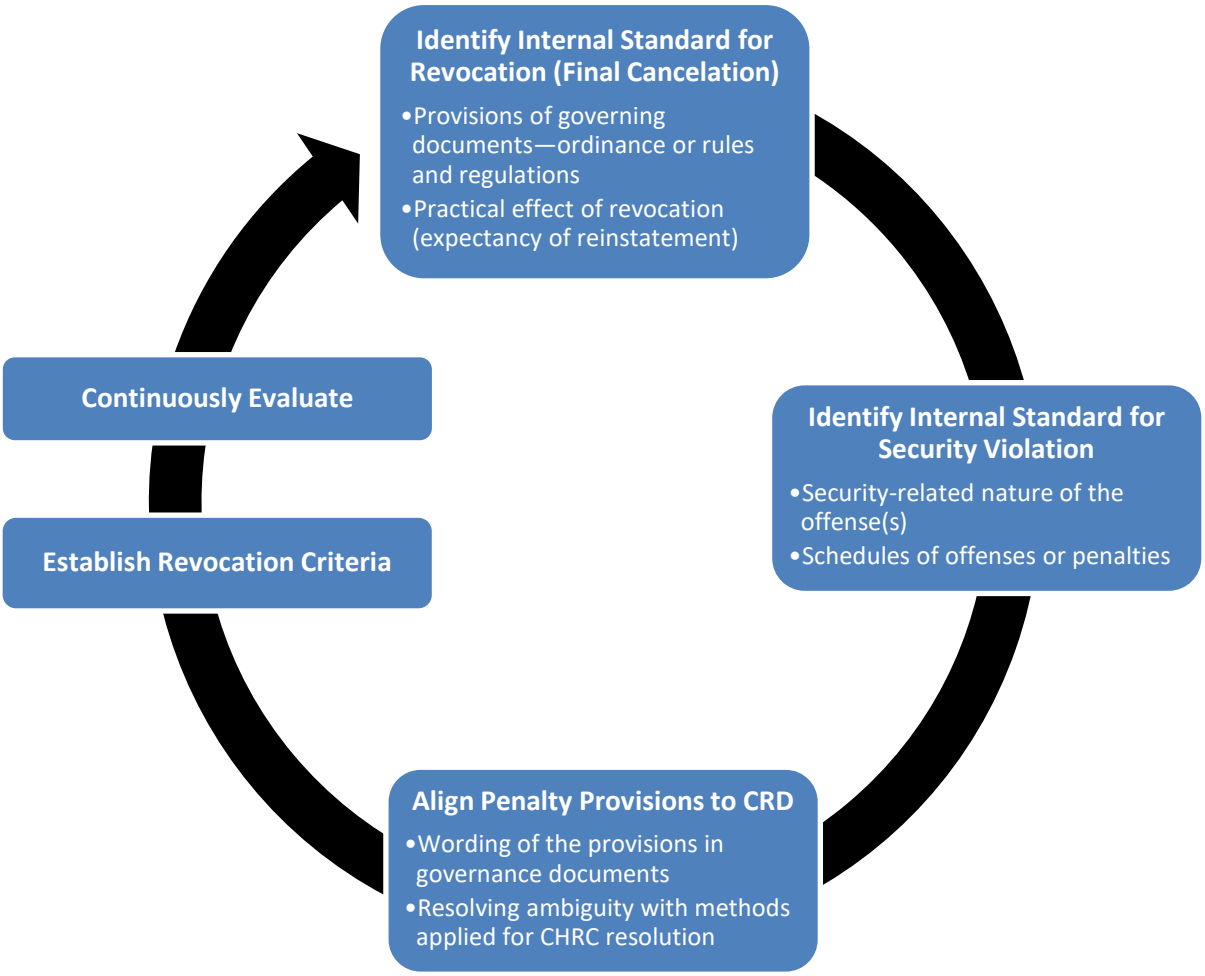
All the airports reviewed in connection with this report indicated that they had a process that afforded notice advising an individual of allegations of security and other violations that could result in fines or penalties, such as suspension or revocation of credential privileges. This notice is often in the form of a citation, complaint, summons or other charging instrument. The airports also uniformly had some process to allow individuals an opportunity to present information and evidence to refute the allegation, or to submit mitigating factors. If the term “appeal” is interpreted to mean that a person who is charged with misconduct is afforded an opportunity to be heard, then the airports reviewed all had such processes.

Final determinations on revocation issues were made through a wide range of hearing formats. Many airports afforded individual hearings before management personnel, hearing officers, or tribunals including a variety of airport stakeholders. Some airports have procedures that give individuals an ability to respond through written process.

Revocation Policy and Practice Workflow

Creating a workflow diagram or document to assess revocation requirements may help airports better visualize the requirements for CRD entry. The figure below is an example of a workflow that airports can use to help evaluate their processes consistently with NA requirements.

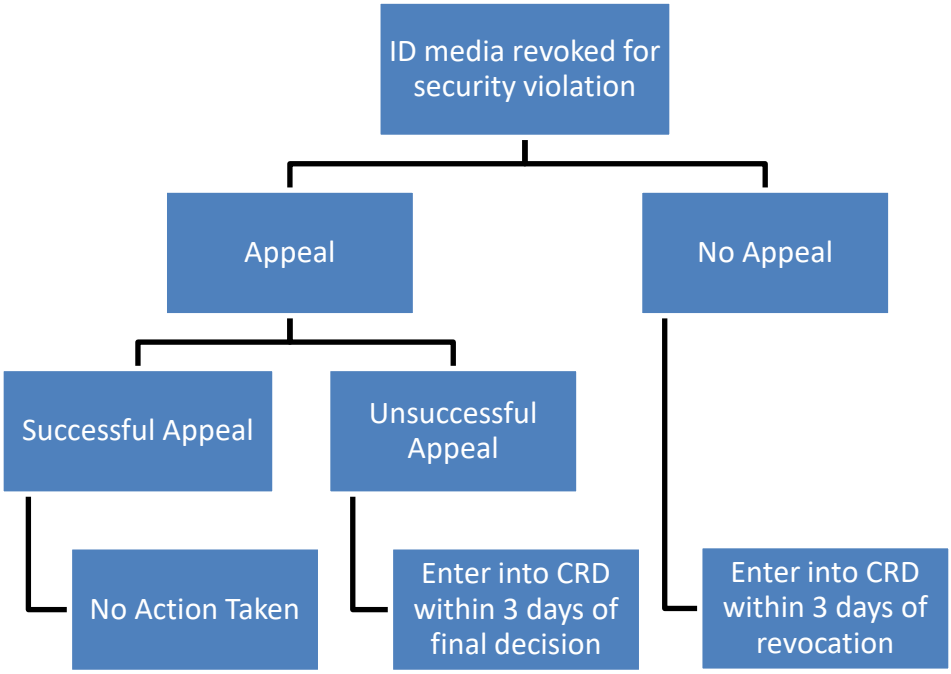
Figure 1. Workflow of Revocation Policies and Practices



SECTION 4: ENTERING INFORMATION INTO THE CRD

The NA identifies revocation actions that are subject to CRD entry and outlines a process for airports to enter that information into the CRD. It also provides a resource for airports or aircraft operators using the information for subsequent decisions concerning credentialing. The chart below indicates the general workflow to enter individuals into the CRD.

Figure 2. Workflow of Entering Individuals into the CRD



Entering information into the CRD requires attention to specific requirements, and can benefit from process efficiencies. The research found that, before entering data into the CRD, airports should ensure that their procedures are aligned with those outlined in the NA, and should address any technical issues that may affect data entry.

To assist airports in their data entry responsibilities, TSA created the CRD User Guide. This guide provides step-by-step instruction to assist Trusted Agents in the entry of data into the CRD. It includes screenshots from the FPRD system where Trusted Agents are required to enter data. The User Guide also provides helpful tips for data entry and identifies points of contact to address user questions.

Quick Reference Guide

Creating a CRD process Quick Reference Guide (QRG) may assist airports when potential revocation situations occur. The CRD User Guide is a great resource for developing an internal guide. For most airports, credential revocations that meet CRD requirements are rare. Therefore, a QRG that covers the nuances of the process could help an airport meet the requirements in a timely fashion. This QRG should not only cover the basics, like requiring a CRD entry within the required period of the revocation

becoming final, but also include instances where an appeal occurs.[10] A CRD QRG should also cover expungement requirements for an individual entered into the CRD due to mistaken identity.[11]

Workflows

In addition to the QRG, the airport might consider creating documented workflows for data entry. A thorough review of the process for entering information into CRD will help address the airport's specific policies and operational needs when creating the workflows. These workflows might include instruction on time frames for data entry, maintenance of supporting documentation, application of different due process standards, or informing or seeking approval from leadership to address problems and concerns raised in the entry process and review of submittals.

Some airports have automated these workflows. For example, a CAT I airport has created a proprietary Adjudication Database that tracks credential revocations and assists the credentialing office in completing necessary processes. Further, this database assists with the workflow for new credential applicants, as it queries the CRD for entries. One large airport uses their Identity Management System to trigger actions for their credentialing office. The system now generates tasks to check the FPRD daily for CRD entries of credential applicants.

Airports who maintain a temporary visitor database may want to consider adding individuals with credential revocations to the database to ensure that factor is considered when allowing temporary escorted access.

Usefulness and Accuracy

When submitting an entry to the CRD, there is little opportunity for airports to present a great deal of specificity into the facts around the revocation given the 120-character limit for data entry. This poses potential issues for other airports who may want to use the information in connection with their determination to issue credentials. Considering this, airports should include the maximum amount of usable information when creating CRD entries so that an airport using the information has the best possible understanding of the basis for the revocation decision. Airports interviewed indicated they would find it helpful for CRD entries to cite code sections or statutes to identify the basis for the reported violation, when possible.

Interviews for this project indicated that airports have experienced great difficulty in making corrections to data entries after CRD submission. The level of difficulty suggests that airport workflows should provide for careful review of records and data before submission. This could be accomplished by ensuring supervisory review and approval of CRD revocation entries. Given the relatively low number of entries, this should not put undue burden on supervisory personnel.

Record Keeping

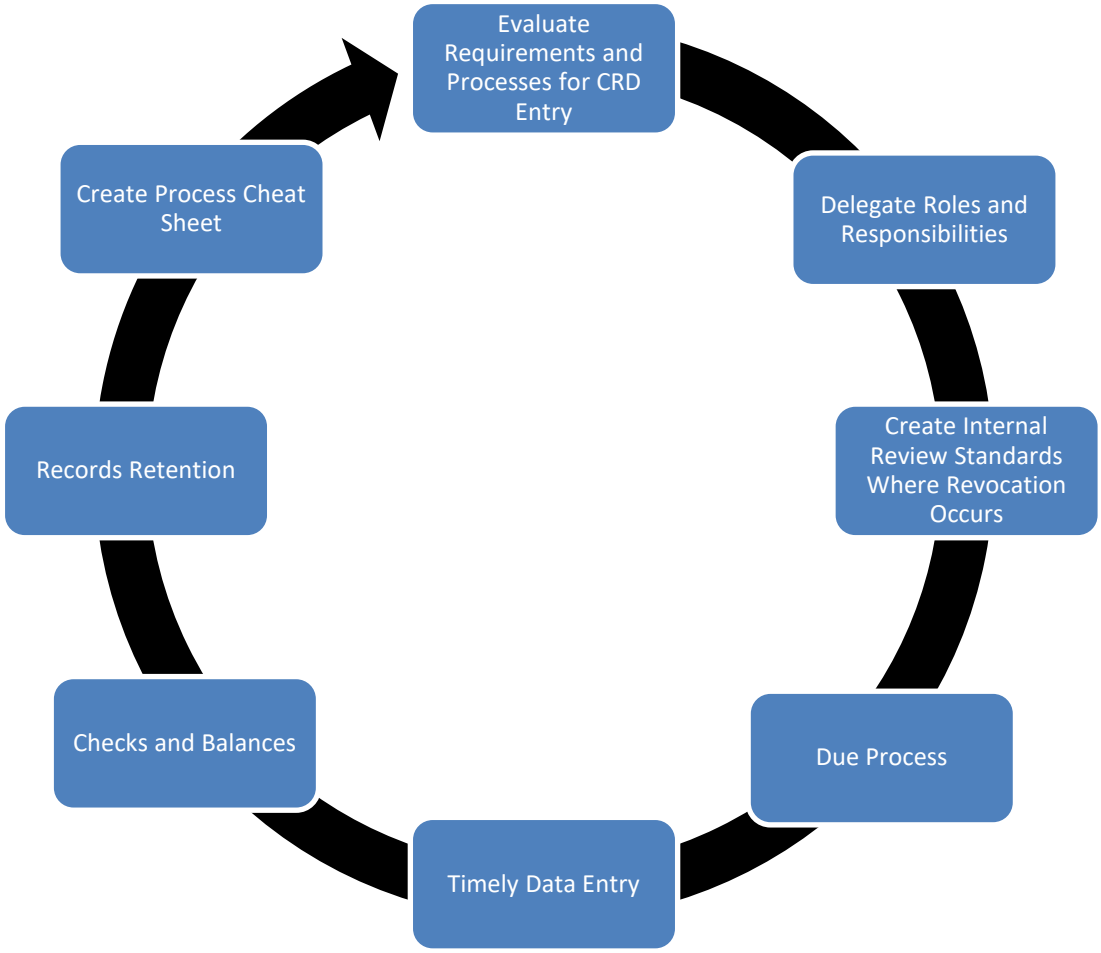
The NA does not address record keeping for decisions to place an individual in the CRD. In the absence of any federal requirements, most airports will retain supporting documentation relating to the revocation proceeding for the standard period of time set forth in their records retention schedule. This would include critical documents like complaints, citations or summons, witness statements, and other evidentiary materials. These materials may be relevant to subsequent challenges to CRD entry decisions

[10] TSA-NA-21-01A § VII.
[11] *Id*. at § IX.

or inquiries from other airports investigating a CRD finding of a badge applicant. Airports may consider reviewing their existing document retention policies with their counsel to ensure they manage airport concerns in light of TSA's five-year retention of the CRD entries.

CRD Entry Policy and Practice Decision Workflow

Figure 3. Workflow of CRD Entry Policies and Practices



SECTION 5: USE OF CRD FINDINGS

The CRD NA requires that airport operators review the database to determine if any badge applicant has been entered into the CRD.[12] The NA does not require airports to use the information in its suitability determination.

The NA gives airport operators wide discretion in how they choose to use the CRD results. This can lead to a range of outcomes, including:

- Airports unwilling to deny credential applications based on CRD results
- Airports denying credentials to any individuals listed in CRD
- Airports assessing CRD findings on a case-by-case basis
- Airports comparing available information regarding the revocation to their own revocation or suspension standards

Like the CHRC process, the CRD review gives airports additional vetting information about persons seeking unescorted access. This information can be used to help identify and mitigate security risk. Unlike the CHRC process, it allows the airport greater flexibility in its use of the information received. Entry in the CRD is not an automatic bar to employment, which contrasts with CHRC review, where the discovery of a disqualifying criminal offense automatically denies unescorted access privileges. The airport has the freedom to craft solutions or interventions for individuals in the CRD. This may include requiring enhanced training or mitigation strategies.

The flexibility granted to airports is not without cost. The absolute prohibition of badging persons convicted of disqualifying criminal offenses shields airports from liability when denying credentials to those individuals. However, where the decision is discretionary, that protection evaporates. In this respect, the CRD places airports in the same position that is experienced by airports that impose more stringent CHRC review standards and suitability determinations by exceeding the federal baseline. That risk is discussed in PARAS 0029 *Criminal History Records Checks (CHRC) and Vetting Aviation Workers Guidebook*.

Airport operators will benefit from considering how they will assess CRD results before they are discovered. This will assist airport operators in making risk-based decisions that align with their airport security posture. As discussed in Section 6, airports have varying security programs to mitigate specific security vulnerabilities on their campuses. Similarly, an airport may have other policies, business strategies, or tenant relationship concerns that require additional consideration before a CRD entry or action occurs. In reacting to a CRD result without consistent processes and practices in place, an airport may miss an important consideration affecting their decision to either issue or deny a badge application.

Written Policies and Procedures

Establishing written policies and procedures will assist airport operators in consistently applying their standards of review. These procedures should consider who has a need to review CRD results or sign off on decisions to deny a credential application. A process that includes too many airport officials may cause unnecessary delay and confusion. Providing the credentialing office or ASC with clear and consistent rules will enable them to make these critical decisions appropriately in a timely manner.

[12] TSA-NA-21-01A § III.

Similarly, these written policies and procedures will assist airport operators in managing challenges such as inconsistent application of revocation definitions.

Additionally, written policies and procedures will assist airport operators in defending their credential issuance decisions if challenged. Having written documentation that establishes processes and criteria for decision making will show that the decision was not arbitrary but based on approved policies. This documentation may aid in internal appeals, legal challenges, or complaints sent to airport leadership.

Gathering Additional Information

Airports should consider how they will research CRD results and what actions they will perform if they cannot obtain sufficient information about the entry. CRD results do not provide a lot of explanatory information due to the 120-character limit, and some results may be less helpful than others.

Airports may choose to contact the entity that entered the revocation to gather additional details. However, privacy rules and regulations may restrict the reporting entity from providing additional information. Airports may also ask the sponsoring company or badge applicant for more information, but that presents some risk. The sponsoring airline or tenant may not be forthcoming with information if they do not agree with the initial revocation, or if they deem the individual suitable for employment. A third option is to leverage airport law enforcement to check other databases such as the Transaction Record Analysis Center to supplement available information.

Airports reviewing a CRD entry while adjudicating credential applications should consider researching the revoking airport's enforcement strategy and violation policies. The airport may find materials online or may have to contact the airport that revoked the badge and ask about their enforcement and reporting policies and processes.

Evaluation Methods

One airport offered a simple plan for evaluating individuals identified in a CRD review. When the CRD entry is reviewed, if the airport determines that additional information is necessary to determine suitability, the following actions would be taken:

- The individual is contacted and required to provide a written statement concerning the circumstances of the incident(s) resulting in revocation.
- The individual is required to sign an authorization form permitting the revoking airport to be contacted for additional information.
- If the individual fails to comply with either request, the credential application or renewal is denied.
- If the individual complies, the revoking airport is contacted, provided with the signed authorization form, and asked to provide supporting information for evaluation.
    - The individual is invited to provide any additional relevant exonerating information they chose to submit.
- The airport then reviews all information gathered, analyzes the totality of the circumstances, and decides whether to issue credentials to grant unescorted access to secured areas.

Many airports interviewed stated that they will develop and apply their own enforcement standards to adjudicate CRD findings. For example, if an applicant has information in the CRD for a revoked badge,

the reviewing airport will assess how they would have penalized the same security violation. If the airport's rules would have required a revocation for the same offense, they would not issue the credential. If the airport would have issued a suspension, fine, or other lesser penalty, they will likely issue the badge. The airport may consider attaching conditions to the badge issuance, such as training requirements or access restrictions.

Post-Credentialing Notifications

Airport operators may receive CRD notifications in their FPRD work queues after credential decisions are made. This situation is not specifically addressed in the NA. Two airports interviewed for this project reported that CRD entries appeared in their FPRD work queues for individuals that were previously credentialed at their airports.[13] An individual can hold credential privileges concurrently at multiple airports, introducing the possibility for one airport to revoke an individual's credentials while they simultaneously hold a badge at another airport. The second airport may have an obligation to review the CRD information of their current credential holder.[14] Airport operators should speak with their legal counsel to determine if they have an obligation to act in this situation.

Airports have multiple options when this occurs. They can choose to take no immediate action and simply address the matter at badge renewal. If the airport does decide to take an action, airports may want to consider their own enforcement policies in assessing the reason for revocations at another airport. Documenting these policies and processes ahead of time will create efficiencies and support decision justifications.

Opportunities for Improvement

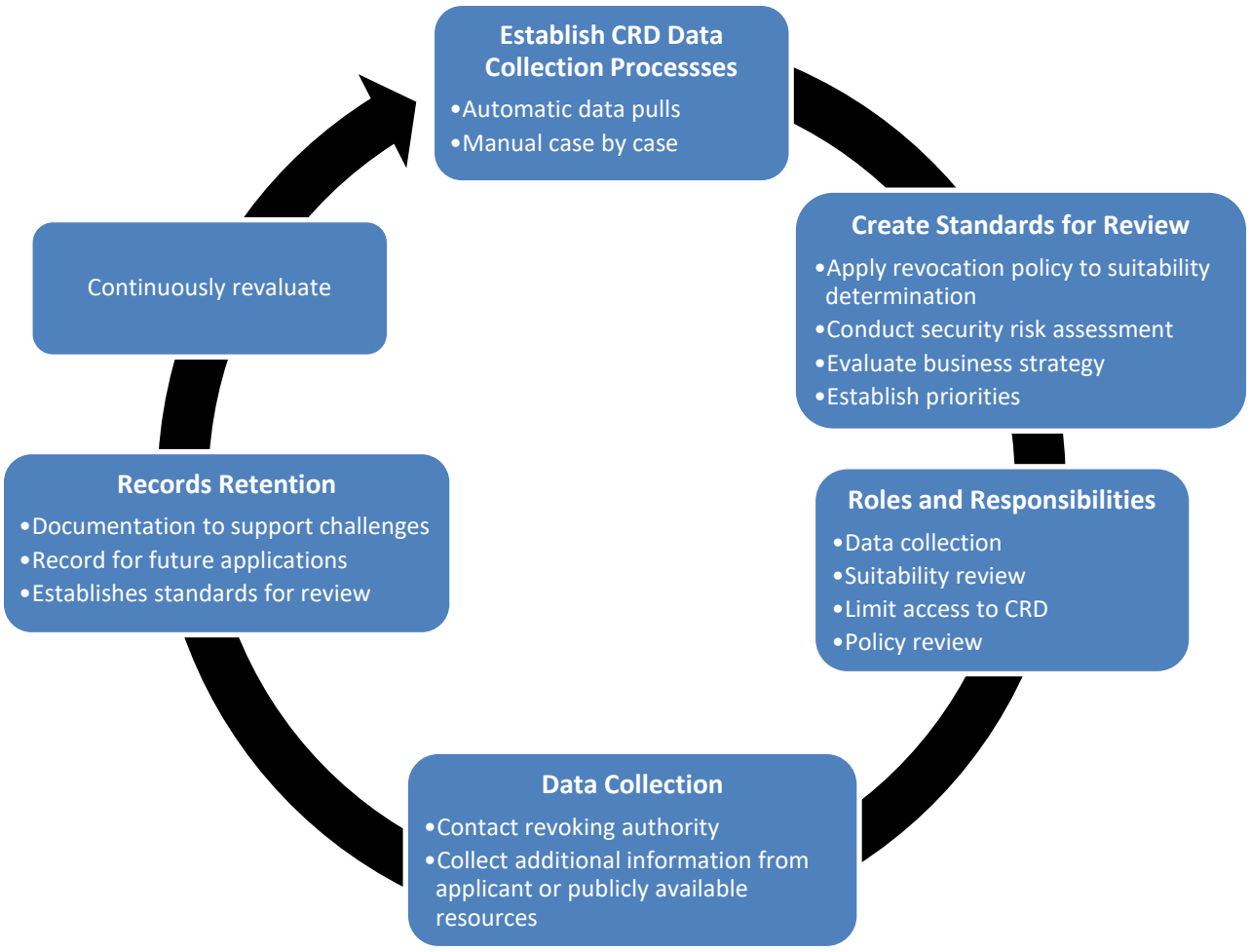
Airport interviewees identified the following opportunities to improve the usability of information in the CRD:

- The ability to create a comprehensive report containing all the entries in the CRD could assist airports in auditing active credentials against the CRD list. Currently, the airport is limited to a search by individual, and can only search the records of those badge holders who have had a CHRC ordered by the airport.
- Due to limitations in the ability to identify the nature of security violations, use of free-form text in the "Other Security Violations" column could help identify commonalities and categories. This option would also provide better reporting for airports, airlines, and TSA.
- Using data from the CRD to create reports could be enhanced by providing the capability to export the data. Adding necessary fields to create a comprehensive report with respect to CRD entrants would also be beneficial; for example, date of birth is missing.

[13] Of note, both airports reported that these individuals did not have current credentials at their airports. These airports did not understand why these former badge holders' current CRD revocations appeared on their FPRD work queues.
[14] TSA-NA-21-01A § III(A).

Use of CRD Findings Workflow

Figure 4. Workflow for Use of CRD Findings



SECTION 6: CRD FIT INTO THE BROADER AIRPORT SYSTEM

Implementation of CRD requirements is heavily dependent on each airport's high-level policies and more granular operating conditions. Accordingly, each airport should consider how the CRD fits into their broader strategic picture.

Airport Security Strategies

Airport operators should evaluate their security strategies and vulnerabilities in conjunction with analyzing CRD policies and practices. Each entity will have unique risks, operational demands, and capabilities to mitigate security vulnerabilities. Some airports may be less inclined to accept the risk imposed in issuing credentials to an individual who has demonstrated an inability to comply with security rules. Effective CRD practices and policies will fit into the broader airport security program policies and practices.

Because of resource burdens, airports may accept airline CHRC certifications, as the airlines may have greater capacity to conduct thorough background checks. These airports will not have access to CRD results for airline-certified individuals, just as those airports would be unable to see the CHRC results for certified individuals.

Questions to consider when assessing an airport's security posture related to the CRD include:

- Does the airport credentialing office have authority to deny issuing badges beyond instances expressly authorized by TSA?
- Does the airport have a policy of accepting airline certifications for credentialing, and is the airport willing to forgo access to CRD entries for individuals certified by airlines?
- Does the airport have the resources to adequately investigate CRD findings?
- What is the risk **tolerance** for issuing airport **badges** to individuals **who** have had their access privileges revoked by another airport or an airline?
- Does the airport have other adequate security measures in place to accept additional known risks?
- Has the airport considered the types of security vulnerabilities that present the greatest risk for them?
- Has the airport considered how tenants vet potential employees or train them before hiring them to work at the airport?

Airport Governance Models

Airport governance often affects how airports can make decisions and change policies and practices. For example, airports run by a city or state often operate as departments of the city or state government. Therefore, changes to airport governing rules or policies require approval from the mayor or governor, as well as city council and legislature. Those airports may follow general city or state policies, which may affect enforcement, vetting processes, or credential denial decisions. Alternatively, quasi-government agencies, such as airport authorities, may have more ability to make independent decisions, and may have less restrictive guidance for enforcement or vetting decisions. For example, one airport authority stated they can change credentialing processes or enforcement procedures within their security

department to respond to emerging threats or new regulatory requirements. The ability of these airports to change practices that surround CRD use will greatly affect implementation.

The labor laws and privacy laws of the state in which an airport is located also affect an airport's ability to adapt to new TSA-imposed privacy requirements. Some states have stringent limitations on using criminal history to determine job suitability, and airports in these states could face legal challenges to updating credentialing policies. These airports must work with their legal counsel to carefully craft the required updates to airport policy language. This takes time, regardless of the airport's size.

These governance distinctions also affect how airports can create new or amend existing policies to meet CRD requirements. In instances where penalties for an infraction are set by an ordinance or a regulation, adapting changes to align the penalty structure to a concept of permanent revocation may be challenging. These airports will also have to account for local political considerations in deciding how to resolve challenges. Creating processes that allow for entry of individuals into the CRD in the absence of a clear airport ordinance definition of revocation may cause political consternation. Airports with fewer resources to make policy and practice changes should consider holistic airport security program changes to incorporate CRD, such as changes to enforcement or vetting policies.

Airports who are prevented from using CRD findings to make suitability determinations due to their governance structure may consider alternative security requirements to mitigate insider threat, such as extra training, mitigation strategies for authorized signatories, or limiting the individual's access authority, among other strategies.

Airport Leadership Buy-in

Having leadership support for badging policies and practices will assist the credentialing office and security team when unpopular decisions are made. CRD information that results in the denial of badging applications may receive pushback from airlines, concessionaires, other tenants, the individuals involved, or boards and oversight committees. Further, certain individuals may bring credential issuance decisions to local political decisionmakers. Therefore, having support from airport leadership teams at the outset is critical to ensuring policies and practices can operate as intended.

The credentialing office or security team should ensure that their airport's leadership is aware of what the CRD is, its origin, compliance requirements, how the security and credentialing teams will use the CRD, and any implications for the airport and its leadership. It may also prove difficult in jurisdictions where political movements press to expand rights to employment. These same types of concerns are also addressed with respect to criminal background checks and efforts to expand the types of disqualifying criminal offenses for airports' SIDA and Sterile Area access.[15] Whatever positions airports decide to take regarding the CRD implementation, it is recommended that they prepare briefing memos and other documents to educate their leadership prior to issues arising.

Airline and Tenant Engagement

Airports may consider their airline partners' positions on vetting and credential revocation when assessing how they will engage with each airline. Individual airlines may have different vetting criteria or thresholds for security violations. If airports do not agree with airlines' vetting standards, they may

[15] Lori Beckman, "*Criminal History Records Checks (CHRC) and Vetting Aviation Workers Guidebook*," National Safe Skies Alliance Program for Applied Research in Airport Security (PARAS) 0029 (October 2020): 22-23.

not want to accept airlines' certifications, or they may want to manage penalties and revocations that affect CRD entry differently.

The introduction of the Rap Back mandate has created some challenges for airports that accept certifications from their airline partners. Submitting the CHRC for an individual automatically subscribes that individual to Rap Back and authorizes the submitting entity (airport or airline) to review and maintain that subscription. However, the other entity will not have the authority to view the case record in the Fingerprint Results Distribution (FPRD) system for that badge holder, and will not directly receive any Rap Back Activity Notifications of subsequent criminal activity.

Send requests for manual entry into CRD, along with accompanying information, to aviation.workers@tsa.dhs.gov

Consequently, airports accepting certifications from airlines have no ability to submit a "Report Revoked Badge" entry into the FPRD portal as described in the CRD User Guide. In such cases, airports should submit complete information regarding the identity of the individual, date(s) of the violation, security violations that occurred, and any additional information to TSA, and TSA will manually enter the data into the CRD.

Further, only the airport or airline that submits the initial CHRC subscription, or has previously established a case record in FPRD, will be notified that an individual has been entered into the CRD by another entity. Airport interviews for this project revealed that at least two airports have received notifications of CRD entries for individuals that had previously held a badge at their airport.

More information on Rap Back and airline certifications can be found in PARAS 0029 *Criminal History Records Checks (CHRC) and Vetting Aviation Workers Guidebook*.[16]

Program Awareness

Engagement and awareness of airport security programs and practices helps strengthen an airport's security culture and achieve program successes. The research conducted for PARAS 0020 *Strategies for Effective Airport Identification Media Accountability and Control* found that the airports that prioritized security culture and security awareness in their airport community had consistently high badge accountability.[17] Similar enhancements to airport security postures may be realized with the CRD. Individuals could be deterred from behaviors or less likely to act negligently because of the possibility of having their name included in the CRD for a five-year period.

Making airport credential holders and applicants aware of their responsibilities and the potential consequences of security violations may assist in building security awareness. NIST's *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*, discusses the benefits of awareness and attitude for changing individuals' behaviors.[18] When individuals understand their

[16] PARAS 0029: https://www.sskies.org/images/uploads/subpage/PARAS_0029.CHRCsVettingAviationWorkers_.FinalReport_.pdf

[17] Anne Marie Pellerin, et. al., "*Strategies for Effective Airport Identification Media Accountability and Control*," National Safe Skies Alliance Program for Applied Research in Airport Security (PARAS) 0020 (December 2019): https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf

[18] "Special Publication 800-12: AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, Chapter 13: Awareness, Training, And Education" National Institute of Standards and Technology, accessed December 12, 2022, https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html#95

responsibilities and consequences, they become more accountable for their actions.[19] This helps to avoid errors and omissions, which are major causes of security failures.[20]

Further, communication strategies assist in setting the airport's standards regarding enforcement of security violations. If individuals know that the airport is earnest about security compliance and will enter security-related revocations into the CRD, they may be motivated to act with more diligence or think twice when disgruntled.[21] Similarly, if tenants know the airport leverages CRD findings, they may increase their diligence in hiring individuals for positions requiring access to airport SIDA and Sterile Areas.

Notifying tenants of CRD practices may help to strengthen airports' security cultures by providing tenants with a better understanding of airports' priorities and decision making. This will help tenants support their airport's objectives, and will enable them to complete their own work in compliance with their airport's priorities. Many of the airports interviewed for this project indicated that they had made little change in notifications to tenants or credential holders for CRD beyond revising the Privacy Act Notice in connection with badge applications and renewals. The Privacy Act notifies applicants and current credential holders of the CRD, and that revocation of access for security violations will result in their name being added to the database for a period of five years.

TSA Privacy Act Statement

TSA has created a "Centralized Revocation Database User Guide for Airports and Aircraft Operators" (User Guide) to assist airports in understanding the CRD requirements. This User Guide provides technical assistance for the entry of ID media revocation decisions into the CRD on the FPRD portal. The User Guide was initially issued in November 2020 and has since been updated. It is accessible through the Homeland Security Information Network (HSIN) and provides both technical assistance on the entry of revocations as well as information on criteria for entry, revocation notification, data correction, and contact information. Appendix A of the user guide contains the most recent Privacy Act Statement required for credential issuance as of the date of this publication.

Airports may use additional processes to inform applicants and badge holders of the CRD.[22] Communications can occur during security meetings or trainings, in newsletters, and in security violation letters where the violation resulted in a fine or suspension. The following are examples of communication strategies that airports have employed regarding CRD:

- One airport prepared a policy memorandum on the new CRD program and circulated it to authorized signatories to advise their companies and badge holders of the new requirements.
- One airport indicated that information about the CRD was provided in credentialing training.
- Another airport indicated a policy of verbal notification to individuals charged with offenses that could result in CRD placement.
- Some airports notify credential holders that entry into the CRD may prevent them from holding a credential at any TSA-regulated airport.
- Multiple airports include language in their credential suspension letters to provide advance notice to badge holders that subsequent offenses may result in credential revocation and entry into the CRD for five years.

[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] See TSA-NA-21-01A § V.

No airport indicated having a policy of notifying applicants of how CRD findings would be considered in their application or renewal processes. However, implementing such a notification may act as a deterrent for some individuals applying for credentials, or it may remind applicants to be vigilant regarding security requirements.

SECTION 7: SUMMARY OF FINDINGS AND CONSIDERATIONS

The CRD poses challenges to airports when identifying qualifying revocations and aligning CRD data input requirements. It also presents challenges as airports develop and implement policies to use CRD findings in connection with their vetting processes and practices.

As airports continue the process of implementing the CRD, dialogue with TSA may mitigate some of the concerns raised by the language in the NA. As the CRD database becomes more robust, and discussions among TSA and airports continue, the value of the CRD and associated knowledge transfer in mitigating the risk of insider threat will be highlighted.

Credential Revocation

- Some of the defined terms around revocation used in the NA are not understood or commonly used by airport operators (e.g., final cancellation, appeal, and hearing). Accordingly, there is a need for airports to evaluate their enforcement programs against the CRD revocation definition and criteria in the NA, and to harmonize the provisions of the NA with their existing penalty structures.[23] The techniques used for statutory analysis for CHRC findings might also be used to align the airport's penalty provisions with the NA.
- Airports may review and refine their airport rules and regulations regarding their revocation practices and appeals processes to ensure they are clearly defined and comply with CRD requirements. The reviews might include discussions with personnel who play a role in the CRD process, such as Trusted Agents, supervisors, compliance officers, and management and executives. Where existing airport processes cannot be harmonized with the NA without changes, the airport should work with their legal counsel and TSA to develop a compliance strategy.
- Airports should consider developing specific written policies and procedures indicating when and how CRD processes are incorporated into their existing procedures for credential revocations. Those procedures should specifically address criteria for placement in the CRD. The written policies and procedures should also identify any additional procedures or processes afforded to an individual prior to placement into the CRD.
- Airports may consider informing credential applicants or holders of the additional CRD requirements through new and renewing badge holder training, security meetings, security training, newsletters, and language in violation letters where the violation resulted in a fine or suspension.

CRD Data Entry

- Many airports enter individuals into the CRD infrequently. Therefore, airports should consult the CRD User Guide for information on the types of revocations that qualify for entry into the

[23] See CRD User Guide at p.6.

CRD,[24] and agents should frequently review CRD requirements to ensure compliance with requirements for entry and expungement.[25]

- Airports can use the CRD User Guide, Frequently Asked Questions (FAQ), and data entry requirements stipulated in the NA to develop plans for CRD data entry,[26] to develop training for Trusted Agents responsible for data entry, and to prepare a QRG or other aid to assist Trusted Agents perfoming data entry tasks.
- The timing of CRD entry requirements may present challenges with airports' existing penalty appeal schedule. Similarly, automated processes may need additional programming to prompt CRD entry after appeal deadlines. Development of workflows that conform with the three calendar-day CRD entry requirement will assist Trusted Agents in ensuring compliance. Those workflows should include:
    - Timelines for compliance with CRD data entry requirements
    - Measures to ensure the availability of required data
    - Measures to ensure hearing requirements are met
    - Measures to ensure proper review and quality control over data entry
- Airports should work with their counsel to establish appropriate coordination with persons and entities conducting hearings or providing appellate reviews so information can promptly be collected for entry.
- Airports should maximize the amount of information they provide within the CRD portal's 120-character limit. Where possible, airports should cite publicly available ordinances or airport rule provisions so airports reviewing the results have a better source of objective information.
- Airports should review their document retention practices concerning credential revocation so that airport CRD entry decisions can be defended, and so that information can be made available to airports seeking information on individuals identified by the CRD in subsequent badging decisions.
- Penalty provisions that consider a range of conduct over time may require assessment by legal counsel, and perhaps consultation with TSA, before entering the revocation into the CRD.

CRD Data Review & Use

- Where an airport determines that it will consider CRD findings, the following actions should be considered:
    - Determine in advance who will retrieve CRD entries and who will adjudicate additional information from the CRD finding.
    - Request additional information about the CRD finding from the applicant through a mandatory written statement or oral interview.

[24] See CRD User Guide at p.6.
[25] See Requirement to Amend TSA-Approved Airport Security Program, Centralized Revocation Database for Individuals with Revoked Identification Media, TSA-NA-21-01A § VIII A. and B. and § IX (Hereinafter TSA-NA-21-01A).
[26] Site CRD User Guide and FAQs.

  - Secure a signed authorization form from the applicant allowing the revoking airport to provide information about the underlying incident(s).
  - Establish procedures for contacting the revoking airport to gather additional information about the underlying incident(s) leading to badge revocation.
  - Allow the applicant to provide any additional evidence relating to the underlying incident(s) related to the revocation.
  - Establish procedures for evaluation of all collected materials and adjudication of results.
  - Establish procedures to notify applicants of the result of the adjudication process concerning the CRD entry.
- Reducing organizational roles and responsibilities within CRD processes can create efficiencies and establish consistent practices in the use of the database. Too much specialization may create confusion and a lack of understanding of the CRD process and how it relates to badge issuance and revocation. It may also cause delays in the process to enter individuals into the CRD, as required.
- The discretionary use of CRD data potentially exposes airports to a range of liability challenges. Airports should consider having a written policy outlining the use of CRD results in credentialing decisions. Policies should indicate whether the airport intends to factor CRD findings into its vetting decisions and the reasons for including or excluding those considerations.
- Understanding what the CRD information means and applying it to the adjudication process during credentialing requires coordination with airport security, legal, human resources, and executive-level decision makers.
- Some airports may be reluctant or unable to provide additional information about revocation decisions due to privacy laws. All airports should examine policies around sharing incident information with airports investigating CRD findings.
- Inconsistent application of revocation definitions creates difficulties for reviewing parties to understand how to evaluate entries in the CRD. Airports may consider applying their own enforcement policies or standards in evaluating an applicant's CRD results.
- Airports issuing credential to individuals with CRD findings may consider imposing special conditions, such as requiring enhanced security training, imposing additional supervision requirements, limiting access, or shortening their badge expiration period.

SECTION 8: ADDITIONAL RESEARCH NEEDS

The Project Team identified the following additional research needs related to CRD.

DUE PROCESS

Airports have varying due process practices and, in some cases, very limited practices. Future research should look at what types of due process practices work for airports and have a positive effect on airport security and overall airport culture.

COMMUNICATION OF CREDENTIALING PRACTICES

Airports differ in what and how they communicate to stakeholders. A study would be helpful to assess communication strategies specifically discussing credentialing programs.

CREDENTIALING SUITABILITY ASSESSMENTS

Airports have multiple resources to assess an individual's suitability for airport access, including CHRCs, Rap Back, and CRD. A study that looks at suitability assessments and decisions would be helpful for airports. Further, the study should evaluate the benefits of exceeding statutory disqualifying offenses through policy or local regulation.

CREDENTIALING PROGRAM DECISIONS' EFFECT ON RISK MANAGEMENT

Airport credentialing decisions affect overall security risk and other program decisions. A study that focuses on how credentialing programs mitigate or shift risk will assist airports in developing and managing a holistic credentialing program.

REFERENCES

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

Badgley, S. (April 27, 2020). *Privacy Impact Assessment for the Airport Access for Aviation Workers. DHS*. https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa020c-airportaccessaviationworkers-april2020.pdf

Bean, B. (December 2017). *Mitigating Insider Threats in the Domestic Aviation System: Policy Options for the Transportation Security Administration*. Naval Postgraduate School, Monterey.

Beckman, L. (October 2020). *PARAS 0029: Criminal History Records Check (CHRC) and Vetting Aviation Workers Guidebook*. National Safe Skies Alliance, Inc. https://www.sskies.org/images/uploads/subpage/PARAS_0029.CHRCsVettingAviationWorkers_.FinalReport_.pdf

Bielby, K. (January 18, 2020). *Updated: Government Employees and Contractors Not Subject to the Same Vetting Process*. Homeland Security Today, Accessed September 18, 2022. https://www.hstoday.us/federal-pages/dhs/government-employees-and-contractors-not-subject-to-the-same-vetting-process/

Bielby, K. (February 27, 2021). *Insider Threat: GAO Weighs in on Airport Worker Screening*. Homeland Security Today, Accessed September 18, 2022. https://www.hstoday.us/federal-pages/dhs/gao-weighs-in-on-airport-worker-screening/

Black, A. (December 2010). *Managing the Aviation Insider Threat*. Naval Postgraduate School, Monterey.

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

Defense Counterintelligence and Security Agency. (n.d.). *Appealing a Denial or Revocation of a Clearance*. Accessed September 11, 2022.

Elias, B. (August 14, 2018). *Strange Occurrences Highlight Insider Threat to Aviation Security*. Congressional Research Service, IN10964.

FAA Reauthorizations Act of 2018 § 1934.

Federal Aviation Administration. (June 10, 2010). 86 FR 31006 Pilot Records Database. https://www.federalregister.gov/documents/2021/06/10/2021-11424/pilot-records-database

Federal Aviation Administration. (June 10, 2021). FAA Form 8060-15, Pilot Records Database. Pilot Records Dispute Supplemental Information.

Federal Aviation Administration. (n.d.). AOV Credentialing and Control Tower Operator Certificate Programs. Federal Aviation Administration. Accessed Aug. 29, 2022.

Federal Register. (June 10, 2021). Pilot Records Database: a Rule by the Federal Aviation Administration; Federal Register. Accessed September 12, 2022.

Flamenbaum, H., Fleet, D., Gaisor, R., & Varwig, Z. (February 2017). *PARAS 0006: Employee Inspections Synthesis Report*. National Safe Skies Alliance, Inc. https://www.sskies.org/images/uploads/subpage/PARAS_0006.Employee_Inspections.FinalReport.pdf

Freedom of Information Act (FOIA), codified at 5 U.S.C. § 552.

GAO. (September 24, 2020). *The Quest to Combat Insider Threats at Our Nation's Airports*. GAO-20-275.

GAO. (December 2021). *Actions Needed to Implement Reforms, Address Challenges and Improve Planning*. GAO-22-104093.

GAO. (February 2021). *Airport Worker Screening TSA Could Further Strengthen Its Approach to Estimating Costs and Feasibility of Security Measures*. GAO-21-273.

General Services Administration. (n.d.). Trusted Workforce 2.0; GSA, Accessed September 18, 2022. https://www.performance.gov/trusted-workforce/

George, A., Arey, B., Ertzinger, B., Michaelson, B., Heck, D., Johnson, D., Demmon, J., Speciale, J., & Smith, K. (2019*). Best Practices in Vetting Prospecting and Current Employees*. 2019 Public-Private Analytical Exchange Program.

Hagen, L. & Turkel, A. (July 29, 2014). *An Overview of Federal Criminal Databases*. National Indigenous Women's Resource Center.

IATA. (n.d.). Insider Threat in Civil Aviation; IATA.

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

Interpol. (n.d.). SLTD database (travel and identity documents); Interpol. Accessed September 11, 2022.

International Civil Aviation Organization. (August 2022). *ICAO Insider Threat Toolkit*. ICAO, Edition 01.

Melendez, E., Button, D., & Stoyko, D. (March 2022). *PARAS 0036: Airport Credentialing Efficiency Toolkit*. National Safe Skies Alliance, Inc. https://www.sskies.org/images/uploads/subpage/PARAS_0036.AirportCredentialingToolkit_.FinalReport_.pdf

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

Moore, A. (August 16, 2019). *Rising to Meet the Credentialing Challenge*. International Airport Review. Accessed Aug. 29, 2022.

National Highway Traffic Safety Administration. (August 2020). *National Driver Register Frequently Asked Questions*. NHTSA.

National Institute of Standards and Technology. (December 12, 2002). *Special Publication 800-12: AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, Chapter 13; Awareness, Training, And Education" National Institute of Standards and Technology*. Accessed December 12, 2022. https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html#95

Pellerin, Anne Marie, Sean Cusson, Donald Zoufal, Mark Crosby, and Michael Keegan. (December 2019). *PARAS 0020: Strategies for Effective Airport Identification Media Accountability and Control*. National Safe Skies Alliance, Inc. https://www.sskies.org/images/uploads/subpage/PARAS_0020.IDMediaAccountabilityControl__.FinalReport__.pdf

Reichmann, K. (November 16, 2020). Is the Aviation Industry Doing Enough to Mitigate Insider Threats Amid the COVID-19 Pandemic?; Aviation Today, Accessed September 20, 2022). https://www.aviationtoday.com/2020/11/16/aviation-industry-enough-mitigate-insider-threats-amid-covid-19-pandemic

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.

RTCA. (June 2021). DO-230K Standards for Airport Security Access Control Systems.

Salus Solutions. (March 2021). *PARAS 0026: Insider Threat Mitigation at Airports*; National Safe Skies Alliance, Inc. https://www.sskies.org/images/uploads/subpage/PARAS_0026_InsiderThreatMitigation.FinalReport_.pdf

Spamer, B. & Packard, G. (December 13, 2017). Effective Use of the National Missing and Unidentified Persons System (NamUs) for Case Resolution; National Indigenous Women's Resource Center.

TSA Aviation Security Advisory Committee. (April 8, 2015). *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control*. Accessed August 5, 2022, https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf

TSA. (October 2, 2020). *Boston TSA officers stop FBI imposter from boarding flight*. Accessed September 12, 2022. https://www.tsa.gov/about/employee-stories/boston-tsa-officers-stop-fbi-impostor-boarding-flight#:~:text=When%20a%20woman%20approached%20the,FBI%20credentials%20and%20a%20badge

TSA. (March 3, 2021). *Centralized Revocation Database (CRD) Frequently Asked Questions (FAQs).*

TSA. (November 15, 2021). *Centralized Revocation Database User Guide for Airport and Aircraft Operators Version 1.3.*

TSA. (n.d.). *Disqualifying Offenses and Other Factors*. TSA. Accessed September 12, 2022.

TSA. (2018). *Insider Threat Awareness ICAO Global Aviation Security Symposium 2018*. TSA. www.icao.int/Meetings/AVSEC2018/Documents/TSA%20Insider%20Threat.pdf

TSA. (2020). Insider Threat Roadmap; TSA.

U.S. Attorney's Office, Northern District of Georgia. (August 15, 2022). *Former baggage handler sentenced for smuggling loaded firearms onto aircraft*. Press Release. Accessed August 15, 2022. http://www.justice.gov/usao-ndga/pr/former-baggage-handler-sentenced-smuggling-loaded-firearms-aircraft

U.S. Department of Homeland Security. (April 27, 2020). *Privacy Impact Assessment for the Airport Access for Aviation Workers.*

U.S. Department of Transportation. (June 10, 2021). *Privacy Impact Assessment Federal Aviation Administration (FAA) Office of Information & Technology Services (AIT) Pilot Records Database (PRD).*