PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0029 August 2023

Criminal History Records Checks (CHRC) and Vetting Aviation Workers Guidebook

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Lori Beckman
Aviation Security Consulting, Inc.

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 0029 PROJECT PANEL

Colleen Chamberlain *American Association of Airport Executives*
Lauren Curtis *Port of Seattle*
Antonella DeFillipis *Massachusetts Port Authority*
Jacob Graef *Port of Oakland*
Arayna Hamilton *Jacksonville International Airport*
Linda Jacobsen *Port of Seattle*
Abedoon Jamal *San Francisco International Airport*
Dawn Lucini *Telos Identity Management Solutions*
Tammi Schreier *State of Alaska Department of Transportation*
Michael Weis *CTI Consulting*

AUTHOR ACKNOWLEDGMENTS

The research conducted for this guidebook was performed under PARAS 0029 by Aviation Security Consulting, Inc. with the assistance of TransSolutions, LLC.

Lori Beckman of Aviation Security Consulting, Inc. was the Principal Investigator for the project update, and Kiran Dhanji was the Subject Matter Expert. Gloria Bender, Andy Entrekin, and Jessica Gafford assisted with the original research and data collection.

The research team would like to acknowledge the airports who took time out of their busy schedules to help make this guidebook robust and useful to all sized airports. It is only through the support of airports that Safe Skies is able to continue to provide the aviation industry with valuable research on practical airport-related topics. Finally, the research team wants to thank the panel of volunteers who lent their expertise and time to ensuring the guidebook would be useful and applicable.

CONTENTS

TABLES & FIGURES

SUMMARY

This document provides step-by-step guidance and reference material for individuals who conduct and adjudicate criminal history records checks (CHRC) required under 49 CFR §§ 1542.209 and 1544.229.

Since the implementation of the CHRC requirement in 1997, there have been few changes or updates to regulations or guidance documents. This has led many in the aviation industry to seek additional guidance to ensure:

- The CHRC process aligns with the present-day threat environment
- Potential vulnerabilities are considered and addressed
- Individuals conducting and adjudicating CHRCs are properly trained
- Industry partners understand how to comply with CHRC and Rap Back requirements

These issues and others are addressed in this guidance.

Some airports have elected to exceed the minimum federal regulations based on their local environment or past incidents. This guidebook provides an overview of the current regulations, along with suggestions and guidance for those airports and air carriers that want to exceed the minimum federal requirements, to provide a more comprehensive vetting process for their employees and subsidiary employees.

Over 200 US airports and numerous air carriers were contacted during this research. The research team performed surveys, interviews, and literature reviews. Other industries that vet their employees were also reviewed to determine if their practices might benefit the aviation industry. Some of the key findings identified during the research include:

- Many airports and air carriers are subject to additional state, local, and in some cases tribal regulations and laws
- Parties may not fully understand the categories of crimes
- Methods to adjudicate potentially disqualifying CHRC and Rap Back results differ among airports
- Airports and air carriers should work closely with their local legal counsel when adjudicating applicants' criminal histories

Airports of any type and size can apply the information in this guidance.

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

ASC	Airport Security Coordinator
CHRC	Criminal History Records Check
CHRI	Criminal History Record Information
DAC	Designated Aviation Channeler
FPRD	Fingerprint Results Distribution
GAO	Government Accountability Office
HSIN	Homeland Security Information Network
ICAO	International Civil Aviation Organization
ID	Identification
IdHS	Identity History Summary
IDMS	Identity Management System
LEO	Law Enforcement Officer
MNC	Manual Name Check
NGI	Next Generation Identification
NPRM	Notice of Proposed Rulemaking
OIG	Office of Inspector General
OPM	Office of Personnel Management
PII	Personally Identifiable Information
RBN	Rap Back Activity Notification
RBUG	Rap Back User Guide
SARP	Standards and Recommended Practices
SAVE	Systematic Alien Verification for Entitlements
SD	Security Directive
STA	Security Threat Assessment
TWIC	Transportation Worker Identification Credential
USCIS	United States Citizenship and Immigration Services

UCMJ	Uniform Code of Military Justice
USPS	United States Postal Service

SECTION 1: BACKGROUND

Airports and domestic air carriers are required to conduct a fingerprint-based criminal history records check (CHRC) on applicants seeking unescorted access to an airport's SIDA or Sterile Area. CHRCs must also be conducted on individuals who will be authorized to perform screening, checked baggage, or cargo functions. The applicant must be subscribed into Rap Back at the same time that the CHRC is requested.

49 CFR §§ 1542.209 and 1544.229 include a list of disqualifying criminal offenses. An applicant or current employee is prohibited from receiving or maintaining a SIDA badge if they have been convicted, or found not guilty by reason of insanity, of any one of those crimes within the past 10 years. An applicant who has been issued a SIDA badge is required to self-report any disqualifying criminal convictions.

As of the date of this report, this list contains 28 disqualifying crimes and has only been expanded once since implementation of the requirement. It represents the minimum disqualifiers, or the baseline. Some airports choose to exceed the federal regulations and impose more rigorous screening and vetting standards in accordance with the laws of their specific jurisdictions.

The research revealed an overall belief that the list of disqualifying crimes should be expanded and the 10-year look-back period increased. Additionally, local authorities face considerable challenges in obtaining criminal history record information (CHRI) beyond the fingerprint-based CHRC in the absence of a federal requirement.

Congress recognized some of these issues in the *FAA Extension, Safety, and Security Act* of July 2016. The act, in part, directs the TSA to propose rulemaking that would expand the look-back period to 15 years. It also requires the TSA to issue a notice of proposed rulemaking (NPRM) to update the disqualifying crimes list. As of this publication, the TSA has not issued an NPRM to update 49 CFR §§ 1542.209 and 1544.229.

Based on concerns expressed by aviation industry representatives during project research, this document offers suggestions and guidance to airports and air carriers to assist them in complying with or exceeding the current federal minimum requirements.

A glossary of common terms used in the vetting process can be found at the end of this guidebook.

DOCUMENT FLOW

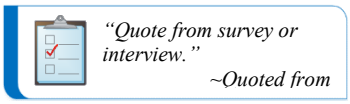
This guidebook moves step-by-step through the CHRC process. The following icons are used throughout the document to call attention to important information:

A Best Practice has been successfully implemented at a US airport and is provided with the intent that other airport operators or air carriers may find it useful in their environment.

Recommendations are based on the authors' research and experience with airport badging and adjudication. Recommendations could be applicable to all airport sizes and categories.

Training opportunities are suggestions to enhance existing training programs or additional training that may improve the CHRC or vetting process.

Caution icons warn the reader of potential legal or regulatory issues. Where a caution note is provided, airport operators or air carriers should consider seeking legal guidance.



Quotation boxes are direct quotes received from the airport operator or air carrier surveys.

Application Process

In order to obtain an airport ID badge, an applicant must first complete an application form. Most airports provide fillable PDF application forms on their website since handwritten forms may be difficult to interpret and data entry errors can cause processing delays. Applicants must provide information about their background and attest that they have not been convicted or found not guilty by reason of insanity of any of the 28 disqualifying crimes listed in the federal regulations. Some airports provide a paper copy of a disqualifying crimes declaration form. The applicant makes the appropriate selections, and then signs and dates the form.

A growing number of airports use an electronic database or system, such as an Identity Management System (IDMS), to collect the badging application information and disqualifying crimes attestation from the applicant. If so, the badging application information may be entered by the Authorized Signatory or applicant via an online portal or link. The disqualifying crimes form is then filled out by the applicant, usually through a secure link sent by the Authorized Signatory or during the fingerprinting process using a tablet in the credentialing office. The applicant must also sign the fingerprint application before fingerprints are captured.

The use of a system like an IDMS reduces the risk of missing information by preventing the application from moving forward until all the required fields have been completed. It also minimizes some types of data entry errors. However, these systems are costly and may not be feasible for all airports.

Authorized Signatories should be trained to assist applicants with the application process and review the application for missing information before it is submitted to reduce processing delays.

When asked about existing processes or lessons learned regarding disclosure and release forms, most airports indicated that they followed the current Security Directive (SD) language. However, many airports have modified their badge application forms to include additional language, which often involves suitability clauses. Examples of additional language collected during airport outreach can be found in Appendix A.

"Make sure you very clearly indicate that you want a crime reported (regardless of look back period) if you want to consider those crimes/look back period."

~Survey Respondent

Verification of Identity and Work Authorization Documents

Following the requirements in 49 CFR §§ 1542.209 and 1544.229, an airport operator's Trusted Agent or an air carrier staff member must verify the identity of the applicant through two forms of identification prior to fingerprinting and ensure that the printed name on the CHRC application is legible. At least one of the two forms of identification must have been issued by a government authority, and at least one must contain a photograph. Form I-9 shows the US Citizenship and Immigration Service

(USCIS) list of acceptable documents that can be presented by the applicant. Go to www.uscis.gov/i-9 for the most current version.

Airport operators are required to examine the documents to determine whether they appear to be genuine and relate directly to the individual presenting them. Some airports do not accept all documents included on the Form I-9 list because they are either unable to authenticate the document presented by the applicant or their staff cannot identify all the documents listed, since some documents on the list are obscure and rarely used.

Airport operators should provide Trusted Agents and Authorized Signatories with ongoing document authenticity training, focusing on the documents listed in Form I-9. Training is available at no cost from many airports' federal or state partners such as the TSA, US Customs and Border Protection (CBP), and local law enforcement officers (LEO). These agencies are often willing to assist airports in authenticating documents that are presented by badge applicants.

Inaccurate application of requirements may result in improper processes. For example, although a passport generally is considered excellent proof of identity and work authorization, individuals may present a variety of other documents in place of a passport, and personnel should be trained to verify the authenticity of each document on the Form I-9.

Remember to check for updates to the Form I-9 list to ensure you are always using the most up-to-date document. Checking for updates every six months is recommended.

Since the security features in most government documents have improved significantly over recent years, CBP officers have noted an increasing trend of legitimate/genuine documents being presented by imposters at major airports. The types of fraudulent or deceptive identity issues experienced by local CBP are often an indicator of what the credentialing office may experience as well.

It is important for airport operators and air carriers to recognize the potential for the use of genuine documents presented by imposters in the credentialing process, and the need to develop policies and procedures to handle a potential imposter who presents genuine documents. Airports that have developed such procedures often have agreements with law enforcement agencies onsite to provide support to the credentialing staff in verifying the authenticity of the documents and the identity of the individual presenting them.

Many federal agencies can provide local imposter recognition and fraudulent documentation training to Trusted Agents to assist with this issue.

E-Verify and SAVE

Airport operators have access to the USCIS's E-Verify system and Systematic Alien Verification for Entitlements (SAVE) system to help determine the eligibility of individuals seeking unescorted SIDA access.

E-Verify is an internet-based system through which employers verify the employment eligibility of their applicants before hire. In short, employers submit information taken from a new hire's Form I-9 through E-Verify to the Social Security Administration and USCIS to determine whether the information matches government records, and whether the new hire is authorized to work in the United States.

The E-Verify website (www.uscis.gov/e-verify) provides a host of information about the program, as well as specific user manuals, quick reference guides, and information on employee rights and employer obligations.

The SAVE program does not determine eligibility for benefits—including airport ID badges—but it does verify immigration status for use in determining such eligibility. Thousands of federal, state, and local agencies use the SAVE program.

According to TSA, some agencies use a web service connection to directly download SAVE electronic responses into their adjudication systems, but most end users access the SAVE website through a secure login, enter certain data points, and receive immigration verification status electronically within seconds. Most verification is completed on the first step. If not, SAVE institutes further verification, requesting any additional information needed. The additional information is then reviewed by USCIS "status verifiers" and a verification result is generally provided within 3–5 days. USCIS provides training on how to use SAVE and can provide training to individual airports if requested.

CHRC Overview

Once an applicant completes the application, the CHRC process can begin. The system used to request a CHRC is managed by the FBI. There are other state-managed or privately run systems for accessing CHRI, but the FBI-managed system is required for issuance of airport ID badges. Understanding the CHRC system used by airports and air carriers is critical for identifying the strengths and limitations of the current system.

When the initial regulatory requirement for background checks was established in 1997, airports and air carriers were given latitude to determine how the requirements would be implemented. Therefore, the CHRC methodology varies by airport and may include:

- Fingerprinting and adjudicating every employee, including air carrier employees covered under the air carrier regulation
- Only fingerprinting those under airport responsibility per 49 CFR § 1542 and requiring the air carriers to manage the entire process for their covered employees

Air carriers are required to manage the process for their covered employees. The process varies by carrier; some primarily adjudicate CHRCs at the corporate headquarters level and provide local stations with certification letters, while others adjudicate at local stations. Certification letters to be provided to the airport must always include the FBI case number, the date the applicant was subscribed into Rap Back, and the date the CHRC was successfully completed. This confirms to the airport that the air carrier has conducted a fingerprint-based CHRC, determined the results revealed no disqualifying convictions, and subscribed the individual into Rap Back (unless the individual has unclassifiable [i.e., illegible] prints).

Some airports choose to accept certification letters, while others prefer to conduct the CHRC and maintain their own Rap Back subscription on the applicant or badge holder. When both the airport and air carrier wish to subscribe the same person, then each organization conducts a separate CHRC and Rap Back enrollment. If the airport chooses to accept the air carrier certification, the airport will not have access to the case record in the Fingerprint Results Distribution (FPRD) and will not directly receive any Rap Back Activity Notifications (RBN) of subsequent criminal activity.

Regulation requires that airports must advise the applicant that a copy of the criminal record received from the FBI may be provided if requested in writing by the applicant, and that the Airport Security Coordinator (ASC) is the applicant's point of contact for questions. Air carriers must provide the same disclosure to applicants along with a point of contact for questions. The applicant must also be informed that federal regulations impose a continuing obligation to disclose to the airport or aircraft operator within 24 hours if they are convicted of any disqualifying criminal offense.

When the airport is notified by an aircraft operator that a certification is withdrawn, the airport must immediately revoke any unescorted access authority. The airport must maintain the letter for a minimum of 180 calendar days after the individual is no longer covered by CHRC requirements.

Rap Back Overview

The FBI's Rap Back program is an automated service that notifies an authorized agency (airport or air carrier) of criminal events or activities that are associated with an enrolled badge holder's fingerprints and are reported after the initial CHRC is conducted. This allows airports and air carriers, as authorized agencies, to evaluate continued badge/access privileges without relying on the badge holder to self-report a disqualifying event. The FBI and TSA do not charge for Rap Back enrollment, but DACs may charge subscription fees.

Rap Back implementation was mandated for airports in TSA-National Amendment 21-03, effective March 29, 2022, with SD 1542-04-0Q, which included Rap Back edits. Aircraft operators also received a mandate that requires that all covered SIDA badge holders who require a CHRC and have classifiable prints be subscribed in Rap Back by March 29, 2024. Badge holders with unclassifiable prints must be subject to a recurrent Manual Name Check (MNC) process by March 29, 2024. All initial CHRCs must be submitted with a "Search and Subscribe" transaction or they will be rejected.

Rap Back and its associated processes are briefly described in this section and referenced throughout the document. TSA's *Rap Back User Guide for Airport and Aircraft Operators*, commonly referred to as the RBUG, is available via TSA's Homeland Security Information Network (HSIN) web board and the Fingerprint Results Distribution (FPRD) site. This document must be referenced in the ASP, and Trusted Agents in the credentialing office who use the FPRD and/or perform applicant suitability determinations must be familiar with its contents. The content is updated as needed and provides detailed information and useful instructions for navigating Rap Back. The version referenced in this document is 3.3, issued in March 2023.

Airports and air carriers should also carefully review all TSA Aviation Worker Bulletins addressing Rap Back to ensure awareness of program or process changes. Airports and air carriers receive these bulletins directly from their Designated Aviation Channelers (DAC), associations, and HSIN.

RAP BACK SUBSCRIPTIONS

To subscribe a current badge holder, the airport or air carrier will submit a Subsequent Rap Back Subscription transaction. When subscribing badge holders in bulk, TSA recommends ensuring there are adequate resources to review the results of new subscriptions within three business days of receipt.

To subscribe a new badge applicant, the airport or air carrier will submit a Search and Subscribe transaction, which includes the request for the initial CHRC fingerprint search and a request that the FBI retain the fingerprints and set up a new Rap Back subscription in NGI. For more information on subscribing new badge applicants, refer to Step 2: Submit via DAC in Section 2 of this guidebook. Detailed enrollment instructions are included in TSA's RBUG.

RAP BACK ACTIVITY NOTIFICATIONS

Triggering events that will result in an RBN are standardized and cannot be changed by the participating agency. They include the following:

- Arrests
- Dispositions, including expungement and partial expungement
- Want/warrant issuance or deletion

- Sex Offender Registry addition or deletion
- Death notices

The events are recorded on the individual's Identity History Summary (IdHS)—formerly known as a rap sheet—which is considered personally identifiable information (PII) and must be protected and kept secured.

RBNs may also be received for Consolidation Notifications and Identity Deletion/Restoration.

Timely RBNs are dependent on available records from law enforcement agencies and courts. RBNs may be received weeks or even months after an arrest or update to a case.

MAINTENANCE TRANSACTIONS

A Rap Back maintenance transaction is used to perform several types of actions for a subscription, such as replacing or modifying biographic data (e.g., name changes, spelling corrections), extending expiration dates, renewing an expired subscription, or cancelling an active subscription.

Airports and air carriers must cancel a Rap Back subscription within five business days from the date they are notified or made aware that the individual is no longer covered by CHRC requirements.

See Rap Back Maintenance in TSA's RBUG for additional information.

SUBSCRIPTION EXPIRATION

All subscriptions are required to have a validation and an expiration date as part of Rap Back's privacy risk management strategies. A Rap Back Renewal Notification is sent 10 days before the expiration date, giving the airport or air carrier time to manage the notifications. TSA recommends that airports and air carriers review each expiration notification within five business days, confirm that the subscription is still valid, and extend it with a new expiration date. Subscriptions are automatically removed from the system by the FBI upon expiration.

TSA states that airports and air carriers must implement a process to review subscriptions as the expiration date approaches. Reports and notifications provided in FPRD can be used in this process.

See Rap Back Renewal Notification in TSA's RBUG for additional information.

Privacy Risk Mitigation

Trusted Agents will handle PII in IdHS. It is important that agents understand how to safeguard this information. These five strategies are part of privacy risk mitigation:

- Provide an **informational briefing** to staff who will handle PII
- Confirm the Trusted Agent has the **authority** to access information in FPRD before viewing it
- **Validate subscriptions** by reviewing reports of subscriptions about to expire, and ensuring that subscriptions are not held on individuals for whom the airport or air carrier is no longer authorized to hold a subscription
- Provide applicants with the **Privacy Act Notice** when fingerprints are captured
- Establish **formalized procedures** for setting, modifying, extending, cancelling, and synchronizing Rap Back subscriptions

TSA Contact Information

Submit inquiries specifically related to Rap Back to rapback@tsa.dhs.gov.

Submit inquiries specifically related to FPRD to FPRD-Helpdesk@tvs.tsa.dhs.gov.

Submit inquiries or requests for support from TSA to aviation.workers@tsa.dhs.gov.

Submit inquiries or requests for support related to the CHRC to CHRCRequests@tsa.dhs.gov.

Section 1 – Summary of Best Practices and Recommendations

- To reduce processing delays, Authorized Signatories should be trained to assist applicants with the application process and review the application for missing information before it is submitted.
- Provide ongoing document recognition training for Trusted Agents and Authorized Signatories focusing on the Form I-9 document list to comply with TSA regulations and SD requirements.
- Check for updates to the Form I-9 list every six months.
- The TSA recommends that airports and air carriers establish a process for extending or canceling Rap Back subscriptions prior to their expiration date.

SECTION 2: THE CHRC PROCESS

Steps 1 through 8 describe the baseline adjudication process flow required by 49 CFR §§ 1542.209 and 1544.229, as well as associated Rap Back steps.

Step 1: Complete Application, Capture Prints, and Request CHRC

The completed airport ID badge application form is either brought by the applicant to the initial fingerprinting appointment or is routed by the Authorized Signatory (see Application Process, page 2).

Fingerprints are generally captured and processed electronically. Many airports have migrated to Type 14 ("slap") prints, replacing the slower individual finger rolling process required in the first generations of electronic technology. The newer technology has reduced the time taken to capture "good" prints and resulted in fewer "null" prints. There are only a few airports and air carriers that continue to roll prints on fingerprint cards, which must be approved by the FBI and distributed by the TSA for that purpose.

TSA recommends cleaning the livescan plate between each fingerprint collection session to help eliminate residual fingerprint patterns ("ghost prints") that may interfere with the fingerprints being collected. Find additional recommendations on technique in the RBUG.

At the time of applicant fingerprinting, the airport Trusted Agent or air carrier staff member must provide the applicant with a fingerprint application that includes the list of the 28 disqualifying criminal offenses and a statement that the individual signing the application does not have a disqualifying criminal offense. In addition, a statement must be provided to inform the applicant of their continuing obligation to disclose to the airport or air carrier, within 24 hours, if convicted (or found not guilty by reason of insanity) of any disqualifying criminal offenses that occur while the individual has unescorted access authority.

The airport must also have the applicant read and sign a certification statement when collecting fingerprints. The language in the certification statement is periodically updated by the TSA, and airports should refer to the latest regulations to ensure they use the current version. The applicant must sign and date the fingerprint application acknowledging their understanding of the regulation prior to submitting fingerprints.

In addition, the airport must present the Privacy Act Notice to each applicant or MNC renewal candidate, which advises that their biographic information will be retained and searched in the FBI database, and that their information may be shared with authorized parties. The language is updated periodically by the TSA, and airports should refer to HSIN to ensure they use the current version.

Airports and air carriers have the right to include additional statements on the badge application, such as security responsibilities acknowledgements. However, prior to adding any statements to the application process, airport operators or air carriers should consult with local legal counsel.

Examples of additional statements reported in airport surveys can be found in Appendix A.

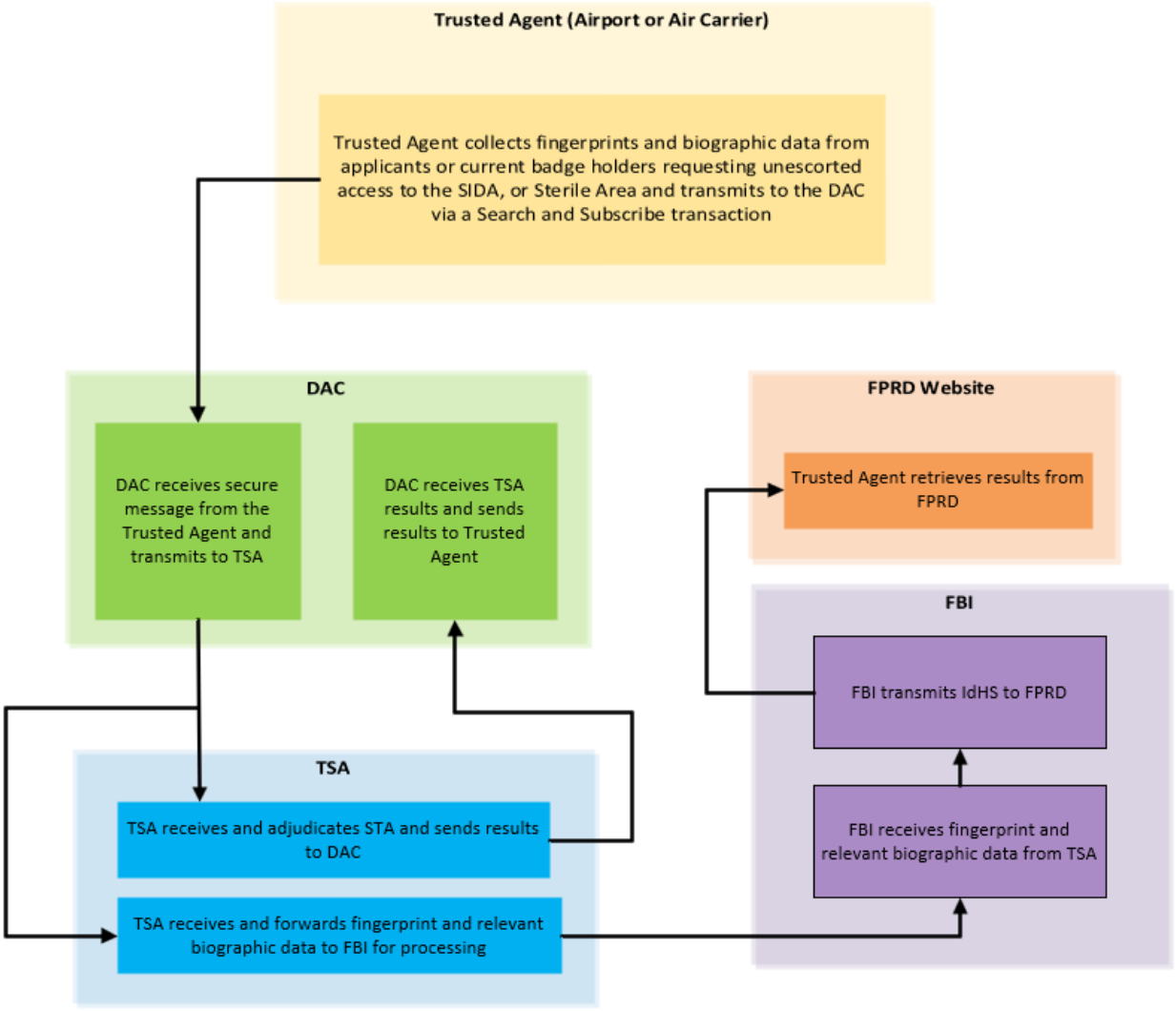
Step 2: Submit via DAC

Airports and air carriers submit biographic and biometric data to a DAC. The DAC channels the data to TSA for it to conduct a security threat assessment (STA), and for the FBI to conduct a CHRC and associated Rap Back transactions. A summary of the history of DACs is in Appendix B.

The DAC provides airports and air carriers with an online method for transmitting biographic and biometric information to the TSA. Most airports transmit biographic STA information to the DAC electronically. However, some airports use Excel spreadsheets to report biographic data to their DAC, which can result in a high rate of error responses and cause delays in receiving STA results. Airports should consider an automated method to transmit biographic data to their DAC in order to reduce errors and encourage prompt receipt of the results.

Regardless of how the information is transmitted, the information flow remains the same (see Figure 1). It is important for Trusted Agents and air carrier staff to be aware of the information flow and how data errors can disrupt or delay the process.

Figure 1. Flow of Information through DAC



ENROLLMENT IN RAP BACK

Requests for CHRCs and Rap Back enrollments both flow through the DAC. Detailed information on enrollment is located in TSA's RBUG.

Requests for an initial CHRC must be submitted as a Search and Subscribe transaction. This results in both the airport receiving the applicant's IdHS and the applicant being enrolled into Rap Back. To

subscribe a current badge holder, Trusted Agents submit a Subsequent Rap Back Subscription transaction.

The subscription expiration date can be set to coincide with the badge expiration date or earlier, but it cannot exceed two years from the date of subscription inception. There is no limit on the number of times a Rap Back subscription can be renewed, but each renewal term is limited to a maximum of two years.

An authorized agency (such as an airport operator) cannot submit a Rap Back Search and Subscribe transaction for another authorized agency (such as an air carrier) using the air carrier's Submitting Organization Number (SON).

If an airport wishes to maintain a Rap Back subscription on an applicant who already has had a CHRC conducted by another agency, the airport must submit its own CHRC request using the Search and Subscribe transaction.

Step 3: Retrieve Results via FPRD

The FPRD website is used by airports and air carriers to obtain the results of badge applicants' CHRCs and any subsequent RBNs.

RBNs are posted in the FPRD whenever there is a triggering event. Airports and air carriers need to have protocols established for the handling of non-disqualifying arrests. For example, driving under the influence (DUI) is not on the list of 28 disqualifying offenses, but if the person has driving privileges, the airport needs to decide if a DUI arrest will trigger any action.

Additionally, airports and air carriers should be prepared to receive RBNs that are superfluous, such as administrative updates from the courts or law enforcement agencies (new court templates, updates to personal information, etc.). These types of notifications can be frustrating and time-consuming for adjudicators and could result in a full adjudication if notes are not made during initial and subsequent adjudication.

Keeping notes on case disposition discoveries may help to eliminate repeated investigations during the badge renewal process. This is especially true for RBNs, which may not indicate what was changed on the IdHS. The FPRD website has a comments section on each individual's record that could be utilized for this process. All comments should include dates for easy reference.

TSA regulations 49 CFR §§ 1542.209 and 1544.229 cover the dissemination of results from criminal record information provided by the FBI.

No person may disseminate the results of a CHRC to anyone other than:

- The individual to whom the record pertains or that individual's authorized representative
- Officials of other airports who are determining whether to grant unescorted access to the individual under this Part
- Aircraft operators who are determining whether to grant unescorted access to the individual or authorize the individual to perform screening functions under 49 CFR § 1544
- Others designated by TSA

Step 4: Evaluate

In this step, the Trusted Agent confirms that a record has been received.

Applicants' fingerprints are sometimes deemed unclassifiable. When this occurs, further action is required through the FPRD, with the exact steps depending on whether potentially matching candidates were found. It is not possible to establish a Rap Back subscription with unclassifiable prints; the airport must conduct recurrent MNCs instead. See TSA's RBUG Appendix G – Unclassifiable (Low Quality) Fingerprints for detailed instructions.

An IdHS may be returned incomplete, meaning that it contains arrests without a final disposition, an expungement, or sealed case information that has been removed from the state and FBI summary. Airports that receive an incomplete summary should request more information from the FBI via the FPRD website. The website recommends that the airport then compares the requested IdHS to the original, incomplete summary to see what has been changed.

Step 5: Determine Record/No Record

Next, the Trusted Agent determines if the individual has a record. If the results show no criminal record, the Trusted Agent may move to Step 8: Final Badging Decision. If the IdHS does show a criminal record, the Trusted must move to Step 6: Adjudicate, in which the data will be reviewed to determine whether the individual is disqualified.

WANTS AND WARRANTS

An IdHS may include an active want or warrant. Many airports elect to focus their efforts solely on the credentialing process and consider wants and warrants to fall under law enforcement jurisdiction. An airport in this circumstance may choose to simply notify the warrant issuer that the individual has applied for a position, but not release any other information (PII such as address or contact number should be kept confidential). Airports need to develop a policy regarding the action they will take if an active want or warrant is found during a CHRC or in an RBN. Local legal advice should be sought when developing policies.

Some airports run an annual Wants and Warrants check for all airport ID badge holders. However, once users are subscribed into Rap Back, annual Wants and Warrants checks become unnecessary as the subcribing entity will receive an RBN for triggering events. Local legal advice should be sought prior to performing a Wants and Warrants check.

Step 6: Adjudicate

Some airports use formally trained active or former police personnel to interpret and adjudicate IdHS and penal codes, since they are generally more knowledgeable on the topic than civilian staff. But many adjudicators have no formal training on the CHRC process, only on-the-job training and the assistance of LEOs.

An individual with prior experience reviewing criminal records will be able to examine the conviction information more easily and efficiently. In addition to knowledge of IdHS terminology and varying penal codes, adjudicators must have an understanding of regulatory requirements to ensure they are applying the regulations correctly. Training information can be found in Appendix C.

Local legal counsel or law enforcement should be consulted if the adjudicator is uncertain as to the elements of past action, complicated records, or when there is possible expungement of a prohibited conviction.

According to 49 CFR §§ 1542.209 and 1544.229, an applicant is disqualified if they were convicted, pled guilty (including no contest), or were found not guilty by reason of insanity for any of the disqualifying crimes in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

Some airports include additional disqualifying crimes and suitability determinations in their policies (See Section 3 for more information).

Adjudicating a record against the 28 disqualifying crimes specified in 49 CFR §§ 1542.209 and 1544.229 involves a three-factor analysis, which assesses whether the individual has:

1. **A disqualifying offense arrest** – The initial review of the IdHS should look at each arrest. The charge describes the reason for the arrest. Depending on the jurisdiction, it may list the criminal code that was violated, or if it was a felony or misdemeanor. Generally, this is enough information to determine whether the arrest falls under one of the 28 disqualifying offenses. If it is unclear whether the arrest may be for a disqualifying offense, move forward to determine if there is a conviction.
2. **A disqualifying offense conviction** – If the charges have been dismissed, then the offense is not disqualifying. It is common for the conviction to be for a lesser charge that may not be disqualifying.
3. **A disqualifying conviction within the specified look-back period** – If the date of the conviction is more than 10 years old (or whatever look back the airport has defined), the offense is not disqualifying. If the conviction is within the look-back period, the individual is disqualified.

Once airports receive potentially disqualifying results from the CHRC, they may adjudicate them differently due to their state and local rules and regulations. Adjudication resources are noted in Appendix D.

Some airports responded that they use a local TSA resource to assist in the adjudicating process. While it is not the TSA's responsibility to vet records, the agency may be consulted for a legal opinion or direction on complex records. An example where TSA may be willing to assist is when a record is returned and the individual supplies legal paperwork that shows their record should have been sealed or expunged. TSA's legal opinion would serve as the final say on these matters.

LACK OF DISPOSITION

Local, state, and federal courts may fail to promptly report final dispositions, so CHRCs often show an arrest but no corresponding conviction. When this occurs, federal regulations require that adjudication staff conduct an investigation to determine that the arrest did not result in a disqualifying offense before issuing that applicant an airport ID badge. Additionally, there may be arrest and conviction information but no indication of sentencing, or the charges may have been plea-bargained, reduced, deferred, dismissed, or enhanced based upon a variety of factors. This compounds the confusion.

Many airports notify the applicant that there is a potentially disqualifying offense and request that they provide official, certified court documentation confirming that they were not convicted.

The best practice for determining the adjudication for these records is to have the applicant provide court-certified copies of the disposition. If the documents are sent electronically, they should come directly from the court to ensure legitimacy of the documents, not from the applicant or the applicant's attorney.

Additionally, the applicant may be required to interview with the airport adjudicator when the documents are presented to the airport. Adjudication interviews can be emotional for applicants, so having two staff members in the interview helps to maintain an orderly and safe environment. This best practice also provides a level of protection from accusations of impropriety.

Some airports have staff research and adjudicate the record. However, investigating court records on behalf of an applicant can consume incredible amounts of time and not all airports have the resources to devote to this level of effort. Locating the proper contact for a given jurisdiction; obtaining the proper, certified documents; paying, if required, the costs associated with retrieval; and demonstrating that you have authority to obtain the documents can be tedious. Typically, applicants have much easier access to these records.

When adjudicating applicants with an arrest or outstanding warrant that has no disposition, airports may choose to wait until the applicant can present evidence that a disposition has been reached before making a final determination on badge issuance.

DISCLOSURE TO APPLICANT

Before making a final badging decision, the adjudication staff must inform the applicant if the CHRC results disclose information that would disqualify them from being issued an airport ID badge (refer to Step 7: Corrective Action and Appeals Process). Airports often send the applicant an email stating that the badge will be denied if information is not provided within 30 days to prove that there is no disqualifying criminal offense.

TSA'S LEGAL GUIDANCE ON CRIMINAL HISTORY RECORDS CHECKS (2004)

In a memorandum entitled "Legal Guidance on Criminal History Records Checks," TSA offers guidance on issues that may present themselves during the adjudication process. While this guidance is not conclusive, most courts will strongly consider an agency's interpretation of its own regulations.

The TSA Memorandum suggests that the meaning of disqualifying crimes is the meaning given under federal law. The document offers case law to support that position. It also notes that entries on the IdHS may be incomplete and require review of judgment and sentencing documents so that the actual offense that serves as the basis for conviction can be identified.

The TSA Memorandum asserts that certain misdemeanor offenses, mostly related to the illegal use or possession of a weapon, can be considered disqualifying. It also states that juvenile records are generally not considered for the purposes of the CHRC statute, except when the juvenile is tried and convicted as an adult. In such circumstances, the criminal record should be considered when determining whether the individual has a disqualifying offense.

TSA also discusses the airport/air carrier's authority to apply suitability criteria when adjudicating CHRCs. These suitability determinations may be used by the airport/air carrier, but should be vetted with the airport/air carrier's legal counsel to ensure compliance with state and local laws, as well as federal regulations.

FEDERAL AND STATE EQUIVALENCE

The disqualifying crimes specified and defined by federal law are often not the crimes that badge applicants are charged with or convicted of. Frequently, the crimes are governed by similar but not identical state law provisions. The first factor of adjudication is an inquiry to determine equivalence. The TSA Memorandum provides little insight on rules to govern this process.

One airport has paid a private law firm approximately $30,000 to develop an analytic matrix ("cheat sheet") comparing their state's offenses to the 1542.209(b) offenses. While this option may be cost prohibitive for many airports, creating a cheat sheet of commonly encountered disqualifying penal codes is more economical and has the added benefit of becoming a training tool for new adjudicators.

Appendix D contains a listing of useful resources for checking state penal codes.

A properly trained person, such as an attorney or LEO, should be consulted when there is a question as to the wording of a conviction as it relates to matching disqualifying crimes. That person will often need to review additional court records to determine if the applicant has been found guilty based on the underlying elements of a disqualifying crime.

Many airports use two people to adjudicate each record. This provides a layer of quality control and consistency in the adjudication process. Adjudicating can be complex, and having a second person review the adjudication decision has been found to be helpful. Ideally, at least one of those reviewers should be a sworn LEO.

In the absence of guidance or information on TSA practices, local legal counsel should look to legal precedence for similar adjudication practice under other federal statutes that may offer guidance for airports. A significant body of case law has grown around the adjudication of federal statutory provisions allowing for mandatory sentencing (like mandatory sentences for individuals who are habitual offenders and have been found to have been convicted of other predicate crimes). As is the case with the 28 disqualifying crimes, the statutes are defined under federal law, but the crimes of conviction may be state law offenses.

EQUIVALENCE BETWEEN STATES

Many adjudicators have been in the position for enough time that they are able to interpret common penal codes from neighboring states with confidence, particularly for airports located near state borders. In the absence of that experience, a state website that describes each penal code is a useful resource in investigating equivalence between states. However, there is always a possibility that the penal codes have changed since the final disposition of the case at hand.

Links to each state's penal code website are located in Appendix D.

LOOK-BACK PERIOD

The current disqualifying look-back period is 10 years from the date of conviction. The TSA Memorandum notes that other transportation disciplines apply other rules with respect to the look-back period for disqualifying crimes. For persons seeking Transportation Worker Identification Credentials (TWIC) with Hazardous Material Endorsements, convictions for some offenses are permanently disqualifying, while conviction for other offenses require an additional look-back period of five years after release from incarceration for those crimes or seven years from the date of the application. Incarceration release date is not considered in the current look-back period for applicants seeking unescorted access under 49 CFR § 1542 or 1544.

However, some airports do not limit their adjudication of records to a 10-year look back from the date of conviction. Some redefine their 10-year look-back period so that it begins post-probation or post-parole. One airport sets a steadfast look-back date of December 6, 1991, which is the look-back period in Federal Aviation Regulation § 107.31 that was enacted in 1998.

MILITARY DISPOSITION CODES

Several airports indicated that they find military charges difficult to understand. The following information may clarify the different forms of court-martial to help airports and air carriers better align these charges with the civilian penal codes.

According to www.military.com, the Uniform Code of Military Justice (UCMJ) provides for three different types of court-martial: summary, special, and general. These forms of court-martial differ in their makeup and the punishments that may be imposed.

1. **Summary court-martial** consists of one commissioned officer and may try only enlisted personnel for noncapital offenses. The punishment that may be imposed depends on the grade of the accused. In the case of enlisted members above the fourth pay grade, a summary court-martial may impose any punishment not forbidden by the law except death, dismissal, dishonorable or bad conduct discharge, confinement for more than one month, hard labor without confinement for more than 45 days, restriction to specified limits for more than two months, or forfeiture of more than two-thirds of one month's pay. In the case of all other enlisted members, the court-martial may also impose confinement for not more than one month and may reduce the accused to the lowest pay grade, E-1.

2. **Special court-martial** consists of not less than three members and a military judge, or an accused may be tried by military judge alone upon request of the accused. A special court-martial is often characterized as a misdemeanor court, and may try all persons subject to the UCMJ, including officers and midshipmen. A special court-martial may impose any punishment authorized under Rules for Court Martial (R.C.M.)1003 except death, dishonorable discharge, dismissal, confinement for more than one year, hard labor without confinement for more than three months, forfeiture of pay exceeding two-thirds pay per month, or any forfeiture of pay for more than 1 year.

3. **General court-martial** consists of not less than five members and a military judge, or an accused may be tried by military judge alone upon request of the accused. A general court-martial is often characterized as a felony court, and may try all persons subject to the UCMJ, including officers and midshipmen. A general court-martial may adjudge any punishment not prohibited by the UCMJ, including death when specifically authorized.

In 49 CFR §§ 1570 and 1572, TSA determined that military personnel with a dishonorable discharge were not automatically disqualified because of the discharge. For individuals applying for a hazardous materials commercial driver's license, the TSA recommends that the underlying crime(s) or offense(s) that led to the discharge should be reviewed closely to determine the individual's suitability. The recommendation to carefully review an underlying charge is also appropriate for the aviation environment.

JUVENILE CASES

Juvenile cases are unique in that they are typically sealed and excluded from the public record when the individual turns 18. However, it is fairly common for the sealing of the records to be missed when the individual or their representative fails to notify the courts. In these instances, an open case without disposition may show up on the IdHS. Most adjudicators will then treat the offense in the same way as any other offense. If it is non-disqualifying, the offense is not a problem; if it is disqualifying, a letter is sent to the applicant stating that the badge will be denied unless paperwork is provided to indicate that there is not a disqualifying criminal offense.

In the TSA Memorandum, TSA asserts that juvenile records are generally not considered for the purposes of the CHRC statute, except when the juvenile is tried and convicted as an adult. In such circumstances, the criminal record should be considered when determining if the individual has a disqualifying offense. It is possible for the individual to work with the court during the appeals process to have the record sealed or expunged, in which case the offense would no longer be considered part of the IdHS.

INTERNATIONAL

Nearly all airports surveyed stated that they do not take extra steps to collect international criminal history. Many indicated that, because non-US citizens require a right-to-work authorization (e.g., Permanent Resident Card) and a criminal background check through the FBI, these serve as suitable proof of no serious criminal history.

RAP BACK ACTIVITY NOTIFICATIONS

When receiving an RBN for criminal activity, adjudicators generally follow the same process as for the initial IdHS. The adjudicator will first determine whether the notification indicates a disqualifying offense or circumstance. If the notification does not indicate a potential disqualifier, it will be marked as reviewed with no further action. Many adjudicators take the stance that the individual is innocent until final conviction.

Most adjudicators stated that if an RBN indicates an arrest for a disqualifying offense but has no disposition yet, the badge holder will be notified directly or sent a letter asking them to come to the credentialing office, and they will then be informed of the notification and any next steps or follow-up required. Badge holders should be given the opportunity to provide official court documentation indicating the updated status of the arrest. Should the arrest result in a disqualifying conviction, the badge must be revoked.

Each notification received must be marked as reviewed within three business days by clicking "Complete Review" on the IdHS Details page within the FRPD. TSA has clarified that "reviewed" indicates that the authorized agency has opened and read the RBN and has initiated the adjudication process, if necessary.

Adjudicators who have dealt with an arrest for a potentially disqualifying RBN offense indicated that the final disposition can take weeks or months from the first notice of arrest. Typically, adjudicators will monitor the situation closely, and will often update the badge expiration to coincide with the next court date or require the badge holder to check in regularly until a disposition has been made. By restricting the length of time the badge is valid, the airport will be able to control the situation and not have someone badged who may have been convicted of a disqualifying crime, thus reducing the potential security risk. If the final disposition shows that the offense or circumstance is disqualifying, the badge is revoked.

Some airports indicated that with the implementation of Rap Back, they have added a clause to the application indicating that failure to notify the badging office of a potentially disqualifying criminal arrest within a set time frame (varying from 24 to 72 hours), will result in the badge being suspended until the final disposition can be determined. Some of these airports require notification of any criminal arrest, regardless of whether the crime is potentially disqualifying or not.

INITIAL DETERMINATION OF DISQUALIFICATION

If the IdHS indicates that the applicant was convicted of any one of the disqualifying crimes, some airports have the adjudicator send the documentation to another party for a second opinion. The second opinion might come from the legal department, a law enforcement agency, or the airport's senior staff.

Other airports move directly to deny the badge unless information is provided to correct the record as outlined in Step 7: Corrective Action and Appeals Process. The applicant must have the opportunity to correct their record if it is inaccurate, but if the conviction is upheld, the applicant is disqualified from obtaining an airport ID badge. Other applicants who do not have a disqualifying crime are moved forward in the process to Step 8: Final Badging Decision.

INVESTIGATION RECORDS

The records of investigations must be maintained in a manner that is acceptable to TSA and in a manner that protects the confidentiality of the individual.

Records should be stored securely and only adjudicating staff should have access to this information. If using an IDMS, appropriate access permissions should be set.

The investigation record for each individual must be maintained until 180 days after the termination of the individual's unescorted access authority. When files are no longer maintained, the criminal record must be destroyed. Only direct airport operator employees under 49 CFR § 1542.209, or direct air carrier employees under 49 CFR § 1544.229, may carry out the responsibility for maintaining, controlling, and destroying criminal records.

Step 7: Corrective Action and Appeals Processes

Badge applicants who are found to have a potentially disqualifying offense in their record have the right to correct information they believe is erroneous or based on incorrect information in the FBI IdHS or federal status databases. This corrective action process is outlined in 49 CFR § 1542.209 (h).

Before final denial of an applicant's badge, the airport must inform the applicant of the potentially disqualifying information and provide a copy of the record upon request. The applicant then has 30 days to notify the adjudication staff in writing of their intent to correct any information they believe to be inaccurate. It is the applicant's responsibility to contact the local jurisdiction and/or the FBI to obtain the complete or correct information.

The adjudication staff must only accept a revised FBI record or a certified true copy of the corrected information from the appropriate court, and should ensure that corrected records have a certified court seal.

Once the corrective action process has been completed, the applicant is sent a letter advising them of the final decision. The employer is also notified that the applicant has been approved for or denied an airport ID badge. Due to TSA regulations, the airport may not provide any other details to the employer.

Regulations will only allow for correction of incorrect information or for providing information on how the offense was not disqualifying. If it is determined that the conviction was of a disqualifying offense, there is no further recourse for the applicant, unless the airport has an additional appeals process.

"Listen to the applicant carefully and make it clear that you personally are not judging them, but regulatory requirements prohibit you from approving them."

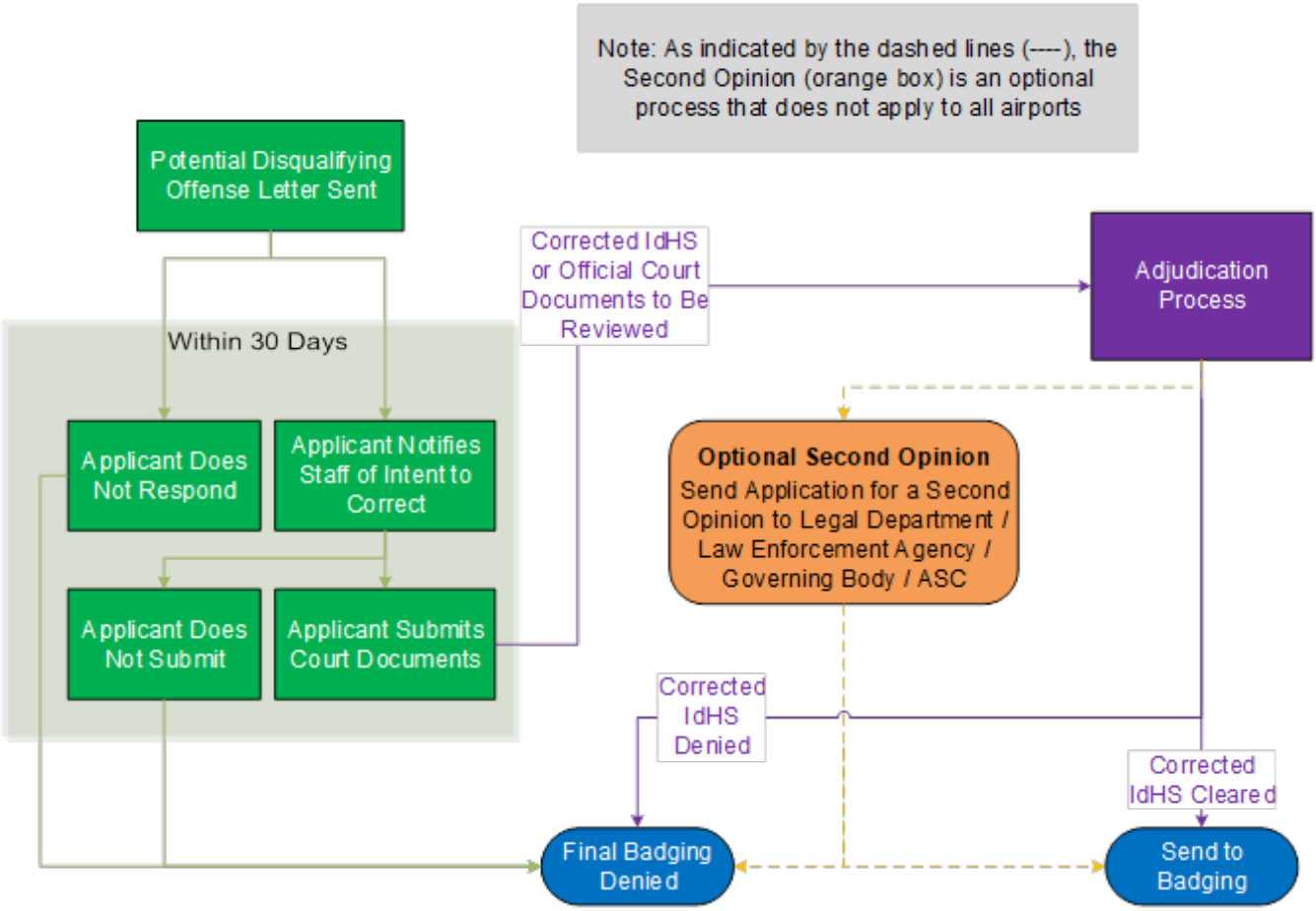
~Survey respondent

Airports are not federally mandated to provide an appeals process in addition to the corrective action process described above. If they choose to, it is up to each airport to define, develop, and publish the protocols for that process.

Airports with an appeals process typically use senior staff to review the adjudication decision. These airports indicated that the ASC, Chief of Police, or Aviation Security Director conducted the appeal and made the final decision. Occasionally, airports will use a governing body or their legal counsel to conduct the appeals process.

The flow chart presented in Figure 2 shows the baseline corrective action process that adjudication Trusted Agents are required to perform, as well as the appeals process (in orange) that some airports provide in addition to the baseline process.

Figure 2. Corrective Action and Appeals Process Flowchart



Step 8: Final Badging Decision

Based on the applicant's CHRC results and/or the corrected information—or lack thereof—submitted during the review process, the adjudication staff must notify the applicant that a final decision has been made to grant or deny an airport ID badge. If a badge is being revoked due to an RBN, the airport must notify the individual's Authorized Signatory of the revocation within 24 hours.

It is important to note that if a badge application is denied or a badge is revoked, the Trusted Agent must cancel the Rap Back subscription so that the airport does not receive RBNs that it is not authorized to receive.

Conducting periodic audits of the adjudication staff's work by a senior official, such as the ASC, confirms that the regulations are being applied correctly and consistently.

Creating an internal do-not-issue/do-not-escort list that is checked prior to issuing visitor credentials could prevent an individual denied an airport ID badge from receiving a visitor badge. However, the list should also include an expiration date for when the individual may be eligible for a badge.

Section 2 – Summary of Best Practices and Recommendations

- ✦ Adopt automated methods to transmit data to the DAC to reduce errors and delays
- ✦ Keep disposition case notes to eliminate repeated work during the badge renewal process
- ✦ Store records securely and with proper permissions to allow access by adjudicating staff only
- ✦ Have an experienced individual with prior knowledge reviewing criminal records examine conviction information
- ✦ Consult legal counsel or law enforcement for assistance with complicated records
- ✦ Require that applicants provide certified court copies of dispositions and corrected records
- ✦ Have two staff members present for adjudication interviews to maintain a safe environment
- ✦ Use two people to adjudicate each record, including at least one sworn LEO
- ✦ Conduct periodic audits of the adjudication staff's work
- ✦ Create an internal do-not-issue/do-not-escort list with expiration dates that is checked prior to issuing visitor credentials

SECTION 3: SUITABILITY & EXCEEDING REQUIREMENTS

Federal regulations provide a baseline of requirements; TSA does not prohibit airports from implementing additional measures in evaluating applicants for airport credentials. However, accessing and using criminal history or other information not related to the disqualifying offenses to make credentialing decisions may have legal implications involving discrimination or invasion of privacy rights.

Legal Implications

By adding criteria to the airport's published rules and regulations, the airport provides transparency to potential badge applicants, and provides additional information that can be used by the airport when deciding to deny badge requests or revoke badges at their airport.

Using any criteria beyond TSA's disqualifying criminal offenses to determine suitability to possess an airport ID badge needs to be well thought out and clearly documented.

Airports that are considering whether they want to add suitability disqualifiers to their adjudication process should consult with legal counsel. Defensibility of policy must be considered. Questions to determine defensibility include:

- For each offense or factor considered, what is the correlated risk to airport security and how is that risk predicted?
- What is the potential impact on protected classes, certain types of work, or a given badge population?
- Is the impact justified by the reduced risk to security?
- Are legal representatives willing to defend this policy in arbitration or court?

Airports should work closely with their legal departments when determining what information will be considered in making credentialing decisions.

To ensure consistent understanding and application, it is important to ensure all measures used in evaluating airport ID badge applicants are clearly stated in airport rules, regulations, and policies.

Applying measures that are not clearly documented in the rules, regulations, and policies could have legal implications.

BAN THE BOX

Nationwide, over 100 cities and counties have adopted what are widely known as Ban the Box statutes, calling for employers to consider a job candidate's qualifications first, without the stigma of a criminal record. The intent is to provide applicants a fair chance by removing the conviction history question on the job application and delaying the background check inquiry until later in the hiring process.

The introduction of additional crimes as a bar to unescorted access to airports—and therefore potential employment at those airports—may result in the introduction of statutes or ordinances to preclude such activity in those jurisdictions where Ban the Box has found traction. They might also result in requirements for additional review or waiver processes with respect to including additional crimes.

Ban the Box statutes would likely not apply to decisions regarding credentialing, but they indicate a sensitive legal environment when considering criminal convictions that automatically preclude employment.

STATE AND LOCAL CONSIDERATIONS

When adding to the airport's list of disqualifying crimes, there is also a need to consider state or local equal employment opportunity provisions. For example, in some locations, consideration of arrest data is prohibited by state law or local ordinance. Similarly, some states and localities have adopted statutes targeted at reducing the importance or consideration of convictions in employment-related decisions. Some states and localities have promoted polices to affirmatively employ ex-offenders as part of offender reintegration programs.

Additionally, local or tribal laws regarding disqualifying crimes that are considered during the adjudication process should be included in the airport rules, regulations, and policies to ensure consistent hiring practices. Information regarding tribal constitutions and other tribal legal matters can be found here: www.tribal-institute.org/lists/tribal_law.htm

Additional Disqualifiers and Suitability Factors

Approximately half of the more than 200 airports interviewed for this research exceed the federal regulations by adding to the list of 28 disqualifying crimes. Airports that have added supplemental disqualifiers indicated that often prompted by incidents at the airport or as a result of working closely with the airport authority and legal department.

"We are more interested in adjudicating for patterns, including misdemeanor patterns, since many are reduced felonies."

~Survey Respondent

Several airports have added a suitability clause to the list of federal disqualifiers that allows the airport police chief or ASC to determine if an applicant is unsuitable to protect the airport's security based on patterns of conduct or other circumstances. In extreme cases, this responsibility falls to the airport authority. Two important suitability considerations are:

1. Is there a criminal offense that results in a conviction?
2. Is there habitual conduct that has an outcome that has not been decided through due process?

Examples of suitability criteria include:

- Demonstrating inappropriate conduct in the badging process
- A conviction of theft, larceny, or violence on airport property
- Patterns of crime or petty crime on airport property
- Any crime committed at the airport that leads to an arrest
- Repeated violations of airport security policy
- Transporting a weapon through the security checkpoint or into the Secured Area
- Crimes involving minors
- A propensity to commit criminal acts (as evidenced by a history of multiple non-disqualifying offenses)

Many airports without the legal authority to alter the list of disqualifiers have opted to add a clause to the badge application that requires the applicant to list all crimes committed in the last 10 years. Lying, omitting, or misrepresenting criminal offenses on the application would result in the applicant being denied a badge.

An analysis of interview responses was conducted to identify common disqualifying factors that airports apply beyond the federal regulations. Table 1 shows a comparison matrix of these additional disqualifying offenses and potential suitability determinations that airports are currently using or would like to use beyond the regulatory requirements.

Table 1. Comparison Matrix of Additional Disqualifying Factors

Disqualifying Offenses & Potential Suitability Disqualifiers	Some Airports Currently Using as Indicated in Their Policies and Procedures	Some Airports Currently Using in Addition to Regulations	Some Airports Would Like to Use
Misdemeanor theft/larceny crimes	✓	✓	
Currently charged and awaiting judicial proceedings or outstanding warrants	✓	✓	
Longer look-back period		✓	
Felony manslaughter	✓	✓	
Registered arsonists	✓	✓	
Registered narcotic offenders	✓	✓	
Voyeurism		✓	
Lying or inappropriate conduct during the application process		✓	✓
Crimes committed in or involving the airport, including misdemeanors	✓	✓	✓
All felonies	✓	✓	✓
Multiple misdemeanors showing disregard for the law	✓	✓	✓
DWIs and DUIs		✓	✓
10-year look-back period starts from date of completion of sentence or probation/parole	✓	✓	✓
Juvenile offenses, especially of a violent nature		✓	✓
Registered sex offenders	✓	✓	✓
Conviction of a sex crime	✓	✓	
Crimes against persons, such as assault or harassment	✓	✓	
Serious crime within the last 20 years (theft, forgery, drugs, domestic violence)			✓
Pattern of behavior that shows intentional disregard for rules, procedures, and issues with authority	✓	✓	
Fraud involving weapons			✓
Crimes against law enforcement			✓

Research into other industries revealed a variety of suitability factors used in conjunction with CHRCs to vet potential employees, with vetting levels determined by the applicant's anticipated job role and responsibilities. Details of this research can be found in Appendix E.

Section 3 – Summary of Best Practices and Recommendations

- ✦ Ensure all measures used in evaluating airport ID badge applicants are clearly stated in airport rules, regulations, and policies

SECTION 4: SUMMARY OF BEST PRACTICES & RECOMMENDATIONS

The following recommendations and best practices are based on survey responses and interviews, as well as the author's research and experience with airport credentialing and adjudication. They may be applicable to all airport sizes and categories, but should be viewed through the lens of the airport's unique operating environment. Airports should seek legal counsel prior to implementing any measures that exceed federal requirements.

Provide periodic document recognition training for Trusted Agents and Authorized Signatories
Ensuring Trusted Agents and Authorized Signatories can differentiate between authentic and false documents decreases the risk of a badge being issued to an imposter or to an individual who is not authorized to work in the US.

Check for updates to the Form I-9 list regularly
The Form I-9 list is updated periodically, so it is a best practice that airport and air carrier staff members check the list at least every six months to ensure the current version is being used.

Adopt electronic methods (such as an IDMS) to transmit biographic data to the DAC
Accurate CHRC results are returned more quickly when there are no errors in the data transmitted via the DAC. Using an automated system to collect and transmit STA biographic information reduces errors. Many airports have upgraded to use Type 14 (slap) prints and have found that the newer technology has reduced the time taken to capture prints and produces fewer null prints. Creating a fillable PDF application form often reduces data input errors by Trusted Agents interpreting handwritten application entries and responses.

Store records securely and only allow adjudicating staff access to this information
The applicant's court documentation and record should be stored in a secure location and be accessible only to adjudicating staff. If using an IDMS, documents should be marked as secure and appropriate access permissions should be set.

Have an experienced individual with training and knowledge reviewing criminal records examine conviction information
Persons with law enforcement experience are generally considered to be more knowledgeable regarding penal codes than civilian staff, and many airports prefer to use their local law enforcement to adjudicate an IdHS or RBN when available.

Consult legal counsel or law enforcement to review the elements of past action, complicated records, or when there is possible expungement of a prohibited conviction
Persons in law enforcement or with legal counsel experience are generally considered to be more knowledgeable regarding penal codes than civilian staff, and make good resources for more complicated records.

Require the applicant to provide certified court copies of dispositions
Placing the burden on the applicant removes the burden from the airport credentialing office. If the documents are sent electronically, they should come directly from the court to ensure legitimacy of the documents, not from the applicant or the applicant's attorney.

Ensure corrected records have a certified court seal
This best practice provides assurance that the corrected records are legitimate and not manufactured or altered by the applicant.

Have two staff members present during interviews
Adjudication interviews can be emotional for applicants, and having two staff members in the interview helps to maintain an orderly environment. This best practice also provides a level of protection from accusations of impropriety.

Use two people – preferably including a sworn LEO – to adjudicate each record
This best practice provides a layer of quality control in the adjudication process. The subject can be complex, and having a second person review the adjudication decision has been found to be helpful, especially if at least one of the adjudicators is a sworn LEO.

Create an internal do-not-issue/do-not-escort list that is checked prior to issuing visitor credentials
If an applicant is denied an airport ID badge through the required vetting process, some airports add them to an internal do-not-issue list that is checked prior to issuing visitor credentials. Visitor credentials should not be issued to failed applicants, and TSA regulations do not allow them to be escorted.

Conduct periodic audits of the adjudication staff's work
Having the ASC or senior airport staff audit the work of the adjudication staff verifies that regulations and policies are being applied correctly and consistently.

Provide documentation training annually to the Authorized Signatory community
Becoming familiar with the wide variety of documents covered by the Form I-9 list takes time, and airports have found it beneficial to conduct annual training. Many of the documents are updated with enhanced security measures, so Authorized Signatories need to stay updated on the newer versions of accepted IDs and the security features they may include. Improving Authorized Signatories' knowledge of authentic and acceptable documents improves efficiency in the vetting process.

Check with your airport's legal counsel or media departments to see if the airport already subscribes to LexisNexis or Westlaw to save on subscription costs
Using these services, a researcher can access the relevant sections of a jurisdiction's criminal code in effect at the time a crime was committed—that is, the operative time for purpose of determining the elements of a crime upon which a conviction is based. See Appendix D for more information.

Ensure all measures used in evaluating applicants with respect to decisions about granting airport ID badges are clearly stated in airport rules, regulations, and policies
Some airports have added felony convictions of any type to the 28 mandated disqualifying crimes, and have also added arrest reporting requirements. Clearly stating all measures used in evaluating an applicant's background will help prevent possible legal action later.

Train Authorized Signatories to assist applicants with the application process, and to establish a routine review of the application before it is submitted to ensure all required information is included
Clearly indicating to Authorized Signatories what steps should be taken to both assist applicants in the process and to review applications prior to submission will help reduce occurrences of missing information. If the airport is using an IDMS, the badging application information may be entered by the Authorized Signatory via an online portal that will not allow submission of an incomplete application.

Keep notes on case disposition discoveries on RBNs to eliminate repeated investigations
Keeping notes on case disposition discoveries may help to eliminate repeated investigations during the badge renewal process. This is especially true of RBNs, which may not indicate what was changed on

the IdHS. The FPRD website has a comments section on each individual's record that could be utilized for this process. All comments should include dates for easy reference.

Establish a process for extending or cancelling each Rap Back subscription prior to its expiration date

Mandatory expiration dates are established during subscription to ensure validation takes place regularly, but the TSA recommends that airports and air carriers review each expiration notification, verify that the subscription is still valid, and extend it with a new expiration date.

Arrange for Trusted Agents to visit other airport credentialing offices or law enforcement entities that perform similar adjudication tasks

Arranging for Trusted Agents to visit other airport credentialing offices or law enforcement entities that perform similar adjudication tasks can prove invaluable in enhancing training, developing a local support network, and sharing best practices.

REFERENCES

"A Review of Access Control Measures at Our Nation's Airports." *Subcommittee on Transportation Security of the Committee on Homeland Security.* 3 February 2015. (Statement of G. Doug Perdue).

"A Review of Access Control Measures at Our Nation's Airports." *Subcommittee on Transportation Security of the Committee on Homeland Security.* 3 February 2015. (Statement of Sharon Pinkerton).

Airport Access Control Security Improvement Act of 2015, H.R. 3102, 114th Cong. (2015).

Airport Security Enhancement and Oversight Act of 2015, S. 2361, 114th Cong. (2015).

ANTN Digicast. (2015). Aviation Security Bill Introduced in Congress. Retrieved from http://www.antndigicast.com/index.cfm?fuseaction=DigiNews&news_id=250188

ASIS International. (2006). Pre-employment Background Screening Guideline.

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

Aviation News Today. (2015). Key Senate Leaders Introduce, Prepare to Consider Aviation Security Bill. Retrieved from http://www.aviationnews.net/?do=headline&news_ID=250499

Aviation Security Advisory Committee. (2015). Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control. Arlington, VA.

Aviation Security Improvement Act of 1990, Pub. L. 101-604, 104 Stat. 3066, codified as amended at 49 USC §101-215.

Babcock, Ernest. *Privacy Impact Assessment for the Next Generation Identification (NGI) Rap Back Service.* Federal Bureau of Investigation. 15 December 2016.

Black, A. (2010). *Managing the Aviation Insider Threat* (Postgraduate Thesis).

Blitsa, D., Jacobs, J. (2008) Sharing Criminal Records: The United States, the European Union and Interpol Compared. Retrieved from http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1631&context=ilr

Boden, Eric. "Employee Screening Takes on New Capabilities." January/February 2007. *Human Capital Magazine.*

Border Insecurity, Take Two: Fake IDs Foil the First Line of Defense: Hearing before the Senate Finance Committee regarding fraudulent documents. (2006) (Testimony of Michael P. Everitt).

Boyd, Aaron. "The Security Clearance Process is About to Get Its Biggest Overhaul in 50 Years." 28 February 2019. *Nextgov.*

Capital One. Criminal Background Inquiry Disclosures.

Center on National Security at Fordham Law. (2016). Case By Case: ISIS Prosecutions in the United States. Retrieved from https://static1.squarespace.com/static/55dc76f7e4b013c872183fea/t/577c5b43197aea832bd486c0/1467767622315/ISIS+Report+-+Case+by+Case+-+July2016.pdf

Counter, Peter. "The Big Deal with Biometric Background Checks." 15 September 2016. *Global Identity Management.*

Crepet, T. Jacobs, J. (2008). The Expanding Scope, Use, and Availability of Criminal Records. 11 New York University Journal of Legislation and Public Policy, Volume 177.

Customs and Border Protection. "CBP Fraudulent Document Workbook."

Department of Defense. (2015, September 11). *Background Checks on Individuals in DoD Child Care Services Programs* (DOD Instruction 1402.05). Washington, DC.

Dover, M.W., and Miller, E.G. (1998). *An Analysis of Federal Airport and Air Carrier Employee Access Control, Screening, and Training Regulations* (Postgraduate Thesis).

Employment History, Verification and Criminal History Records Check, 14 CFR §107-108 (1998).

FAA Extension, Safety, and Security Act of 2016, H.R. 636. 114th Cong. (2016).

Falsification of Security Records, 14 CFR §107-108 (1996).

Federal Bureau of Investigations. *Checks on Employees of Banks and Related Entities.* Retrieved from https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/checks-of-bank-employees/banknoticecontribtorltr

Fingerprint-based Criminal History Records Check (CHRC), 49 CFR §1542.209 (2010).

Fingerprint-based Criminal History Records Check (CHRC), 49 CFR §1544.229 (2011).

Fingerprint-based Criminal History Records Check (CHRC), 49 CFR §1544.230 (2011).

First Advantage. (2013). Employment Screening Best Practices.

General Dynamics/NASSCO. (2015). Terms and Conditions for Labor Providers. Retrieved from http://www.nassco.com/purchasing/terms-conditions/tc_labor.html#background

Government Accountability Office. (1995). *FAA Can Help Ensure That Airports' Access Control Systems Are Cost-Effective.* (GAO Publication No. 95-25). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2003). *Progress Since September 11, 2001, and the Challenges Ahead.* (GAO Publication No. 03-1150T). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2011). *Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload.* (GAO Publication No. 12-60). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2015). *TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed.* (GAO Publication No. 15-559T). Washington, DC: U.S. Government Printing Office.

Government Accountability Office. (2015). *TSA Has Taken Steps to Improve Vetting of Airport Workers.* (GAO Publication No. 15-704T). Washington, DC: U.S. Government Printing Office.

Heathrow Airport. (2013). ID Pass Application Standard 2013. http://www.heathrow.com/file_source/Company/Static/PDF/Partnersandsuppliers/idc-standard.pdf

Homeland Security Act of 2002, Pub. L. 107-296. 116 Stat. 2135.

International Civil Aviation Organization. (2011). *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. Quebec, Canada: ICAO.

International Civil Aviation Organization. (2014). *Aviation Security Manual, eighth edition*. Quebec, Canada: ICAO.

International Civil Aviation Organization. (2017). Annex 17: Safeguarding International Civil Aviation Against Acts of Unlawful Interference, tenth edition.

International Civil Aviation Organization. (2016). Annex 19: Safety Management, second edition.

JPMorgan Chase & Co. (2013). Contingent Worker Pre-Engagement Screening (PES) Process Guide.

JPMorgan Chase & Co. (2013). Instructions & Guidelines for Contractors Working on JPMorgan Chase Premises.

Kellett, Jeff, John Kane, and Rachel Tucker. "FBI Rap Back Focus Group Briefing."

Kofman, Ava. "The FBI is Building a National Watchlist that Gives Companies Real-Time Updates on Employees. 4 February 2017. *The Intercept.*

LaJoye, Darby. "Securing Our Skies: Oversight of Aviation Credentials." 3 February 2016. Transportation Security Administration.

Legal Services for prisoners with Children. Ban the Box Campaign. http://www.prisonerswithchildren.org/our-projects/allofus-or-none/ban-the-box-campaign/

Leidos. "Improving criminal identification."

Melber, A. (2015, November). Obama Bans the Box. http://www.msnbc.com/msnbc/obama-bans-the-box

Mills, Robert, Michael Grimalila, Gilbert Peterson, and Jonathan Butts. "A Scenario-Based Approach to Mitigating the Insider Threat." May 2011. *ISSA Journal*.

Nakashima, Ellen. (2016) "FBI Wants to Exempt its Huge Fingerprint and Photo Database from Privacy Protections." The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html

National Air Transportation Association. (2010). Security Directive for Airports.

National Association of Criminal Defense Lawyers, Inc. (2015). Chart #5 - Consideration of Criminal Record in Licensing and Employment.

National Association of Professional Background Screeners. (2013). The Facts about Background Checks.

National Association of State Directors of Teacher Education and Certification. "FBI NGI Rap Back Service Overview." 29 October 2014.

National Employment Law Project. (2007). A Worker's Guide to the Transportation Worker Identification Credential (TWIC) Application, Appeal, and Waiver Process. Oakland, CA.

Nixon, W. B. (2016, February). Why Reference Checking Matters. *SecurityMagazine.com*, 50-52.

O'Neal, S. (2007). Terrorist Precursor Crimes: Issues and Options for Congress. https://www.fas.org/sgp/crs/terror/RL34014.pdf

U.S Department of Transportation. Office of Inspector General. *Aviation Security, Federal Aviation Administration.* Report No. AV-1998-134. Washington, DC: GPO, 1998. https://www.oig.dot.gov/sites/default/files/av1998134.pdf

———. Office of Inspector General. *Aviation Security, Federal Aviation Administration.* Report No. AV-1999-068. Washington, DC: GPO, 1999. https://www.oig.dot.gov/sites/default/files/av1999068.pdf

———. Office of Inspector General. *Aviation Security, Federal Aviation Administration.* Report No. AV-2000-076. Washington, DC: GPO, 2000. https://www.oig.dot.gov/sites/default/files/av2000076.pdf

———. Office of Inspector General. *Controls Over Airport Identification Media, Federal Aviation Administration.* Report No. AV-2001-010. Washington, DC: GPO, 2001. https://www.oig.dot.gov/sites/default/files/av2001010.pdf

U.S. Department of Homeland Security. Office of Inspector General. *A Review of Background Checks for Federal Passenger and Baggage Screeners at Airports.* Report No. OIG-04-08. Washington, DC: DHS, 2004. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG-04-08_ReviewofScreenerBackgroundChecks.pdf

———. Office of Inspector General. *A Follow-up Review of the Transportation Security Officer Background Check Process.* Report No. OIG-07-67. Washington, DC: DHS, 2007. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-67_Aug07.pdf

———. Office of Inspector General. *Audit of Access to Airport Secured Areas (Unclassified Summary).* Report No. OIG-07-35). Washington, DC: DHS, 2007. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_07-35_Mar07.pdf

———. Office of Inspector General. *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening (Revised for Public Disclosure).* Report No. 09-05. Washington, DC: DHS, 2008. https://www.oig.dhs.gov/assets/Mgmt/OIGr_09-05_Oct08.pdf

———. Office of Inspector General. *TSA Can Improve Aviation Worker Vetting (Redacted).* Report No. OIG-15-98. Washington, D.C., 2015. https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-98_Jun15.pdf

———. Office of Inspector General. *The DHS Personnel Security Process*. Report No. 09-65. Washington, DC: DHS, 2009. https://www.oig.dhs.gov/assets/Mgmt/OIG_09-65_May09.pdf

U.S. Office of Management and Budget. Suitability and Security Processes Review: Report to the President. Washington, DC: White House Office, 2014.

U.S. Office of Personnel Management. (2002). *General Questions and Answers About OPM Background Investigations*. http://archive.opm.gov/products_and_services/investigations/faqs.asp

———. (2008). *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*. https://www.opm.gov/suitability/suitability-executive-agent/policy/final-credentialing-standards.pdf

———. (2008). *Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide*. https://www.opm.gov/suitability/suitability-executive-agent/policy/decision-making-guide.pdf

Phalen, Charles. "Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) Rap Back Service Available for Continuous Evaluation (CE)." Federal Investigations Notice No. 19-02. 31 October 2018.

Pfizer. Criminal Background Check Policy.

President's Commission on Aviation Security and Terrorism. (1990). *Report of the President's Commission on Aviation Security and Terrorism*. Washington, DC: U.S. Government Printing Office.

Project People. (2009). Employment Screening Best Practice in the Telecommunications Sector.

Public Law 92-544 of 1972, Pub. L. 92-544, 85 Stat.

Sandia National Laboratories. U.S. DOE Security Clearances. Retrieved from http://www.sandia.gov/fso/clearances.htm

SIDA Badge Expiration Period. *American Association of Airport Executives Member Hub*. [Forum]. 16 October 2019.

Simio, T., Trinidade, R. (2014, December). The Well Vetted Workforce. *ASIS International.* Retrieved from https://sm.asisonline.org/Pages/the-well-vetted-workforce.aspx

Spear, Carol, et al. *PARAS 0001: Criminal History Records Checks (CHRCs) and Vetting Aviation Workers Guidebook*. May 2017. National Safe Skies Alliance, Inc.

States with FCRA Criminal Reporting Provisions. http://www.starpointtenantscreening.com/states-with-FCRA-Criminal-Reporting-Provisions.html

Texas Department of Public Safety. *Criminal Justice Rap Back User Guide*. March 2018.

Transportation Security Administration. "Disqualifying Offenses and Other Factors." https://www.tsa.gov/disqualifying-offenses-factors.

Transportation Security Administration. (2009). Legal Guidance on Criminal History Records Checks. Washington, DC: U.S. Government Printing Office.

Transportation Security Administration. (2004). Legal Guidance on Criminal History Records Checks. Washington, DC: U.S. Government Printing Office.

Transportation Security Administration. (2022). *Rap Back Overview and Privacy Informational Briefing for Airports and Aircraft Operators.* [PowerPoint].

Transportation Security Administration. *Rap Back User Guide for Airports and Air Carriers v 3.3.* 24 March 2023.

Transportation Security Administration. *SIDA Airport Security: Fiscal Year 2017 Report to Congress*. 6 February 2018.

Transportation Security Administration. (2015). *TSA Updates on ASAC Recommendations.* https://www.tsa.gov/news/releases/2015/07/14/tsa-update-asac-recommendations

United States, Congress. Public Law 114-190. 130 STAT. 615. 15 July 2016.

United States Department of Agriculture. (2010). *Emergency Preparedness Division (EPD) Personnel Security Transition*. (Notice AO-1477). Washington, DC: USDA.

United States Department of Justice, Criminal Justice Information Services Division. *Summary Reporting System (SRS) User Manual*, June 20, 2013.

United States Department of Justice, Federal Bureau of Investigation. *Uniform Crime Reporting Handbook*, 2004.

United States Department of Justice, Law Enforcement Information Technical Standards Council (LEITSC). *Standard Functional Specifications for Law Enforcement Records Management Systems (RMS),* 2009.

United States Department of Justice, Office of the Attorney General. *The Attorney General's Report on Criminal History Background Checks*, June 2006. Washington, DC: U.S. Government Printing Office.

United States Government Accountability Office. (2016) "GUN CONTROL: Analyzing Available Data Could Help Improve Background Checks Involving Domestic Violence Records." *Report to the Acting Ranking Member, Subcommittee on Commerce, Justice, Science, and Related Agencies, Committee on Appropriations, House of Representatives.* Retrieved from http://www.gao.gov/assets/680/678204.pdf

United States Government Accountability Office. *TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016.* GAO-17-662. September 2017.

United States House of Representatives, Committee on Homeland Security. *TSA Integrity Challenges: Examining Misconduct by Airport Security Personnel*, Hearing. July 31, 2013 (Serial No. 113-29). Washington, DC: U.S. Government Printing Office.

United States Postal Service. (1999). *Administrative Support Manual, Issue 13*. Washington, DC: USPS.

United States Postal Service. (2015). Handbook AS-805 – Information Security.

United States Postal Service. (2015). Handbook EL-312 – Employment and Placement.

Vice President's Task Force. (1986). *Public Report of the Vice President's Task Force on Combatting Terrorism*. Washington, DC: U.S. Government Printing Office.

Wells Fargo. (2012). Wells Fargo Background Checks and Fingerprint Screenings: Compliance with Section 19 of Federal Deposit Insurance Act.

White House Commission on Aviation Safety and Security. (1997). *Final Report to President Clinton.* Washington, DC: U.S. Government Printing Office.

Worsham, R. What Kind of Background Checks Does UPS Do? Retrieved from http://www.ehow.com/list_7609254_kind-background-checks-ups-do.html

GLOSSARY

Adjudication	According to the TSA Personnel Security Manual, adjudication is "…an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk." The adjudication process is used to determine a person's risk to security and public trust. While there are 28 crimes that are considered immediate disqualifiers if indicated on an applicant's IdHS, the TSA recommends airports and air carriers also use suitability determinations to understand an applicant's risk to the aviation community.
Appeals	An appeals process is a formal means for applicants to challenge adjudication decisions. Not all airports offer an appeals process. It is up to each airport to define their appeals process, since there are no federal requirements for airports to provide an appeals process.
Applicant	An individual who is applying for an airport ID badge or access privilege.
Covered Individual	An individual for whom the airport operator has accepted an air carrier CHRC certification.
Criminal History Records Check (CHRC)	A search for an individual's criminal history by submitting a covered individual's fingerprints and biographic information to FBI's Next Generation Identification (NGI) system and reviewing any criminal history records the NGI returns.
Designated Aviation Channeler (DAC)	The National Crime Prevention and Privacy Compact created a rule to authorize outsourcing of the CHRI process to private third parties known as Channelers. The Channeler facilitates the submission and management of biometric and biographic information for the STA and CHRC. TSA requires airports and air carriers seeking CHRCs for applicants to use one of the Channelers that holds an agreement with the agency.
Identity History Summary (IdHS)	The report of all identification, demographic, and event information (criminal or civil) within an FBI identity record disseminated to an authorized entity. The FBI uses this term interchangeably with the term 'rap sheet'.
Identity Management System (IDMS)	IDMS is an integration of systems, processes, procedures, applications, database management systems, and interfaces that work together to perform various credentialing functions. IDMS solutions and options vary widely between providers, but usually support: • Management and secure storage of biographic and biometric and information • Management of information related to the issuance and maintenance of airport ID Badges, including audits • Management of background check investigation documents • Limiting the issuance or continued use of an airport ID badge if work authorization is not current • Limiting the issuance or continued use of an airport ID badge if the required security checks are not completed • Limiting the issuance or continued use of an airport ID badge if the required training is not completed
Manual Name Check	The procedures by which an airport operator submits a request to the FBI to conduct a name-based CHRC after the FBI has determined a covered individual's fingerprints are unusable or unclassifiable due to low image quality.
Next Generation Identification (NGI) System	Replacement for the FBI's Integrated Automated Fingerprint Identification System that provides new functionality and improves upon existing capabilities, in particular for criminal history records search functions.
Rap Back	A program that uses the FBI NGI to enable airport operators to receive ongoing notifications of criminal history information for covered individuals who have submitted fingerprints as part of a CHRC.

Rap Back Activity Notification	If during the Rap Back subscription term an arrest (or other event that is included in the list of triggering events) is reported in NGI and matches the fingerprints in the Rap Back subscription, an Unsolicited Rap Back Activity Notification will be sent to the airport.
Rap Back Maintenance	The Rap Back Maintenance transaction is used to perform several types of maintenance actions related to a Rap Back subscription. There are four types of maintenance transactions: replace or append biographic data, change expiration date, cancel subscription, and un-cancel subscription. Rap Back Maintenance Un-Cancel Transaction Response (RMBNTR) reports any criminal activity that may have occurred between when the subscription was cancelled and when it was un-cancelled. Rap Back Maintenance Replace Transaction Response (RBMNTR) reports any criminal activity that may have occurred between when the subscription expired and when it was re-activated with a new expiration date.
Rap Back Overview Privacy Information Briefing	A guide that provides a general understanding of TSA's implementation of the FBI Rap Back service, and includes descriptions of Rap Back transactions, the subscription management process, and the roles and responsibilities of participating airport and aircraft operators.
Rap Back User Guide (RBUG)	A technical document developed by TSA to provide guidance to personnel responsible for aviation worker suitability determination, badging, and/or CHRC adjudication.
Reviewing	In the context of this guidebook, reviewing refers to the process of examining the applicant's CHRC results prior to final adjudication.
Search and Subscribe Transaction	A Search and Subscribe transaction completes the fingerprint submission for a CHRC and also sets a field in the transaction record that alerts the FBI to retain the fingerprints in their NGI civil repository and to set a new Rap Back subscription.
Security Threat Assessment (STA)	A check of relevant databases, conducted by TSA, to confirm: (1) that an individual does not pose a security threat, (2) that an individual possesses lawful status in the United States, and (3) an individual's identity.
Social Media	Social media encompasses applications that allow for the creation and exchange of user-generated content and allows for communication among individuals, businesses, organizations, and communities. As of the publication of this guidebook, the most common platforms used include Twitter, Facebook, LinkedIn, YouTube, and Instagram, although the popularity of each platform changes over time.
Subsequent Rap Back Subscription Transaction	A Subsequent Rap Back Subscription (RBSR) transaction can be initiated for an individual who has previously completed a CHRC and been issued ID media, but was not subscribed into Rap Back. New criminal activity could have occurred in the interim and would be reported with the RBSR.
Suitability	According to the OPM, suitability is the "…identifiable character traits and conduct sufficient to decide whether an applicant is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness." Suitability adjudication is an evaluation of the fitness—the character and trustworthiness—of the applicant for the position; the process considers an applicant's personal conduct throughout their careers. The assessment is intended to establish a reasonable expectation that the applicant will protect the integrity or promote the efficiency of the agency.
Triggering Event	Refers to a fingerprint match event within the FBI NGI system that meets certain criteria that may be pertinent to a suitability determination, and results in the FBI sending a Rap Back Activity Notification to the Subscriber.
Trusted Agent	An airport operator employee or agent who collects information from applicants and current airport ID media holders for use in the CHRC and STA, transmits the information to a DAC, authorizes the issuance of ID media, or issues the ID media.

APPENDIX A: ADDITIONAL BADGE APPLICATION FORM STATEMENTS

The statements below were reported by airports as additions to the standard language.

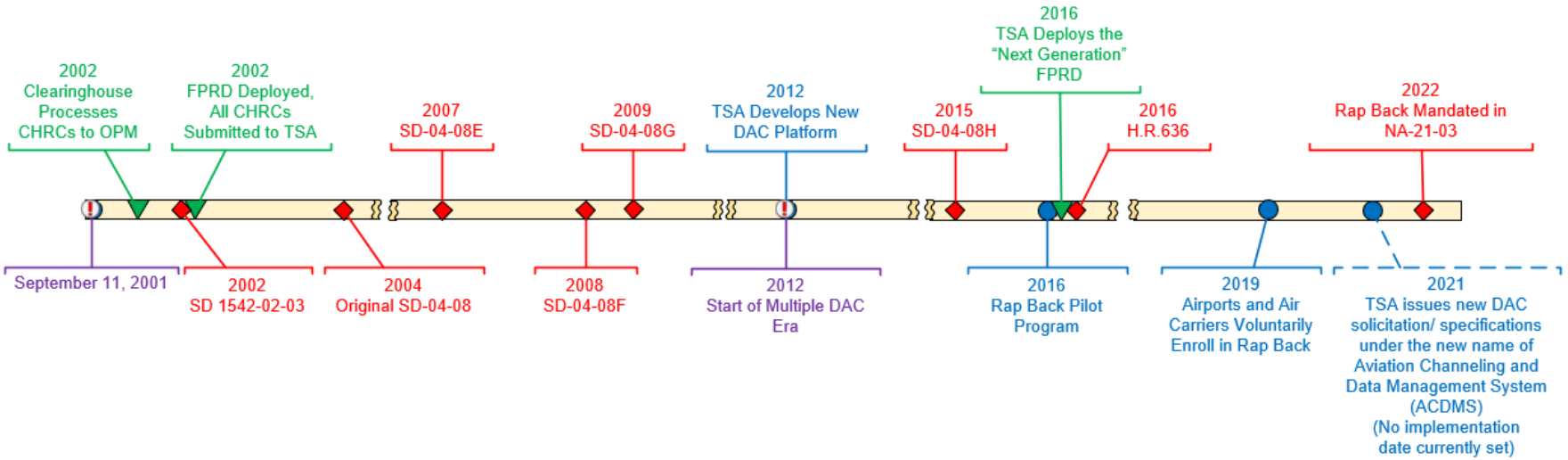
- I will not divulge or reveal to anyone not associated with, and authorized by, the airport any information concerning security, security systems, or security procedures used at the airport.
- An airport ID badge is a privilege.
- The Airport has the authority and makes the final determination whether to grant, deny, or revoke a badge at any time it feels that an individual may jeopardize the Airport Security Program.
- The Airport Manager reserves the right to conduct a further investigation on an individual at the cost of the employer. Fraudulent claims are punishable to the full extent of the law.
- My security identification badge is issued to support my job duties and responsibilities at the airport and should only be used for official business purposes. I will never utilize my security identification badge when off-duty or for personal use.
- The Airport Security Coordinator or designee may deny issuance of an ID badge based on an applicant's conviction for a non-disqualifying offense if the offense occurred on Airport property and the offense interfered with or threatened the property, safety, comfort, efficiency or security of passengers, employees, tenants or Airport operations. Maximum period of denial under this provision shall be (1) for a misdemeanor conviction, 1 year from the conviction date; (2) for a gross misdemeanor conviction, 3 years from conviction date.
- Persons with a conviction of a Disqualifying Crime shall be ineligible to apply for an ID badge for at least 12 months from the date of release from imprisonment for a Disqualifying Crime.
- Any person applying for an ID badge who is charged with a Disqualifying Crime and awaiting a final judicial disposition will be denied issuance of an ID badge until a final judicial disposition is made. If you have any outstanding warrants, your badge will not be issued until the warrant is handled (within 30 days).
- The airport, or its designated representatives may release any or all of the above information and/or records, or any other records or information it may have about me, to any law enforcement or other governmental agency which the airport, in its sole discretion, believes has a need to know. I hereby release and discharge the airport, its employees, agents, clients, and customers from any and all liability, claim, damage, or cause of action which may arise directly from or out of their compliance with the requests and authorizations herein.
- I acknowledge that I work in a position of trust and that if I misuse my badging privileges to circumvent any security system, measure or procedure including smuggling of contraband or dangerous devices, I will be subject to civil and criminal sanctions, including revocation of my badge and access privileges.
- I understand that any false or misleading information on this application may be cause for this application to be disapproved or for any permit or ID badge issued as a result to be revoked. I specifically authorize the airport, or its designated representatives, to investigate me and my background and my activities in any lawful manner and to any extent that the airport, in its sole discretion, deems from time to time advisable. This may include, but is not limited to, contact with former employers, contact with my present employer, my co-workers, additional criminal history checks, including but not limited to non-fingerprint-based state and local records and litigation checks. I understand that the reason for these investigations is for security purposes and

that had I not consented to and authorized the same, I would not be granted an ID badge and the privileges associated therewith, nor would my application for the same be processed and/or considered and the processing and/or consideration of my application for an airport ID badge is bargained for consideration, the receipt and sufficiency of which is hereby acknowledged.

APPENDIX B: HISTORY OF DESIGNATED AVIATION CHANNELERS (DAC)

Prior to 2002, airports experienced difficulties sending biometric information and receiving the resulting IdHS. This was due in part to the Office of Personnel Management (OPM-aviation channeler) and FBI being overwhelmed with the background check requests for new airport worker applications. In 2002, the first DAC was created through a non-compete agreement with FAA, the aviation security regulator at the time. In 2011, TSA opened up the DAC process to public bid opportunity, and additional organizations became TSA-certified DACs. A timeline of the relevant regulations concerning the DAC is presented in Figure B-1.

Figure B-1. History of DAC Timeline



APPENDIX C: ADJUDICATION TRAINING

Many new adjudication staff members are shown how to complete their tasks but are not told why they need to complete a specific task in a particular way. As a result, they may in good faith change a process, and by doing so later discover they are not in regulatory compliance.

Many new adjudicators are fearful of making a mistake in the adjudication process as they lack confidence in their knowledge of the regulations or understanding of the information in an IdHS. TSA regulations and SDs are subject to updates and contain extensive information that often requires clarification, so it is important for adjudicating staff to fully understand the requirements and ensure that they are applying the regulations correctly.

Research shows that there are no specific CHRC adjudication training classes available to airport and air carrier staff. However, airports and air carriers do have access to a range of formal training options that provide valuable context and knowledge to support the adjudication process. Many options are available through industry associations or federal agencies, including:

- TSA Rap Back Overview and Privacy Informational Briefing
- Trusted Agent training
- ASC training
- Handling of SSI/PII
- Fraudulent Documentation and Imposter Recognition

Informal or on-the-job training is also an important resource available to new staff, as it often offers practical insight into the role of the adjudicator by adding a better understanding of the local environment. Airports might consider exposing adjudicating staff to discussions with their local law enforcement agencies and legal counsel to better understand state penal codes, common criminal records codes, and how to read court documentation.

Arranging for staff to visit other airport credentialing offices or law enforcement entities that perform similar adjudication tasks can prove invaluable in enhancing training, developing a local support network, and sharing best practices.

On-the-job training curricula for new adjudicators need to be documented and tailored to local airport or air carrier circumstances. Adjudication training should be provided by experienced adjudication staff or by the ASC.

A suggested training checklist for adjudicating staff is included below and can be modified as needed.

In addition to training adjudicating staff, training Authorized Signatories is also important. One airport surveyed provides documentation training annually to the Authorized Signatory community to help them maintain their vigilance and competency in document validation. This program was well received and has the added benefit of improving communication between the credentialing office and the Authorized Signatories.

Training Checklist

- ☐ CHRC progression
- ☐ Rap Back Process
- ☐ Submittal/retrieval process
  - TSA-approved DAC
  - FPRD
- ☐ Regulatory summary
  - Airport obligations/limitations
  - Air carrier obligations/limitations-certification
  - Rap Back Overview and Privacy Informational Briefing for Airports and Aircraft Operators
- ☐ TSA's Rap Back User Guide
- ☐ FPRD IdHS review
  - No record
  - Record
    - IdHS – how to read
    - Various codes that are standard
    - What to investigate further
    - Adjudication process for specific airport
  - Unclassifiable; MNC process
- ☐ CHRC Process
  - Trusted Agent confirms authority to retrieve CHRC
  - Trusted Agent retrieves CHRC results
  - "No record" entered into badging system
    - Notification to Authorized Signatories of cleared employees
  - IdHS with activity
    - Review, no disqualifying process?
    - Review, potential disqualifying process?
- ☐ How to obtain additional information to adjudicate?
  - Internal follow-up
  - Provide applicant with the opportunity to supply official court documentation
    - How to further verify returned information
      - LEO
      - Court
- ☐ How is IdHS record marked when approved or denied?
  - Stamped
  - Other

- ☐ Approvals
  - Who makes final approval on a record adjudication and how?
  - Enter into badging system
  - Is a denial escalated beyond adjudicator?
    - Security Director
    - Attorney, LEO, or other
- ☐ Appeals process, when applicable
- ☐ Rap Back Subscription process
- ☐ Rap Back Activity Notifications (RBN)
- ☐ RBN adjudication and appeal process
- ☐ Properly secure adjudicated records, limiting access to Trusted Agents with a need to know

APPENDIX D: ADJUDICATION RESOURCES AND STATE PENAL CODES

Since adjudication of a crime frequently requires a comparison of state and federal criminal statutes, finding the applicable provisions of state law is essential to the process. When reviewing conviction information, the examiner should analyze the law in place at the time the offense was committed.

There are several resources available to assist airports and air carriers in understanding and interpreting disposition codes. For example, Larry Henry and Derek Hinton wrote *The Criminal Records Manual: 3rd Edition: Criminal Records in America: A Complete Guide to Legal, Ethical, and Public Policy Issues and Restrictions* in September 2008. The book provides a useful appendix with definitions of disposition codes. The US Courts website also has a glossary of legal terms, which can be used during the adjudication process: www.uscourts.gov/glossary.

Most legal professionals will research statutes by utilizing proprietary search tools like:

LexisNexis www.lexisnexis.com/en-us/products/lexis-advance.page
Westlaw legalsolutions.thomsonreuters.com/law-products/westlaw-legal-research/

These subscription-based web tools operated by private services are the most effective and accurate way to search code sections. The services often offer training in how to conduct the kinds of searches that would be necessary to compare a state criminal statute to a federal one.

Using these services, a researcher can access the relevant sections of a jurisdiction's criminal code in effect at the time a crime was committed—that is, the operative time for the purpose of determining the elements of a crime upon which a conviction is based. Use of these systems by trained personnel (preferably by lawyers, paralegals, law enforcement personnel, or others trained in statutory interpretation) is the optimal way to accurately assess a conviction for comparison to the relevant federal statute for a disqualifying crime. Check with your airport's legal counsel or media department to see if the airport already subscribes to LexisNexis or Westlaw to save on subscription costs.

While subscription services like those outlined above are the best way to find the relevant legal standards, there are some publicly accessible collections of state criminal codes. Table D-1 below is a guide to public collections of criminal statutes maintained by state governments. The relevant statute/code provisions regarding criminal law are noted and a hyperlink to code sections is provided.

These collections are most often maintained by a state's legislative body. In some states, the court system maintains these compilations. Some of the collections are maintained by contract providers, like LexisNexis, at the direction of a state government.

In some states, the sites are deemed the official citation for laws, and in others the website notes that they are not the official citation. These free public sites may also be limited in providing information about changes to the statute over time. While the statutes are accurate in outlining the current state of the law, they are frequently less informative about the elements of a crime at the time of convictions. While most provisions of the criminal law do not fluctuate radically, there may be changes over time that would affect comparability to federal laws.

The table below is a useful resource for checking penal codes from other states. Since they can change frequently, specific examples of each penal code are not included in this guidebook. Airports and air carriers may want to consider having a resource developed specifically for their region that covers the areas most commonly found on an IdHS. If a resource document is developed, it must be regularly updated.

Table D-1. State Penal Code Websites

State	Code Selection	URL
AL	Alabama Criminal Code	https://tinyurl.com/ALcriminalcode
AK	Alaska Statutes Title 11	https://tinyurl.com/AKTitle
AZ	Arizona Criminal Code, Title 13	https://tinyurl.com/AZ-Title13
AR	Arkansas Criminal Code, Title 5	https://tinyurl.com/ARTitle5
CA	Penal Code of California	https://tinyurl.com/CA-Penal
CO	Colorado Criminal Code, Title 18	https://tinyurl.com/CO-Title18
CT	Connecticut Penal Code (Section 952)	https://tinyurl.com/CTSection952
DE	Delaware Code, Title 11	https://tinyurl.com/DETitle11
DC	Code of the District of Columbia, Title 22	https://tinyurl.com/DCTitle22
FL	Florida Statutes, Title XLVI	https://tinyurl.com/FLTitleXLVI
GA	Code of Georgia, Title 16	https://tinyurl.com/GATitle16
HI	Hawaii Penal Code (Title 37)	https://tinyurl.com/HITitle37
ID	Idaho Statutes, Title 18	https://tinyurl.com/IdahoTitle
IL	Illinois Criminal Code of 2012	https://tinyurl.com/IL-CriminalCode
IN	Indiana Code, Title 35	https://tinyurl.com/INTitle35
IA	Iowa Code, Title XVI	https://tinyurl.com/IATitleXVI
KS	Kansas Statutes, Chapter 21	https://tinyurl.com/KSChapter21
KY	Kentucky Revised Statutes, Title XL	https://tinyurl.com/KY-TitleXL
LA	Louisiana Revised Statute, Title 14	https://tinyurl.com/LATitle14
ME	Maine Revised Statutes, Title 17	https://tinyurl.com/METitle17
MD	Code of Maryland, Criminal Laws	https://tinyurl.com/MDStatutes
MA	Commonwealth of Massachusetts General Laws, Part IV	https://tinyurl.com/MAPartIV
MI	Michigan Penal Code	https://tinyurl.com/MIpenalcode
MN	Minnesota Statutes, Chapter 609	https://tinyurl.com/MNChapter609
MS	The Mississippi Code of 1972, Title 97	https://tinyurl.com/MSStatutes
MO	Missouri Revised Statutes, Title XXXVIII	https://tinyurl.com/MOStatutes
MT	Montana Code Annotated 2015, Title 45	https://tinyurl.com/MTTitle45
NE	Nebraska Criminal Code (Chapter 28)	https://tinyurl.com/NEChapter28
NV	Nevada Revised Statutes, Title 15	https://tinyurl.com/NVTitle15
NH	New Hampshire Statutes, Title LXII	https://tinyurl.com/NHTitleLXII
NJ	The New Jersey Code of Criminal Justice (Title 2C)	https://tinyurl.com/NJCriminalLaw
NM	2015 New Mexico Statutes, Chapter 30	https://tinyurl.com/NMChapter30
NY	New York State Law (Penal Law)	https://tinyurl.com/NYpenal
NC	North Carolina General Statutes, Chapter 14	https://tinyurl.com/NCChapter14
ND	North Dakota Century Coe, Title 12.1	https://tinyurl.com/NDTitle12-1

State	Code Selection	URL
OH	Ohio Revised Code, Title XXIX	https://tinyurl.com/OHTitleXXIX
OK	The Penal Code of Oklahoma (Title 21)	https://tinyurl.com/OKTitle21
OR	Oregon Revised Statutes, Title 16	https://tinyurl.com/ORStatutes
PA	Pennsylvania Consolidated Statutes, Title 18	https://tinyurl.com/PATitle18
RI	State of Rhode Island General, Title 11	https://tinyurl.com/RITitle11
SC	South Carolina Code of Laws, Title 16	https://tinyurl.com/SCStatutes
SD	South Dakota Codified Laws, Title 22	https://tinyurl.com/SDStatutes
TN	Tennessee Code, Title 39	https://tinyurl.com/TNTitle39
TX	Texas Statutes, Penal Code	https://tinyurl.com/TXpenalcode
UT	Utah Criminal Code (Title 79)	https://tinyurl.com/UTTitle79
VT	Vermont Statutes, Title 13	https://tinyurl.com/VTTitle13
VA	Virginia Crime Codes	https://tinyurl.com/VAStatutes
WA	Washington Criminal Code (Title 9A)	https://tinyurl.com/WATitle9A
WV	West Virginia Code Chapter 61	https://tinyurl.com/WVChapter61
WI	Wisconsin Statutes Chapters 939-951	https://tinyurl.com/WIChapters
WY	Wyoming Statutes, Title 6	https://tinyurl.com/WYTitle6

ICAO

The International Civil Aviation Organization (ICAO) adopts Standards and Recommended Practices (SARP) concerning the prevention of acts of unlawful interference to civil aviation. The formulation and adoption of SARPs for international aviation is incorporated into 19 technical annexes. ICAO's measures to prevent and suppress all acts of unlawful interference against international aviation are designated in Annex 17, which states, in part, that:

> 3.4.1 Each Contracting State shall ensure that the persons implementing security controls are subject to background checks and selection procedures.
>
> 4.2.4 Each Contracting State shall ensure that background checks are conducted on persons other than passengers granted unescorted access to security restricted areas of the airport prior to granting access to security restricted areas.

The two Standards discussed above are mandatory requirements for each Contracting State (country) that is a signatory to ICAO. Along with SARPs, ICAO also issues guidance material on how to implement their requirements. That guidance appears in ICAO Aviation Security Manual, DOC 8973, which is a restricted document.

APPENDIX E: GOVERNMENT AND OUTSIDE ENTITIES

GOVERNMENT

The government sector employs a wide variety of tactics to determine the suitability of employees for hire.

One of the distinct differences in vetting employees for the public sector or government versus the private sector is the fact that government employees are part of a system of public trust. These positions are often enforcement or regulatory in nature and have a great deal of latitude when determining outcomes of programs, funding, rulemaking, and enforcement. Another difference is that government often hires for careers, meaning that they expect to have these employees until they are eligible to retire—careers of 20 plus years are not unusual.

Positions involving the enforcement of laws, courts, and specific regulatory enforcement employ the following considerations in their vetting process:

- Psychological screening
- Character suitability, involving the following ten established factors of conduct:
    - Intoxicant use and frequency
    - Illegal drug use
    - Financial irresponsibility
    - Criminal and antisocial conduct
    - Dishonesty (including by act of omission)
    - Disruptive or violent behavior
    - Employment misconduct and negligence
    - Firearms and weapons violations
    - Statutory debarment
    - Miscellaneous agency-specific requirements

The value of psychological screening and character suitability extends to positions of great trust, high responsibility, critical decision making, safety, and the enforcement of laws and rules.

It is worth noting that OPM takes a much broader view of suitability than just convictions. OPM conducts the majority of the background checks for the private sector when a government contract requires a clearance level that includes a fingerprint-based CHRC. The difference with OPM checks is that they take a number of factors into account when determining an applicant's suitability. These additional factors include how recent the conduct was, the severity of the offense, rehabilitation, and frequency of criminal conduct. Aviation checks, on the other hand, are by regulation simply either "yes" or "no" based on a conviction for one of the enumerated crimes within the look-back period.

If an airport or air carrier decides to include suitability requirements to supplement the TSA CHRC requirements, the additional considerations below could be helpful in determining whether an individual should be granted access to Secured Areas of the airport. The challenge is that this kind of review takes significantly more skilled vetting resources than the current system.

OPM and the private entities interviewed (e.g., banks and pharmacies) use suitability and pattern behavior factors in addition to the CHRC. Examples of suitability factors include:

- Misconduct or negligence in employment
- Criminal or dishonest conduct
- Material, intentional false statement, or deception or fraud in examination or appointment
- Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant, appointee, or others
- Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation
- Knowing and willful engagement in acts or activities designed to overthrow the US Government by force
- Any statutory or regulatory bar that prevents the lawful employment of the person involved in the position in question

OPM and agencies must consider any of the following additional considerations to the extent OPM or the relevant agency, in its sole discretion, deems any of them pertinent to the individual case:

- Nature of the position for which the person is applying or in which the person is employed
- Nature and seriousness of the conduct
- Circumstances surrounding the conduct
- Time of the conduct
- Age of the person involved at the time of the conduct
- Contributing societal conditions
- Absence or presence of rehabilitation or efforts toward rehabilitation

Airports could consider strengthening the vetting procedures based on the type of airport ID badge the applicant is applying for, regardless of whether the applicant has a record. This approach would assist in reducing potential risks from badge holders working in Secured Areas, and is specifically mentioned in federal regulations as an option for airport operators.

OTHER INDUSTRIES

Eight other industry case studies were conducted. Several of the organizations interviewed requested that their organization not be publicly identified to prevent potential applicants from having in-depth knowledge of their vetting policies. The industries reviewed included law enforcement agencies, the medical industry, and the transportation industry.

When using suitability determination factors in approving a background check, non-aviation entities tend to base the suitability determination factors on the type of position and level of trust. In addition, the look-back period is based on position requirements. If an applicant was convicted of a felony on the disqualifying crimes list but the look-back period has passed, suitability is still determined based on position type and trust level and may be denied.

Law enforcement entities that were interviewed follow suitability determination measures as discussed above, and include others, for example:

- Verification of date and place of birth
- Verification of education

- Verification of employment for last 10 years or since 18th birthday
- Interviews of five references
- Traffic/criminal record checks of police departments, state's attorneys, sheriff's offices, and circuit clerks where the applicant has lived, worked, or attended school
- Verification of military discharge status
- Computer checks of immediate family
- Credit checks
- Verification of place of residence for last 10 years
- Verification of professional licenses
- Personal interview
- Interview of spouse (not mandatory)
- Review of Department of Corrections inmate log
- Review social networking sites

The process for conducting background investigations in other industries spans a wide spectrum. Individual sectors and trade organizations such as ASIS International, which is a global community of security practitioners, have made recommendations on standards or best practices.

The following are best practices employed across industries such as pharmaceuticals, banking/securities, telecommunications, and media, as well as private companies in any industry. Most of these best practices are involved in pre-employment screening, rather than the vetting that is done once a person is hired and applies for a security badge. The most significant factors to consider are the time, personnel, and costs associated with implementing these measures.

Fingerprint-Based CHRC
Fingerprint-based CHRCs verify felonies and misdemeanors at the federal, state, and local levels. The value of a fingerprint-based CHRC is that it is a relatively easy process, and provides an objective analysis of a person's past actions. This can be measured against clear standards and, if applied uniformly, offers a consistent measure between individuals.

Some of the challenges with this practice are the specific training needed to adjudicate records and the ability to reconcile charges between various jurisdictions. Individual states and territories often have different levels or classifications of crimes, different penalties for these crimes, and report these crimes differently to databases. Therefore, determining whether an arrest led to an eventual conviction can often be confusing. To magnify the confusion, many charges can be plea-bargained, reduced, deferred, dismissed, or enhanced based upon a variety of factors.

Credit Checks
A credit check includes the amount of debt an applicant holds and is often considered a pre-employment screening tool. The value of this process focuses on decision making; having a large burden of debt generally limits an individual's choices and may make them vulnerable to poor decision making or compromise in the future.

Employment Verification
Verification of work history is best suited to pre-employment screening, but generally shows consistency in how people conduct their lives. The verification has a high value and demonstrates the stability of a person's life and decision-making abilities. Employment verification is best suited to determine patterns of behavior and may establish the authenticity of an applicant. Some challenges using

this as a tool include factoring external forces beyond the control of applicants, such as injury, illness, personal circumstances, or economic conditions. Additionally, age, geographic location, and education are factors that influence employment history.

Education Verification
Verification of transcripts and grades is a relatively simple process. It has value in establishing a consistent pattern of behavior and confirms the veracity of an applicant. While simple, it is potentially a time-consuming process and may not have an obvious connection to many positions or types of work. This is also an area that is more suited to pre-employment screening.

Travel Abroad
When considering someone's past travel abroad, take into account their travel destinations, reasons for travel, and frequency of travel. This has limited value for most types of employment but may be considered as a pre-employment screening tool for some positions.

Drug Testing
Pre-employment and ongoing/random testing may be a valuable screening tool, and may be related to criminal conduct, safety, and credibility. This process is expensive and can be fraught with legal exposure and challenges.

Social Media
Using social media to support the evaluation of an applicant's suitability for an airport ID badge was not mentioned by any of the airports or air carriers that were interviewed.

Review of social media forums must be evaluated carefully due to legal restrictions. This is probably the most controversial and least developed tool of pre-employment screening in security-sensitive industries. It is a developing and evolving area, and the technologies are outpacing how this can or should be used when evaluating candidates and measuring risk. This is also dependent on the age of a person, what media platforms they utilize, what they use each for, how often each is used, and the boundaries of free speech.

Some industries complete social media checks as part of their employment vetting procedures, conducting a basic internet search for any information about the candidate—without requesting username or password, which is prohibited in several states. The challenge in reviewing social media is how do you know that the "John Smith" you have found is the same "John Smith" applying for employment or an airport ID badge? Also, how are you able to verify that the information posted is accurate?

Airports and air carriers are looking for ways to protect against potential insider threats. While checking news media or social media may seem like a promising tool, there are many questions concerning how this could be applied. It would be important to apply the same criteria to all applicants, and essential to consult with legal counsel before implementing any social media checks.

REGULATIONS COMPARED

Table E-1 shows a comparison matrix of disqualifying crimes and potential suitability disqualifiers as defined by the TSA, CBP, OPM, United States Postal Service (USPS), Transportation Worker Identity Credential (TWIC), international agencies, and non-aviation industries. This information was gathered from literature review and case studies performed by the authors.

Interviews with other industries were used to help gather real-world perspectives, procedures, and methods currently used or under consideration. The case studies targeted other industries where

innovation has been applied or where valuable lessons were learned. These industries included a public transit agency, law enforcement agencies, private sector organizations serving the federal government, a state government agency, the medical industry, public organizations, and OPM. Disqualifying crimes and suitability disqualifiers are included in the comparison matrix below.

Table E-1. Comparison of Various Agency, Organization, and Industry Disqualifiers

Disqualifying Offenses & Potential Suitability Disqualifiers	TSA* 49 CFR 1542.209 & 1544.229	CBP* 19 CFR 122.183	OPM† 5 CFR 731.202	USPS†	TWIC*	International*	Other*† Industries
Forgery of certificates, false marking of aircraft, and other aircraft registration violation	✓	✓					
Interference with air navigation	✓	✓				✓	
Improper transportation of a hazardous material	✓	✓			✓		
Aircraft piracy	✓	✓					
Interference with flight crew members or flight attendants	✓	✓			✓		
Commission of certain crimes aboard aircraft in flight	✓	✓					
Carrying a weapon or explosive aboard an aircraft	✓	✓					
Conveying false information and threats	✓	✓			✓	✓	
Aircraft piracy outside the special aircraft jurisdiction of the United States	✓	✓					
Lighting violations involving transporting controlled substances	✓	✓					
Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements	✓	✓					
Destruction of an aircraft or aircraft facility	✓	✓					
Murder	✓	✓			✓	✓	✓
Assault with intent to murder	✓	✓			✓	✓	✓
Espionage	✓	✓			✓	✓	
Sedition	✓	✓	✓	✓	✓	✓	
Kidnapping or hostage taking	✓	✓			✓	✓	✓
Treason	✓	✓			✓	✓	✓
Rape or aggravated sexual abuse	✓	✓			✓	✓	
Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon	✓	✓			✓	✓	✓
Extortion	✓	✓			✓	✓	
Armed robbery	✓	✓			✓	✓	✓

Disqualifying Offenses & Potential Suitability Disqualifiers	TSA* 49 CFR 1542.209 & 1544.229	CBP* 19 CFR 122.183	OPM† 5 CFR 731.202	USPS†	TWIC*	International*	Other*† Industries
Distribution of, or intent to distribute, a controlled substance	✓	✓			✓	✓	✓
Felony arson	✓	✓			✓	✓	✓
Felony involving:							
Willful destruction of property	✓	✓				✓	✓
Importation or manufacture of a controlled substance	✓	✓			✓	✓	✓
Burglary	✓	✓				✓	✓
Theft	✓	✓		✓		✓	✓
Dishonesty, fraud, or misrepresentation	✓	✓	✓		✓	✓	✓
Possession or distribution of stolen property	✓	✓				✓	✓
Aggravated assault	✓	✓				✓	✓
Bribery	✓	✓			✓	✓	✓
Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year	✓	✓			✓	✓	✓
Violence at international airports		✓					
Felony involving a threat		✓					✓
Embezzlement		✓		✓			✓
Perjury		✓				✓	✓
Robbery		✓			✓	✓	✓
Crimes associated with terrorist activities		✓			✓	✓	✓
Sabotage		✓					
Assault with a deadly weapon		✓		✓	✓	✓	✓
Illegal use or possession of firearms or explosives		✓			✓	✓	✓
Any violation of an immigration law		✓			✓	✓	
Any violation of customs law or any other law administered or enforced by customs involving narcotics or controlled substances, commercial fraud, currency or financial transactions, smuggling, failure to report, or failure to declare		✓			✓		
Airport security violations		✓					
Discharged or disciplined at prior employment for dishonesty, incompetence, insubordination, absenteeism, tardiness, or failure to follow regulations‡			✓	✓			✓

Disqualifying Offenses & Potential Suitability Disqualifiers	TSA* 49 CFR 1542.209 & 1544.229	CBP* 19 CFR 122.183	OPM† 5 CFR 731.202	USPS†	TWIC*	International*	Other*† Industries
Alcohol abuse, without evidence of substantial rehabilitation‡			✓	✓			
Criminal or dishonest conduct‡			✓	✓	✓		
Refusal to furnish testimony‡			✓	✓			
Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question‡			✓				
Known or suspected involvement in activities of serious violence against persons or property‡						✓	✓
May be prone or induced to commit or assist in an act that may unlawfully interfere with civil aviation‡						✓	
Known or suspected to be or has been a member or participant in activities of criminal organizations‡					✓	✓	✓
Perverting the course of justice‡						✓	✓
Crimes against law enforcement (assaulting an officer, assaulting a police officer)						✓	✓
Cruelty to a child or child endangerment						✓	✓
Used drugs while employed in any law enforcement or prosecutorial position that carries with it a high level of responsibility, or while employed in a position involving public trust‡							✓
Misrepresentation of history of drug use‡							✓
Used any illegal drug, other than marijuana, within the last 10 years, or has engaged in more than minimal experimentation at any point‡				✓			✓
Used marijuana within the last 3 years or has used marijuana frequently over a substantial period of time at any point‡				✓			✓
Conduct indicating dishonesty‡							
Theft				✓			✓
Forgery							✓
False impersonation					✓		✓
Identity theft					✓		✓
Bribery							✓
Computer crimes							✓
Fraud				✓	✓		✓

Disqualifying Offenses & Potential Suitability Disqualifiers	TSA* 49 CFR 1542.209 & 1544.229	CBP* 19 CFR 122.183	OPM† 5 CFR 731.202	USPS†	TWIC*	International*	Other*† Industries
Money laundering							✓
Deceptive practices				✓	✓		✓
Disorderly conduct or mob action‡				✓			✓
Driving record‡							
A single incident involving reckless driving or driving under the influence of alcohol or mood-altering substances within the last 5 years				✓			✓
More than one DUI or reckless driving incident, regardless of the date				✓			✓
Any incident that resulted in the suspension or revocation of a driver's license on two or more occasions				✓			✓
Dishonorable Discharge or Bad Conduct Discharge from the US Armed Forces, National Guard, or State Militia							✓
Indebtedness, defaulted on any loan, or has inconsistent payment pattern‡							✓
Solicitation							✓
Conspiracy							✓
Discrimination‡							✓
Illegal gambling‡							✓
Fraudulent entry into a seaport					✓		
Violation of the Racketeer Influenced and Corrupt Organizations (RICO) Act or comparable state law					✓		
Robbery					✓		
Smuggling					✓		
Conspiracy or attempt to commit any of the aforementioned criminal acts	✓	✓	✓	✓	✓	✓	✓

* *Information gathered from literature review*
† *Information gathered from case studies*
‡ *Potential suitability disqualifiers in other industries*

Items marked with a (‡) in Table E-1 are used as potential suitability disqualifiers in some other industries, including USPS. These potential suitability disqualifiers are adjudications of character and conduct that may impact the integrity or efficiency of the organization or agency.