OFFICE OF INSPECTOR GENERAL

TWIC Background Checks are Not as Reliable as They Could Be

Homeland Security

September 1, 2016

OIG-16-128

DHS OIG Highlights

TWIC Background Checks are Not as Reliable as They Could Be

September 1, 2016

Why We Did This Audit

As of October 2015, the Transportation Security Administration (TSA) issued more than 3.5 million biometric credentials to individuals needing unescorted access to secure areas of the Nation's maritime facilities and vessels.

We conducted this audit to determine whether TSA's background check processes ensure only eligible individuals receive credentials and remain in the program.

What We Recommend

We made five recommendations to address TSA's oversight of the TWIC program.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

TSA's leadership, responsible for issuing Transportation Worker Identification Credentials (TWIC), does not provide sufficient oversight and guidance to ensure that the TWIC program operates effectively. Specifically, within the background check process, which TSA calls the security threat assessment:

- Fraud detection techniques are not monitored and used in completing the background check;
- Adjudicators may grant TWICs even if questionable circumstances exist;
- Key quality assurance and internal control procedures are missing from the background check and terrorism vetting processes; and
- New efforts tested for continuous vetting for disqualifying criminal or immigration offenses lack measures to determine the best solution.

These issues exist, in part, because TSA leadership relies on the TWIC program office to implement necessary improvements; however, the TWIC program office focuses more on customer service than effectiveness of the program. Additionally, because of TSA's organizational structure, the TWIC program office lacks visibility into and authority over the other offices within TSA that support the TWIC program. As a result, there is a risk that someone with major criminal or immigration offenses maintains access to secured areas of maritime facilities.

Agency Comments

TSA concurred with the recommendations and has already begun implementing corrective actions.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SEP 1 2016

MEMORANDUM FOR: Thomas L. Bush
Assistant Administrator
Transportation Security Administration

FROM: for Mark Bell
Assistant Inspector General for Audits

SUBJECT: *TWIC Background Checks are Not as Reliable as They Could Be*

Attached for your action is our final report, *TWIC Background Checks are Not as Reliable as They Could Be.* We incorporated the formal comments provided by your office.

The report contains 5 recommendations aimed at improving the Transportation Security Administration's (TSA) oversight of the Transportation Worker Identification Credential program. Your office concurred with all 5 recommendations. Based on information provided in your response to the draft report, we consider recommendations 1, 2, 4, and 5 open and resolved. Recommendation 3 remains open and unresolved until you provide evidence to support how TSA's existing metrics are sufficient to address the intent of the recommendation. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act,* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Donald Bumgardner, Deputy Assistant Inspector General for Audits, at (202) 254-4100.

Attachment

Table of Contents

Background 1

Results of Audit 5

TSA Leadership Does Not Provide Sufficient Oversight 5
Ineffective Fraud Detection Techniques 6
Inadequate Guidance 7
Missing Internal and Quality Controls 9
Insufficient Planning for Recurrent Vetting 10

Conclusion 10

Recommendations 10

Appendixes

Appendix A: Objective, Scope, and Methodology 14
Appendix B: TSA Comments to the Draft Report 16
Appendix C: TWIC Disqualifying Offenses 23
Appendix D: Excerpt of TSA's Organization Chart 26
Appendix E: Statistical Sample Results 27
Appendix F: Recurrent Vetting Options 29
Appendix G: Office of Audits Major Contributors to This Report 30
Appendix H: Report Distribution 31

Abbreviations

FBI	Federal Bureau of Investigations
GAO	Government Accountability Office
IDENT	Automated Biometric Identification System
MTSA	*Maritime Transportation Security Act of 2002*
OIA	Office of Intelligence and Analysis
OIG	Office of Inspector General
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services

Background

The *Maritime Transportation Security Act of 2002*[1] (MTSA) requires that all individuals who need unescorted access to MTSA regulated facilities obtain a biometric identification credential.[2] The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) established the Transportation Worker Identification Credential (TWIC) and jointly manage the TWIC program. TSA oversees the eligibility and the background check process, and issues the card. USCG enforces the use of TWICs and other MTSA requirements at the ports, as pictured in figure 1.

Figure 1. MTSA Facility

Source: United States Coast Guard (USCG)

TWIC is integral to the safety of the ports and other maritime facilities. Both private and public facility owners rely on TSA to conduct thorough background checks, which TSA refers to as security threat assessments, on individuals seeking jobs that require unaccompanied access to restricted areas. Having a TWIC alone (a sample of which is shown in figure 2) does not grant access to restricted areas. The person must also have a verified need to be in the area, which the respective facility authorizes.

Figure 2. Sample TWIC

Source: USCG

[1] Pub. L. No. 107-295

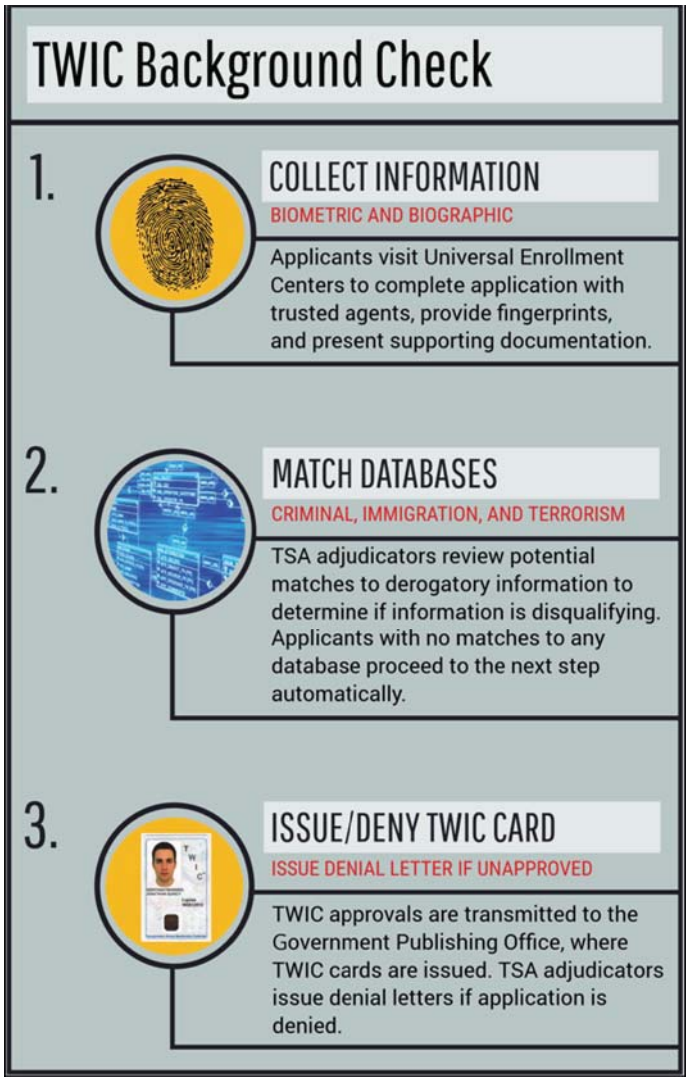
[2] TSA embeds the Transportation Worker Identification Credential with an encrypted file containing a cardholder's name, photo, two fingerprints, and the expiration date of the credential.

As of October 2015, TSA had issued more than 3.5 million TWICs, including both initial cards and renewals, of which approximately 2.1 million unique cards were active. As of February 1, 2015, it costs applicants $128 to apply for a 5-year TWIC. The TWIC population consists primarily of dockworkers, truckers, port employees, and U.S. merchant mariners.

TWIC Background Check Process

TSA is responsible for reviewing TWIC applications within 30 days of receipt. Figure 3 provides an overview of the steps TSA takes to complete the background check process.

Figure 3. TWIC Background Check



Source: Office of Inspector General (OIG) analysis of the Transportation Security Administration (TSA) data.

Step 1.
Applicant goes to a TSA contracted Universal Enrollment Center to complete an application disclosure form, provide required documents, provide a set of fingerprints, sit for a digital photograph, and pay a fee. Trusted Agents, who work for the center, assist applicants and confirm that the documents provided match the identity of the individual, are certified, and valid.

Step 2.
TSA uses the applicants' biographic and biometric information, housed in TSA's Technology Infrastructure Modernization system, to correlate against four databases to check for criminal, immigration, and terrorism-related offenses that could preclude the applicant from obtaining a TWIC.

Under TWIC regulations at 49 Code of Federal Regulations (CFR) 1572.5(a), TSA determines that an applicant poses a security threat and may deny a TWIC if —

(1) The applicant has a disqualifying criminal offense described in 49 CFR 1572.103. Per the regulations, there are 12 permanently disqualifying and 15 interim disqualifying offenses. Appendix C provides the list of disqualifying offenses TSA uses.
(2) The applicant does not meet the immigration status requirements described in 49 CFR 1572.105.
(3) TSA conducts the analyses described in 49 CFR 1572.107 and determines that the applicant poses a security threat.
(4) The applicant has been adjudicated as lacking mental capacity or committed to a mental health facility, as described in 49 CFR 1572.109.

Permanent disqualifying offenses include espionage, treason, murder, and a Federal crime of terrorism. *Interim disqualifying offenses* include extortion, immigration violations, unlawful possession, use, or sale of a firearm or other weapon.

Source: TSA

To perform the background check and complete its analyses, TSA compares the applicant's information against four main systems. These systems include:

- Federal Bureau of Investigation's (FBI) Next Generation Identification System that provides criminal history information;
- U.S. Citizenship and Immigration Services' Systematic Alien Verification for Entitlements to verify lawful immigration status;
- TSA's Transportation Vetting System, which matches an applicant's information against select terrorist watch lists, U.S. Marshals Wants and Warrants, and Office of Foreign Asset Control persons of interest; and
- Office of Biometric Identity Management's Automated Biometric Identification (IDENT) system for a biometric and fingerprint-based check against derogatory information provided by DHS, the Department of State, the Department of Justice, and the Department of Defense.

Approximately 40 percent of all applications trigger no matches against any of the data systems screened. For those applications, the TSA automated information system electronically adjudicates and approves the file. Electronic adjudications take approximately 1 to 39 days to reach a decision. The remaining 60 percent of the applications may match one or more databases and require a manual review. Adjudicators in the Security Threat Assessment Operations Adjudication Center conduct the manual adjudication. They are Federal employees trained to review each piece of information available and determine whether to grant or deny a TWIC. They also process waivers and

appeals. Manual adjudications typically apply to cases that are more complex. Based on our review of 235 manually adjudicated cases, adjudicators may take up to 140 days to reach a decision.

Step 3.
Once applicant eligibility is approved, TSA's automated information system sends a signal to the Government Publishing Office to issue the TWIC. When adjudicators determine that the applicant is not eligible to receive a TWIC, they issue a denial letter. Applicants may request a waiver or appeal of the TSA decision.

TWIC Funding

The revenue generated by the enrollees funds the program for approximately 5 years. Congress does not appropriate funds to operate the TWIC program. Instead, TSA carries over any unused portion of the TWIC fees it collects each year to the next fiscal year. Between FYs 2012 and 2015, TSA collected approximately $221 million in fees.

Prior Audits

In May 2011 and May 2013, the Government Accountability Office (GAO) published two audit reports[3] on the TWIC program. In 2011, GAO identified internal control weaknesses with TSA's background check process and found that TSA did not have program controls for ensuring that TWIC holders maintained their eligibility. In 2013, GAO identified issues with the electronic card reader pilot intended to test enforcement of TWICs at ports through biometric card readers. Among its recommendations, GAO recommended the Secretary of DHS strengthen the TWIC program's controls for preventing and detecting fraud. GAO also recommended that TSA define the term "extensive criminal history" for use in the adjudication process and identify mechanisms for detecting whether TWIC holders continue to meet TWIC eligibility requirements. As of April 2016, all five of GAO's recommendations remained open[4] and MTSA facilities were not required to use card readers for TWIC cards[5].

[3] *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives* (GAO-11-657) and *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Need to Be Reassessed* (GAO-13-198)
[4] After the issuance of the draft report, GAO closed two of its five recommendations. One recommendation was closed as not implemented, and the other because of Congressional action. The three remaining open recommendations pertain to DHS's oversight of the TWIC program and the need for internal control reviews of the various parts of the process from application to use at secure facilities.
[5] The TWIC reader requirements final rule (81 FR 57652) was published on August 23, 2016, and will be effective August 23, 2018.

Results of Audit

TSA's Office of Intelligence and Analysis (OIA) has not provided sufficient oversight and guidance to ensure that changes to the TWIC program improve its effectiveness or correct internal control weaknesses. Specifically, ineffective fraud detection techniques, inadequate guidance, missing quality controls, and insufficient planning for recurrent vetting reduce the reliability of TSA's background check process. OIA leadership relies on the TWIC Maritime Program Management Office to manage the program, but its focus is more on customer service than effectiveness of the program. Additionally, because of TSA's organizational structure the program office lacks visibility into and authority over the other offices that support the TWIC program. As a result, there is a risk that someone with major criminal or immigration offenses maintains access to secured areas of maritime facilities.

TSA Leadership Does Not Provide Sufficient Oversight

OIA leadership has not provided sufficient oversight and guidance over the TWIC Program. Instead, OIA relies on the TWIC program office and various other offices to manage segments of the TWIC credentialing process, but does not ensure that each office's procedures adequately identify and mitigate potential risks. For example:

The TWIC program office responsible for performance, schedule, cost, oversight, and guidance has not established metrics to measure TSA's success in achieving TWIC program core objectives. The program office's metrics focus mostly on customer service, including metrics for average enrollment wait time, enrollment time, enrollment help desk resolution time, and enrollment help desk response time. These metrics do not align with TWIC's core objectives for effectiveness of the program and instead create competing priorities that increase the risk that TSA may issue TWIC credentials to someone who is not qualified.

TWIC Program Core Objectives

- Positively verify the identity of those seeking access to secure areas.
- Conduct a Security Threat Assessment to determine the eligibility of those individuals seeking access.
- Deny access to unauthorized individuals.
- Revoke access to individuals immediately upon their loss of eligibility.

Source: TSA

Furthermore, because of TSA's organizational structure, the TWIC program office does not have oversight or authority over the TWIC vetting offices and is

unaware they are missing critical quality controls.[6] The Adjudication Center is responsible for completing the manual background checks and processing waivers and appeals. It is located within the Office of Law Enforcement/Federal Air Marshal Service, not OIA. The Colorado Springs Operations Center, which performs terrorism vetting using TSA's Transportation Vetting System, is located within the OIA directorate but does not report to the TWIC Maritime Program Management office. Appendix D illustrates the complexities of TSA's management structure as it relates to the TWIC program.

Ineffective Fraud Detection Techniques

TSA poorly executed its fraud prevention techniques — including electronic and visual document validation — when verifying applicants' identities at TWIC enrollment centers. In 2011, GAO recommended[7] that TSA strengthen TWIC program controls for preventing identity fraud. TWIC management officials implemented electronic document validation using a digital scanner and required Trusted Agents to conduct a visual review and make notes on the validity of documents presented. However, TSA did not monitor or use these fraud detection techniques when completing the background checks.

Electronic Document Validation

TSA implemented the use of a digital scanner for electronic document validation without first defining how the agency would interpret and use scores generated by the scanner. As required by TSA's statement of work, Trusted Agents began using a digital scanner in 2012 to help identify fraudulent documents. The digital scanner is a device that can evaluate visible and non-visible security features on a document to determine if the document is fraudulent while also scanning and uploading the document to TSA's information system. The digital scanner generates a score based on the scanner's analysis of the document's authenticity. However, TSA never defined benchmarks for these scores or determined how it would interpret and use the scores the digital scanner generated. Consequently, since its inception in 2012, TSA has not used the full capability of the scanner, missing potential fraud detection opportunities the scanner could provide.

[6] As of June 12, 2016, TSA moved its Security Threat Assessment Operations Division, including the Adjudication Center, to the Office of Intelligence and Analysis. The realignment occurred after the OIG had completed its fieldwork and the OIG did not test the effectiveness of the changes.
[7] *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives* (GAO-11-657)

Manual Document Review

In addition to using the digital scanner, Trusted Agents have a responsibility to ensure the validity of documents presented during enrollment. We identified the following issues with the Trusted Agent's manual review process.

Fraudulent Document Detection Training
TSA requires Trusted Agents to visually inspect the documents provided and make notes in the enrollment record if the agent believes fraud or other inconsistencies exist. However, TSA has not provided Trusted Agents with training to detect fraudulent documents. Instead, Trusted Agents rely on their own knowledge to decide what information to annotate. Additionally, TSA did not provide standardized note selections to facilitate documenting and subsequent review of issues identified.

TSA Did Not Review Trusted Agent Notes
TSA does not have a process in place to review, rank, or analyze the information provided in the notes. A review of all notes documented revealed that Trusted Agents recorded 527,956 notes between March 2014 and December 2015. Trusted Agent notes included statements such as "SSC feels to be fraudulent" and "His social security card is a fraud it is typed on the front and pieced together on the back from another SS card." TSA adjudicators never reviewed or considered these notes when reviewing background information and deciding whether to issue a TWIC.

Because of our inquiries, TSA recognized the need for improvements in this area and requested that Trusted Agents take fraudulent document detection training. According to TSA, 82.5 percent of the staff completed the interactive web-based training as of December 2015.[8] TSA also worked on a change request with the enrollment center contractor to standardize the notes field, and the contractor began implementing standardized comments in April 2016.

Inadequate Guidance

Lack of guidance may have allowed adjudicators to grant TWICs even if questionable circumstances exist. TSA has not provided guidance to adjudicators on how to use certain regulations, how to consider violations of TSA policy, or how to best use the IDENT information. Additionally, TWIC's primary guidance is disorganized and difficult to use.

[8] After completing our fieldwork, TSA provided additional information that as of July 2016, approximately 98 percent of staff had completed the interactive web-based training.

TWIC senior management has not provided adjudicators necessary guidance on the following issues:

- *Applying 49 CFR 1572.107* — As of February 2016, adjudicators have not used this regulation when reviewing extensive criminal background histories because TSA has not developed guidance on when and how the criteria can be applied. This regulation provides that when reviewing background information and deciding to issue a TWIC, TSA may determine an applicant poses a security threat if research reveals extensive criminal convictions or convictions for serious crimes not listed as permanent or interim disqualifying offenses. Appendix C provides information on all disqualifying offenses.

- *Violations of TSA policy* — A TWIC cardholder did not face consequences when they disregarded TSA policy for self-reporting disqualifying offenses. TWIC regulations at 49 CFR 1572.19(d)(1), require cardholders to self-report to TSA and surrender their TWIC when charged with a disqualifying offense. However, according to TSA officials, this has only occurred once since the program began in 2007. We identified one instance in our sample where a TWIC cardholder did not face consequences for failing to self-report a disqualifying offense. TSA approved the cardholder's TWIC renewal application even though the individual had not reported a charge for aggravated assault with a weapon — a disqualifying event. TSA adjudicators said they approved the TWIC renewal because the charge had not resulted in a conviction. Although we understand that at the time of the renewal the applicant was technically qualified, the lack of regard for TSA policy should warrant a closer look.

- *Use of IDENT information to adjudicate TWIC applications* — Although TSA compares applicants information to the IDENT system, we found that TSA adjudicators do not use the IDENT match results when reviewing TWIC cases because they do not understand its content or significance. IDENT is a valuable tool when completing background checks because it not only provides biometric and fingerprint-based information on potentially disqualifying criminal offenses, but also immigration offenses. IDENT provides adjudicators access to information reported by DHS, and the Departments of State, Justice, Defense.

Additionally, TWIC's primary guidance is a disorganized collection of emails and memorandums without a table of contents or index. Adjudicators told us this guidance is a primary reference tool for TWIC eligibility criteria. However, to find specific information, they must perform time-consuming keyword searches. One new adjudicator said it is difficult to use the guidance to

adjudicate cases based on its format. During the audit, adjudication center managers began revising the guidance and provided us with sections of a draft manual, including a fully indexed table of contents and a table of updates, but TSA has not finalized it.

Missing Internal and Quality Controls

OIA leadership has not ensured key internal and quality controls are included in the TWIC adjudication process, as well as those processes used to check for ties to terrorism. Specifically, controls for proper separation of duties and consistent procedures to review adjudication decisions and analysts' terrorism vetting decisions are missing. Internal and quality assurance controls prevent manipulation of information and ensure that programs are operating as intended. Without these controls, the background check process is at risk of unintentional errors and insider threats.

The Adjudication Center does not have processes in place to ensure the proper separation of duties — an element of strong internal controls. Under the current process, any adjudicator can assign him- or herself a case, adjudicate it, review the adjudication, and perform the quality assurance check. Additionally, when managers perform quality reviews, they have no consistent oversight plan. There is no specified criteria for what cases to review, how many, or a requirement that cases be reviewed at all. At times, heavy workloads can influence a manager's availability to perform quality reviews, and in those instances, no quality checks may occur.

Similarly, we identified missing controls in the Colorado Springs Operations Center terrorism vetting process to prevent a positive match from going undetected. The terrorism vetting operation uses an automated scoring system to grade matches between an applicant's biographical information and terrorism vetting information. An analyst independently reviews the scores to determine if there is a match. The higher the score, the more likely the applicant's biographic information matches the information in TSA's terrorism vetting system. When the analyst confirms a match, a supervisor reviews the analyst's report to verify the match. However, if an analyst concludes there is not a match, there is no review of the analyst's decision. Therefore, if an analyst accidentally or intentionally fails to identify a terrorist threat, TSA does not have controls in place to catch the error. TSA needs to implement a system flag to alert supervisors when an analyst clears a high scoring match requiring a supervisor to conduct a secondary review and protect against missed positive matches.

Insufficient Planning for Recurrent Vetting

Insufficient planning impedes TSA's ability to implement available recurrent vetting options successfully and efficiently. TSA is testing two methods to implement recurrent vetting into its credentialing programs but it does not have plans to evaluate the two efforts. The Aviation Worker Program is testing the use of the FBI's Rap Back program to check for criminal violations,[9] and the TWIC program is planning to begin use of DHS' IDENT system to check for both criminal and immigration violations. Appendix F provides additional details on both systems.

Although TSA's planning documents discuss the potential for expanding each system's use for TWIC and other TSA vetting programs, these plans do not include a method TSA will use to determine the best approach. Without clear measurable and comparable objectives, TSA is unlikely to have the best information to make accurate decisions.

Conclusion

Vulnerabilities in the TWIC background check process inhibit TSA from providing assurance that individuals with unescorted access to secure maritime facilities have not committed disqualifying criminal or immigration offenses and continue to be eligible. Given the complexity of the TWIC program's management structure, OIA leadership should provide greater guidance and oversight to ensure thorough risk analyses of TWIC processes and to verify improvements to the TWIC program effectively correct identified weaknesses.

Recommendations

Recommendation 1: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration identify a cross-functional coordinating entity with authority, responsibility, and accountability to provide regular guidance and leadership across all Security Threat Assessment processes and supporting offices.

Recommendation 2: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration conduct a comprehensive risk analysis of the Security Threat Assessment processes to identify areas needing additional internal controls and quality assurance

[9] OIG Report, *TSA Can Improve Aviation Worker Vetting* (OIG-15-98) identified the need for recurrent vetting within the Aviation Worker Program.

procedures; and develop and implement those procedures, including periodic reviews to evaluate their effectiveness.

Recommendation 3: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration improve Transportation Worker Identification Credential program-level performance metrics to ensure they align with the program's core objectives, and direct management officials to use these metrics for all the supporting offices.

Recommendation 4: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration review current Transportation Worker Identification Credential Security Threat Assessment guidance to ensure it provides adjudicators the necessary information and authority to complete Security Threat Assessments.

Recommendation 5: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration establish measurable and comparable criteria to use in evaluating and selecting the best criminal and immigration recurrent vetting option.

TSA Comments

TSA concurred with all five recommendations and has already begun implementing corrective actions. We have included a copy of management's comments in their entirety in Appendix B. TSA also provided technical comments to our report. We incorporated these technical comments in our draft report, as appropriate.

OIG Analysis of TSA Comments

Recommendation 1: Concur. TSA OIA and Office of Law Enforcement / Federal Air Marshal Service leadership recognized the need to more effectively coordinate and integrate the Security Threat Assessment Operations Division to OIA, which oversees the TWIC program and vetting functions, and realigned its offices in June 2016. With the realignment, leadership is further promoting unity of effort and establishing a single point of accountability within TSA for all security threat assessment programs management and operations. TSA's estimated completion date for these corrective actions is December 31, 2016.

OIG Analysis: TSA's proposed actions are responsive to the recommendation. This recommendation is resolved, but will remain open until TSA provides documentation formalizing the Security Threat Assessment Operations Division realignment to the OIA and its establishment of a single point of accountability within TSA for all security threat assessment program management and operations.

Recommendation 2: Concur. TSA recognizes that an end-to-end internal controls system, including risk analysis and management, will support the TWIC program's efforts to achieve goals and objectives. TSA will perform a risk analysis to review existing controls, identify and analyze risks, and promote control activities. TSA also plans to make improvements to its Technology Infrastructure Modernization system to include an additional quality assurance component in which the system will automatically select cases for Senior Adjudicators to review and to incorporate into the overall reporting and monitoring activities. Additionally, TSA is making policy changes to the Terrorism Vetting System to require a quality assurance review when an analyst determines that a "100-strength" system match is not in fact a match, and TSA plans to continue reviewing this policy to make adjustments, as needed. TSA's estimated completion date for full implementation of this recommendation is September 30, 2017.

OIG Analysis: TSA's proposed actions are responsive to the recommendation. This recommendation is resolved, but will remain open until TSA provides documentation to support actions taken to assess and improve the risk associated with the internal controls and quality assurance processes within the security threat assessment and terrorism vetting processes.

Recommendation 3: Concur. TSA understands that performance metrics are a critical component of effective program management and agrees it can enhance the TWIC performance measures for more direct one-to-one mapping to the TWIC program charter. TSA said it maintains performance measures that support DHS, TSA, and TWIC program objectives and that OIA collects and monitors more than 150 other operational metrics on TWIC program adjudication, card production, enrollment, vetting, and transactions, among other performance indicators. TSA plans to coordinate with OIG to ensure this recommendation is resolved and closed with reporting on current performance measures. The estimated completion date is December 31, 2016.

OIG Analysis: TSA's proposed corrective action is partially responsive to the recommendation. We agree that a more direct one-to-one mapping between its performance metrics and the TWIC program's core objectives will assist TSA in effectively managing and monitoring the TWIC program. However, TSA has not demonstrated how its current performance metrics address the core objectives on how TSA positively verifies the identity of those seeking access to secure areas, denies access to unauthorized individuals, and revokes access to individuals immediately upon their loss of eligibility. This recommendation is unresolved and open pending detailed evidence to support how TSA's current performance metrics address the recommendation.

Recommendation 4: Concur. The Security Threat Assessment Operations Division Adjudication Center has implemented a revised Training Manual and is working closely with TSA Senior Management to investigate the impact and criteria for disqualification under 49 CFR 1572.107. TSA is also updating adjudication Standard Operation Procedures related to the totality of criminal history criteria. TSA's estimated completion date is May 31, 2017.

OIG Analysis: TSA's corrective action is responsive to the recommendation. This recommendation is resolved, but will remain open until TSA provides documentation to support corrective actions taken, including a copy of the adjudication center's revised Training Manual, standard operating procedures, and additional guidance developed related to 49 CFR 1572.107.

Recommendation 5: Concur. TSA is completing the planning phase for recurrent criminal and immigration vetting. The planning phase includes coordination with industry and legal subject matter experts to assess feasibility, resourcing, funding, and operational constraints. TSA will update OIG to resolve and close this recommendation as it finalizes criteria and establishes its long-term path forward for recurrent criminal vetting. TSA estimates it will complete these corrective actions by December 31, 2016.

OIG Analysis: TSA's corrective action is responsive to the recommendation. This recommendation is resolved, but will remain open until TSA completes the recurrent criminal and immigrations vetting planning phase and provides finalized criteria for selecting its long-term recurrent vetting option.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

Our audit objective was to determine whether the applicant screening process for Transportation Worker Identification Credential (TWIC) is operating effectively and ensuring only eligible TWIC cardholders remain in the program. To answer the objective, we:

- obtained and reviewed pertinent Federal laws and regulations, departmental and component regulations, policies, procedures, and guidance relevant to the TWIC program;
- reviewed and analyzed GAO reports from May 2011 and May 2013;
- reviewed and analyzed DHS OIG relevant reports;
- interviewed TSA and USCG officials responsible for the management, oversight, and execution of the TWIC program; and
- performed data reliability testing of TSA's Technology Information Management System recorded between October 1, 2011, and May 31, 2015.

To assess the effectiveness of the background check processes, we compared a sample of 435 TWICs against 4 data systems to determine whether the sample remained eligible for unaccompanied access to secure maritime facilities. We also tested whether TSA adjudicators followed policies and procedures when reaching their decisions. Because essential information in some instances was unavailable, we were precluded from comparing all sampled cases. As a result, we did not make general conclusions regarding the overall effectiveness of TSA's Security Threat Assessments completed for the 1,421,541 TWICs issued during the scope of our audit. Appendix E provides details of the statistical sample and the results of our comparisons.

We also conducted site visits in the following locations:

- TSA and USCG Headquarters in Washington, DC;
- DHS Screening and Coordination Office, Washington, DC;
- TSA Adjudication Center, Reston, VA;
- Colorado Spring Operations Center, Colorado Springs, CO;
- Office of Biometric Identity Management, National Protection and Programs Directorate for IDENT, Washington, DC;
- Government Publishing Office, Washington, DC;
- MTSA Facilities in Boston, MA, and Port Everglades, FL; and
- Enrollment centers in Boston, MA, and Fort Lauderdale, FL.

We conducted this performance audit between May 2015 and May 2016 pursuant to the *Inspector General Act of 1978,* as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
TSA Comments to the Draft Report

~~FOR OFFICIAL USE ONLY~~

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation
Security
Administration

MEMORANDUM FOR: Mark Bell
Assistant Inspector General for Audits
Office of Inspector General
U.S. Department of Homeland Security

FROM: Huban A. Gowadia, Ph.D.
Deputy Administrator
03 AUG 2016

SUBJECT: Formal Response to the OIG Draft Report: *TWIC Background Checks are Not as Reliable as They Could Be* (Project Number OIG-15-104-AUD-USCG, TSA)

This memorandum and attachment constitute the Transportation Security Administration's (TSA) formal response to the subject audit report. Thank you for the opportunity to review and comment on this draft report.

TSA appreciates the Office of the Inspector General's (OIG) description of the security threat assessment (STA) process for Transportation Worker Identification Credential (TWIC) applicants. As noted in the OIG report, "TWIC is integral to the safety of the ports and other maritime facilities."

Overall, TSA concurs with OIG's recommendations as the program continuously seeks to improve program security and operations. TSA conducts internal assessments of the program across multiple functional areas from technology, policy, and operational perspectives. The OIG's findings on internal controls and recommendation for a risk analysis will help TSA achieve TWIC program objectives and allow TSA to enhance and update its control activities. While TSA concurs with the ongoing need for improved oversight, controls, and guidance, the report does not include a comprehensive discussion on the existing internal controls and quality assurance mechanisms that TSA currently uses to manage the TWIC program.

TSA's Office of Intelligence and Analysis (OIA) maintains detailed adjudication and vetting guidance, policies, procedures, and training to enroll workers for a TWIC and

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

conduct STAs. TSA has developed metrics, roles, and reviews to provide appropriate controls for the TWIC program. The TWIC program contributes to the Agency-wide Management Control Objective Plan (MCOP). Aligned with Office of Management and Budget (OMB) Circular A-123 and the Financial Manager's Financial Integrity Act (FMFIA), TSA established MCOP to implement, evaluate, and report on TSA's management controls. In addition, the TWIC program conducts operational assessments that provide program status reporting, including metrics aligned to TSA's strategic, business, customer service, and financial performance goals. These measures are submitted through the DHS capital planning and investment system on a monthly basis. The assessments and measures are reviewed and approved by both TSA and DHS Office of the Chief Information Office staff. These oversight functions are integral to management of the program, and should be included in the report to more fully convey the management and operational activities in place to ensure the TWIC program meets its security objectives.

The draft report contained five recommendations with which TSA concurs. Please see the attached detailed response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. TSA appreciates the work of OIG during the course of this audit and will use the information to assist our ongoing efforts to improve the TWIC program's oversight and guidance. Technical comments were previously provided under separate cover. If you have any questions, please feel free to contact me.

Attachment:
TSA Response to OIG Recommendations

~~FOR OFFICIAL USE ONLY~~

Attachment: TSA Response to Recommendations Contained in Draft Report, *TWIC Background Checks are Not as Reliable as They Could Be*, June 2016

The Office of the Inspector General (OIG) recommended the following:

Recommendation 1: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration identify a cross-functional coordinating entity with authority, responsibility, and accountability to provide regular guidance and leadership across all Security Threat Assessment processes and supporting offices.

TSA Response: The Transportation Security Administration (TSA) concurs with this recommendation. Before the OIG report was drafted, TSA leadership was coordinating activities to realign the Security Threat Assessment Operations (STAO) Division from the Office of Law Enforcement/ Federal Air Marshal Service (OLE/FAMS) to the Office of Intelligence and Analysis (OIA), which oversees the Transportation Worker Identification Credential (TWIC) program and vetting functions. TSA finalized the realignment in June 2016. TSA OIA and OLE/FAMS leadership recognized the need to more effectively coordinate and integrate these functions. With the realignment, leadership is further promoting unity of effort and establishing a single point of accountability within TSA for all security threat assessment (STA) program management and operations. The realignment facilitates more seamless integration and communication for managing and developing current-state and future-state STA/vetting technology and case management requirements, policy, and procedures. The realignment enhances mission effectiveness and reinforces accountability for resource utilization to perform end-to-end STA functions for the multiple vetting programs critical to an intelligence-driven, risk-based approach to our counterterrorism mission. TSA's emphasis on driving effective, high-performance counterterrorism operations demands that a combination of intelligence and vetting functions inform daily security operations. TSA will coordinate with the OIG to ensure this recommendation is resolved and closed with documentation formalizing STAO's realignment to the OIA. Estimated Completion Date (ECD): December 31, 2016

Recommendation 2: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration conduct a comprehensive risk analysis of the Security Threat Assessment processes to identify areas needing additional internal controls and quality assurance procedures; and develop and implement those procedures, including periodic reviews to evaluate their effectiveness.

TSA Response: TSA concurs with this recommendation. TSA recognizes that an end-to-end internal controls system, including risk analysis and management, will support the

TWIC program's efforts to achieve goals and objectives. As a major information technology investment, the TWIC program completed several control and risk reviews to support U.S. Department of Homeland Security (DHS) mandated operational assessments. Also, the TWIC program contributes to TSA's Agency-wide internal control plan, the Management Control Objective Plan (MCOP). TSA recognizes the value of conducting a risk analysis and developing a more integrated system of controls to account for TWIC procedures from enrollment to credential issuance.
TSA will perform a risk analysis to review existing controls, identify and analyze risks, and promote control activities. TSA will establish the appropriate control environment and monitoring system to regularly review TWIC risk responses and control activities. In addition, a planned modification to the Technology Infrastructure Modernization (TIM) system will contain an additional quality assurance component in which STA cases are automatically selected for review by Senior Adjudicators and will be incorporated into the overall reporting and monitoring activities. Also, TSA OIA established an additional quality assurance (QA) process where the Transportation Vetting System automatically forwards every "100-strength" matches that were determined to be a "no match" in the vetting system to an experienced and qualified vetting analyst for quality assurance review of the match. TSA will continue to analyze this QA measure and adjust appropriately based on findings. Interim ECD: March, 31, 2017; Risk assessment complete and internal controls identified. ECD: September 30, 2017

Recommendation 3: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration improve TWIC program-level performance metrics to ensure they align with the program's core objectives, and direct management officials to use these metrics for all the supporting offices.

TSA Response: TSA concurs with this recommendation. TSA understands that performance metrics are a critical component of effective program management. One of the program's key tenets is to continually assess and enhance measures and procedures to improve program security and operations; TSA will continue to do so. TSA agrees that the performance measures could be enhanced for more direct one-to-one mapping to the TWIC program charter for clarity and improve integration of measures across functions tied to overall program core objectives.

TSA OIA maintains 10 performance measures for the TWIC program that support DHS, TSA, and TWIC program objectives. In addition to those performance metrics, OIA collects and monitors daily more than 150 other operational metrics on TWIC program adjudication, card production, enrollment, vetting, and transactions, among other performance indicators. In compliance with U.S. Office of Management and Budget (OMB) Circular A-11 and DHS Chief Information Officer requirements, the measures concern Strategic and Business Results, Financial Performance, and Customer

Satisfaction. The program's measures are reviewed by TSA and DHS and results are posted to the OMB Federal Information Technology (IT) Dashboard. As a major information technology program for DHS, OIA established and exceeded performance measurement requirements for the TWIC program.

The existing performance measures are annually reviewed and accepted by DHS and OMB. TSA will align current and future measures to department, agency, and program objectives to ensure effective monitoring and management over TWIC program operations that are the responsibility of TSA. As part of effective performance management, the TWIC program will review its list of identified measures annually, identify inputs on TWIC processes, and enhance output or outcome measures that inform on program effectiveness as appropriate.

The OIG review stated that customer service metrics "do not align with TWIC's core objectives…and instead create competing priorities that increase the risk that TSA may issue TWIC credentials to someone who is not qualified." TSA views that "customer service" metrics as an important component of program-wide controls for the TWIC program. Effective customer service is a critical component of DHS Strategic Goal One: Reduce Risk to the Nation's Critical Infrastructure, Key Leadership, and Event; as well as TSA Strategic Goal Two: External Engagement – Sustain transparent and proactive relationships with external stakeholders and the traveling public. Also, Customer Satisfaction measures are a requirement for major information technology (IT) programs submitted under OMB Circular A-11.

Metrics on applicant data corrections, support tickets, and enrollment center availability support accurate and secure adjudication steps. Customer service metrics relate to the accuracy of information being captured to ensure vetting accuracy tied to applicant identity, as well as accuracy of communicating with applicants on responsibilities for enrolling for a TWIC. Similarly, the measures monitor the program's effectiveness at implementing its security requirements without undue burden to those impacted by the regulation. Part of TSA's core mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TWIC applicants require the credential to hold a specific job, and disruptions and delays in customer service in the TWIC process could directly impact their movement and the flow of commerce when they are prevented from continuing to work. As part of sound internal controls and risk management, TSA will preserve the TWIC program metrics that help TSA ensure TWIC credentials are granted to applicants in an appropriate manner.

TSA will coordinate with the OIG to ensure this recommendation is resolved and closed with reporting on current performance measures, including the alignment to core TWIC objectives that fall under the purview of TSA. ECD: December 31, 2016

Recommendation 4: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration review current Transportation Worker Identification Credential Security Threat Assessment guidance to ensure it provides adjudicators the necessary information and authority to complete Security Threat Assessments.

TSA Response: TSA concurs with this recommendation. During the audit period, the STAO Division Adjudication Center implemented a revised Training Manual that contains a Table of Contents and index. The Adjudication Center is working closely with TSA Senior Management to investigate the impact and criteria for disqualification under 49 CFR §1572.107 and in the process of providing even more detailed guidance to update the adjudication Standard Operation Procedures related to the totality of criminal history criteria. ECD: May 31, 2017

Recommendation 5: We recommend that the Assistant Administrator, Office of Intelligence and Analysis, Transportation Security Administration establish measurable and comparable criteria to use in evaluating and selecting the best criminal and immigration recurrent vetting option.

TSA Response: TSA concurs with this recommendation. TSA OIA is in the process of completing its recurrent criminal and immigration vetting planning phase and beginning analysis for the long-term, automated recurrent criminal and immigration vetting solution for all STA programs. The planning is in conjunction with the TIM program, Federal Bureau of Investigation (FBI) Rap Back service, and DHS Automated Biometric Identification System (IDENT). Planning also includes coordination with and input from each program's respective industry and legal subject matter experts to assess feasibility, resourcing, funding, and operational constraints required by TSA, and regulated entities (e.g., airports, air carriers, and states as well as Transportation Worker Identification Credential authorities).

For clarification purposes, DHS IDENT was built to hold all DHS fingerprints and provide biometric encounter information across agencies. The FBI Rap Back service provides updated rap sheets for recurrent criminal hits on enrolled populations. Also, rap sheets can be obtained through IDENT. TSA will use IDENT as its primary system to store fingerprints and conduct biometric vetting against derogatory information datasets. Currently, TWIC applicant biometrics are transmitted to IDENT. The TWIC program has already initiated the receipt of manual notification of criminal and immigration vetting from the IDENT system while awaiting the technical implementation of additional, automated recurrent IDENT biometric vetting as part of the TIM program future capabilities. These additional capabilities are planned for the TWIC program for fiscal year 2017. TSA will update OIG to resolve and close this recommendation as the

~~FOR OFFICIAL USE ONLY~~

5

measurable and comparable criteria are finalized and established in support of selecting its long-term path forward for recurrent criminal vetting. ECD: December 31, 2016

~~FOR OFFICIAL USE ONLY~~

Appendix C
TWIC Disqualifying Offenses

Per TSA's website (https://www.tsa.gov/disqualifying-offenses-factors), the following permanent and interim criminal offenses may disqualify an individual from being granted a TWIC.

PERMANENT DISQUALIFYING CRIMINAL OFFENSES

An applicant will be disqualified if he or she was convicted, pled guilty (including 'no contest'), or found not guilty by reason of insanity for any of the following felonies regardless of when they occurred:

1. Espionage or conspiracy to commit espionage.
2. Sedition or conspiracy to commit sedition.
3. Treason or conspiracy to commit treason.
4. A Federal crime of terrorism as defined in 18 United States Code (U.S.C.) 2332b(g), or comparable State law, or conspiracy to commit such crime.
5. A crime involving a TSI (transportation security incident). Note: A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101. The term "economic disruption" does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.
6. Improper transportation of a hazardous material under 49 U.S.C. 5124 or a comparable state law.
7. Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).
8. Murder.
9. Threat or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportations system, or an infrastructure facility.
10. Violations of the *Racketeer Influenced and Corrupt Organizations Act*, 18 U.S.C. 1961, et seq., or a comparable State law, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the permanently disqualifying crimes.
11. Attempt to commit the crimes in items (1)-(4) of this section.

12. Conspiracy or attempt to commit the crimes in items (5)-(10) of this section.

An applicant may apply for a waiver for any disqualifying offense listed above for numbers 5 through 12 (49 CFR 1515.7).

INTERIM DISQUALIFYING CRIMINAL OFFENSES

Conviction for one of the following felonies is disqualifying if the applicant was convicted, pled guilty (including 'no contest'), or found not guilty by reason of insanity within 7 years of the date of the application; OR if the applicant was released from prison after conviction within 5 years of the date of the application.

1. Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.
2. Extortion.
3. Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering, where the money laundering is related to a crime listed in Parts A or B (except welfare fraud and passing bad checks).
4. Bribery.
5. Smuggling.
6. Immigration violations.
7. Distribution, possession w/ intent to distribute, or importation of a controlled substance.
8. Arson.
9. Kidnapping or hostage taking.
10. Rape or aggravated sexual abuse.
11. Assault with intent to kill.
12. Robbery.
13. Fraudulent entry into a seaport as described in 18 U.S.C. 1036, or a comparable State law.
14. Violations of the *Racketeer Influenced and Corrupt Organizations Act* (RICO) under 18 U.S.C. 1961, et seq., or a comparable State law, other than any permanently disqualifying offenses.
15. Voluntary Manslaughter.[10]
16. Conspiracy or attempt to commit crimes in this section.

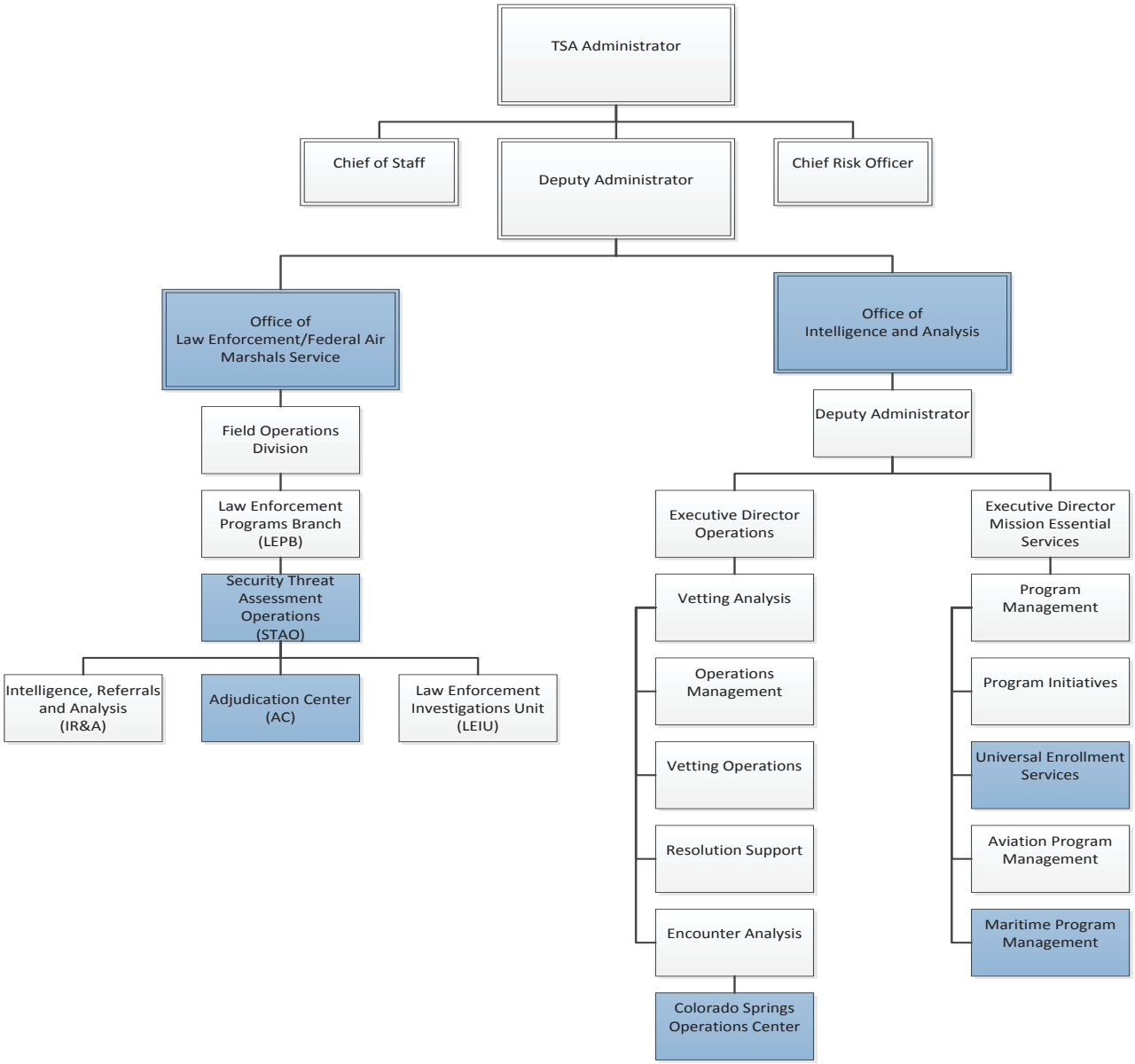
[10] Voluntary manslaughter is not listed as an Interim Disqualifying Criminal Offense in the Federal regulations (49 CFR 1572.103). TSA's website includes this offense based on an April 1, 2014 internal determination that was not subject to formal or informal rulemaking.

Note: For the TWIC program, an applicant may apply for a waiver for any interim disqualifying offense (49 CFR 1515.7).

UNDER WANT, WARRANT, OR INDICTMENT

A person will be disqualified if he or she is wanted or under indictment in any civilian or military jurisdiction for a felony listed as a permanent or interim disqualifying offense until the want or warrant is released or the indictment is dismissed.

Appendix D
Excerpt of TSA's Organization Chart
as of May 30, 2016



***Source**:* OIG Analysis of several TSA Organization Charts

Appendix E
Statistical Sample Results

TSA issued 1,421,541 TWICs between October 1, 2011, and May 31, 2015. Given the universe of 1,421,541 TWICs, 95 percent confidence interval, 5 percent sampling error and 50 percent population proportion, the statistically valid sample size was 385. To have a larger sample for our analysis, we increased it to 435. We stratified our sample to include Automatically Approved TWICs (200 TWICs) and Manually Approved TWICs (235 TWICs). We used IDEA software to randomly select all 435 TWIC samples as shown in the following table.

Table 1. Statistical Sample

Stratum	Description	# of Applications in Universe	% of Population	Sample Size
1	Automatically Approved TWICs	633,072	44.5%	200
2	Manually Approved TWICs	788,467	55.5%	235
Total		1,421,539	100%	435

Source: OIG

TWICs Compared Against Four Data Systems

We planned to compare the background check information for the 435 sampled TWICs against 4 data systems to determine whether the sample remained eligible for unaccompanied access to secure maritime facilities. The data systems used to compare the sampled TWIC cases were (1) the FBI Terrorist Screening Center's Consolidated Watchlist; (2) the U.S. Citizenship and Immigration Services' (USCIS) Computer Information System; (3) the Office of Biometric Identity Management IDENT System; and (4) the Social Security Administration OIG's Death Master File. Because essential information in some instances was unavailable, we were precluded from comparing all cases to the IDENT and Death Master File systems. As a result, we cannot make general conclusions regarding the overall effectiveness of TSA's Security Threat Assessments completed for the 1,421,539 TWICs.

We compared the 435 sampled TWICs against the following four data systems as follows:

(1) ***FBI Terrorist Screening Center's Consolidated Watchlist*** data was matched against the sampled TWIC biographic information to determine whether any individual was a known or suspected terrorist.

(2) ***USCIS's Computer Information System*** data was matched against the names and available alien or resident numbers from our TWIC sample to determine whether any of the sample cardholders' immigration statuses changed since enrolling in the TWIC program.

Of the 435 sample TWICs, 388 claimed U.S. Citizenship when they applied for a TWIC. Although they may not have had a resident or alien number associated with their case, we provided USCIS with their name and other biographic information to test whether they were in the database.

(3) ***Office of Biometric Identity Management IDENT System*** data was matched against the sampled TWICs biometric information to determine the presence of any new derogatory information, including immigration and criminal offenses. TSA completed the background check using its legacy data system for 319 of the 435 sampled TWICs. TSA's legacy system biometric file format was incompatible with IDENT. Therefore, we could not compare 319 of the 435 sampled cases to IDENT.

(4) ***Social Security Administration OIG's Death Master File*** was matched against the names and available Social Security numbers for the TWIC sample to determine whether any cases included potentially fraudulent identities. Because social security numbers are not required, TSA's records did not contain the social security number for 18 of the 435 sampled cases.

Results for Comparisons Against Four Data Systems

Based on our comparison of the sampled TWIC cases to the four systems selected, we did not identify any disqualifying information or violation of Federal regulation or TSA procedures as illustrated in table 2. We did identify instances where additional guidance and oversight is needed as described in the report.

Table 2. Results for Comparison against Four Data Systems

System Number	Description of System Compared	TWIC Cases Compared/Sample Size	Percent Compared	Number of Issues Identified/Number Compared	Percent Error
1.	FBI Terrorist Screening Center	435/435	100%	0/435	0%
2.	U.S. Citizenship and Immigration Services	435/435	100%	0/435	0%
3.	Office of Biometric Identity Management IDENT System	116/435	27%	0/116	0%
4.	Social Security Administration OIG Death Master File	417/435	96%	0/417	0%

Source: OIG

Appendix F
Recurrent Vetting Options

Rap Back

The FBI deployed the FBI Next Generation Identification Rap Back. The Rap Back Service provides authorized agencies with notification of criminal and, in limited cases, civil activity of individuals that occurs after the initial processing and retention of criminal or civil transactions. The Rap Back Service implements new response services to notify agencies of subsequent activity for individuals enrolled in the service. This feature provides a more timely process of confirming suitability of those individuals placed in positions of trust and notifying users of criminal activity for those individuals placed on probation or parole.

IDENT

The Automated Biometric Identification System (IDENT) is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; and other background investigative purposes. It stores and processes biometric data — digital fingerprints, photographs, iris scans, and facial images — and links biometrics with biographic information to establish and verify identities. As far back as 2007, DHS has identified IDENT as the target application for the collection and use of biometric information

Agencies that update the IDENT system with new information on persons encountered include the Departments of Justice, Defense, and State; and DHS components such as Customs and Border Protection and Immigration and Customs Enforcement. IDENT can provide information to agencies when new derogatory information has been added to an individual's profile.

Appendix G
Office of Audit Major Contributors to This Report

Donald Bumgardner, Deputy Assistant Inspector General for Audits
Paul Wood, Director
Christine Haynes, Acting Director
Yesi Starinsky, Audit Manager
Tricia Benson, Program Analyst
Douglas Campbell, Program Analyst
Armando Lastra, Auditor
Oluwabusayo Sobowale, Auditor
Kevin Dolloson, Communications Analyst
Elizabeth Argeris, Communications Analyst
Mohammad Islam, Statistician
David Kinard, Independent Report Referencer
Matthew Neuburger, Attorney

Appendix H
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
TSA Administrator
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
TSA Audit Liaison
USCG Audit Liaison
DHS Audit Liaison
USCIS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305