Department of Homeland Security

# Office of Inspector General

## Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs

OIG-14-139

September 2014

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

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

September 10, 2014

MEMORANDUM FOR: Charles R. Armstrong
Assistant Commissioner and Chief Information Officer
U.S. Customs and Border Protection

FROM: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs*

Attached for your information is our final report, *Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs*. We incorporated the formal comments from the U.S. Customs and Border Protection in the final report.

The report contains two recommendations aimed at improving CBP's use of radio frequency identification technology in their Trusted Traveler Programs. Your office concurred with two recommendations. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Based on information provided in management's response to the draft report, we consider both recommendations to be open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to OIGITAuditsFollowup@oig.dhs.gov. Until your response is received and evaluated, the recommendations will be considered open and unresolved.
Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to appropriate 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 Chiu-Tong Tsang, Director, Information Security Audit Division, at (202) 254-5472.

Attachment

# Table of Contents

## Appendixes

## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| DHS | Department of Homeland Security |
| FAST | Free Access and Secure Trade |
| PII | personally identifiable information |
| RFID | Radio Frequency Identification |
| SENTRI | Secure Electronic Network for Travelers Rapid Inspection |
| TTP | Trusted Traveler Programs |

# Executive Summary

The United States Customs and Border Protection (CBP) employs radio frequency identification technology in its Trusted Traveler Programs to allow pre-screened travelers expedited processing at designated ports of entry. Radio frequency identification is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. The flexibility and portability of radio frequency identification technology has introduced new security risks to agency systems, such as cloning of an identification tag and the security of the database that stores personal data. Without effective security controls and procedures over this technology and its supporting infrastructure, unauthorized individuals could modify identification tag content or access sensitive data stored in the system databases.

Our overall objective was to determine whether CBP has effectively managed the implementation of radio frequency identification technology. In addition, we determined whether the component had implemented effective controls to comply with DHS information security program requirements.

CBP implemented effective physical controls over the readers and computer equipment supporting the trusted traveler systems at the ports of entry visited. Also, CBP implemented effective controls on the servers and database that support the Trusted Traveler Programs. Further, CBP had secured the personal information collected under the component's Trusted Traveler Programs and minimized the risk of using the radio frequency identification technology by restricting information stored on the trusted traveler cards.

However, CBP can make further improvements by implementing the required security settings on the system that supports its Trusted Traveler Programs. Also, administrators that manage the system must receive specialized training annually to ensure that they have the skills necessary to secure the data collected under the Trusted Traveler Programs.

We are making two recommendations to the Assistant Commissioner and Chief Information Officer to improve the security of its systems that support the Trusted Traveler Programs. CBP concurred with all recommendations and has begun to take actions to implement them. CBP's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

## Background

Radio Frequency Identification (RFID) is a form of automatic identification and data capture technology that uses radio frequencies to transmit information. RFID tags are affixed or embedded to items to provide identification. The tag has a unique identifier that can hold additional information. Devices known as RFID readers communicate wirelessly with the tags to identify the items connected to each tag and read or update additional information stored on the tag. The system of tags and readers is often supported by servers, databases, and workstations. Figure 1 shows the components of an RFID system, including a tag, reader, and database.

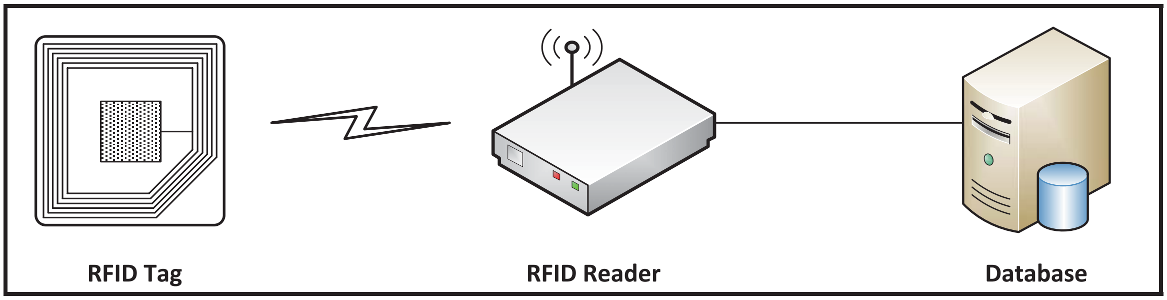


**Figure 1. Components of an RFID system**

Tags need power to perform functions, such as sending radio signals to a reader, storing and retrieving data, and performing other computations. The four types of tags include:

- Active tags have an internal power source and can transmit over a greater distance.

- Semi-active tags remain dormant until they receive a signal from the reader to activate.

- Passive tags do not use a separate or external power source, but instead obtain operating power from the tag reader. Passive tags are typically cheaper, smaller, and lighter than other types of tags.

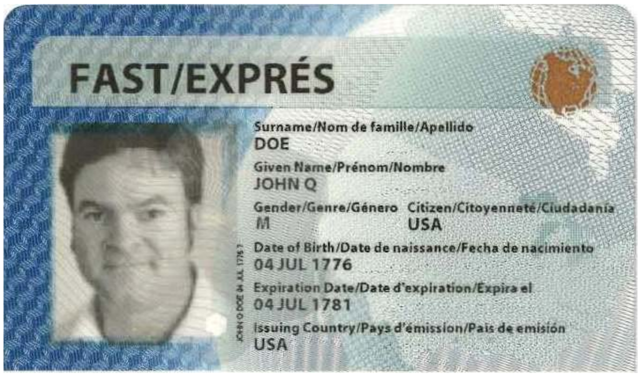
- Semi-passive tags use an internal power source to monitor environmental conditions and require radio frequency energy transferred from the reader to power a tag's response.

The flexibility and portability of RFID technology has introduced new security risks to agency systems, such as cloning of an RFID tag and the security of the database that stores personal data.[1] Without effective security controls and procedures over this technology and its supporting infrastructure, unauthorized individuals could modify tag content or access sensitive data stored in the system databases.

CBP employs RFID technology as part of its Trusted Traveler Programs (TTP) to allow pre-screened travelers expedited processing at designated ports of entry. CBP attaches an RFID tag in each TTP card. Travelers who wish to participate in TTP voluntarily submit personally identifiable information (PII) through a web-based application system CBP uses to handle TTP's enrollment and vetting processes. CBP stores applicants' data (e.g., biographic data, facial photographs, and background investigation results) in a database. At the border, RFID readers scan the TTP cards and use the unique number embedded in each card to retrieve the traveler's data through an encrypted network. The CBP Officer uses the traveler's information displayed on a monitor to authenticate the traveler's identity. CBP employs RFID technology in the following three subprograms within TTP:

<u>Free Access and Secure Trade (FAST)</u>

FAST is available for commercial truck drivers, who have completed favorable background checks and fulfill certain eligibility requirements, at 17 land ports of entry on the northern border and 17 on the southern border that serve commercial cargo. The majority of dedicated FAST lanes are located along the northern border ports in Michigan, New York, and Washington, and at southern border ports from California to Texas. As of September 2013, there were approximately 86,000 drivers approved for this program. Figure 2 shows a FAST TTP card.



FAST/EXPRÉS

Surname/Nom de famille/Apellido
DOE

Given Name/Prénom/Nombre
JOHN Q

Gender/Genre/Género
M

Citizen/Citoyenneté/Ciudadanía
USA

Date of Birth/Date de naissance/Fecha de nacimiento
04 JUL 1776

Expiration Date/Date d'expiration/Expira el
04 JUL 1781

Issuing Country/Pays d'émission/País de emisión
USA

JOHN Q DOE 04 JUL 1776

**Figure 2. FAST TTP card**

<u>NEXUS</u>

NEXUS is available for pre-approved, low-risk travelers between the U.S. and Canada via the air, land, or sea environments. As of September 2013, there were approximately 250,000 travelers enrolled in NEXUS.

[1] Cloning is the illegitimate duplication of the information stored in the RFID tag portion of the RFID enabled card.

Secure Electronic Network for Travelers Rapid Inspection (SENTRI)
SENTRI is available for pre-approved, low-risk travelers along the southern land border. SENTRI is available for both vehicle and pedestrian border crossers. Each of the participating ports has designated vehicle and pedestrian lanes for SENTRI cardholders. Vehicles must be pre-inspected, registered, and issued with a windshield decal for border crossings. As of September 2013, there were approximately 91,000 travelers enrolled in SENTRI. Figure 3 shows SENTRI RFID reading equipment and associated border lanes.

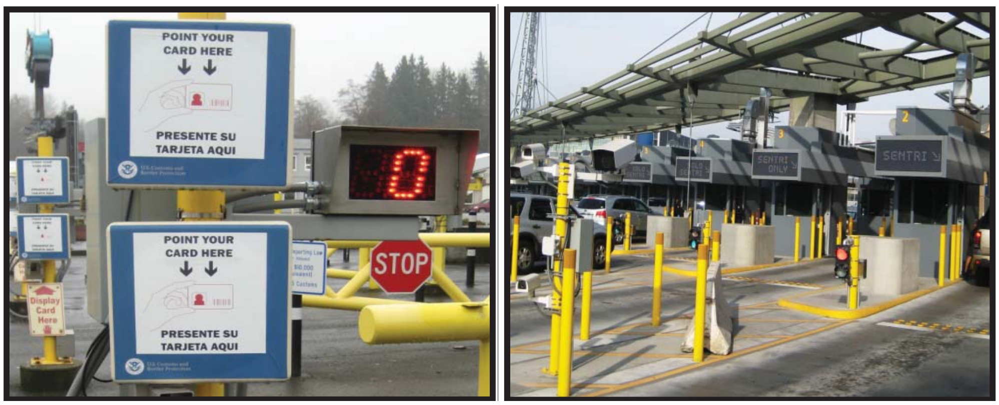


**Figure 3. SENTRI RFID reading equipment and border lanes**

In May 2006, we reported that CBP had not implemented effective controls to protect critical data processed by its trusted traveler systems. In addition, CBP had not developed adequate policies and procedures to ensure that security controls were implemented consistently by all ports of entry to protect the trusted traveler systems. Lastly, CBP had not ensured that its trusted traveler systems fully complied with all *Federal Information Security Management Act* requirements.[2]

## Results of Audit

### Using RFID To Expedite Border Crossings

CBP has expedited border crossings by using RFID technology for registered travelers enrolled in the TTP. In addition, CBP maintains the integrity of the TTP through a stringent screening process that includes automated searches against multiple law enforcement databases, 24-hour system checks to verify status of enrolled travelers, and random selections of registered travelers for secondary inspection. Further, CBP developed a TTP handbook that includes procedures for inspecting travelers at the ports

[2] *CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security* (OIG-06-36, May 2006).

of entry and policies for enrolling travelers into the TTP. To reduce the risk of theft of PII, CBP stores a unique identification number embedded in TTP cards and locks the RFID memory chip to prevent modification of stored data.

CBP has taken the following actions to create an environment and infrastructure necessary to enhance legitimate trade and travel:

- Implemented effective physical controls over the readers and computer equipment supporting the trusted traveler systems at the ports of entry visited. Specifically, we noted that readers were protected from unauthorized access in a locked box and supporting information technology infrastructure (i.e., access to the database and servers) are located within a gated, restricted access facility.

- Established a test environment that simulates land border inbound and outbound inspection operations to test new and existing applications at CBP's government test lane facility.

Patch Program Supporting the TTP

CBP has implemented a program to apply security patches on the servers and databases that support the TTP.[3] CBP has developed policies and procedures to outline its patching and change control processes to apply changes to the system in a controlled and coordinated manner. Additionally, CBP has instituted a Vulnerability Assessment Team to conduct security assessments monthly to identify missing patches on its systems. Lastly, CBP has created testing environments to observe the effects of security patches prior to deploying to production systems.

RFID Tag Security

We used a commercially available RFID tag reader to access the information stored on TTP cards at selected ports of entry along the northern and southern borders and evaluated the effectiveness of security controls implemented on TTP cards. We simulated the same process used by CBP's RFID reader and attempted to record TTP enrollees' information with our own reader, as the travelers entered the lanes. We verified that CBP did not store any PII on the TTP cards and only the unique identification number was present. In the event that an attacker obtained this information to produce a duplicate card, CBP officers can minimize the threat by

[3] A security patch is an update designed to fix vulnerabilities in applications or operating systems.

verifying the travelers' PII and picture presented on their terminal. We performed testing at eight ports of entry, with different lane types, to determine if CBP consistently implemented the RFID technology across the TTP. Figure 4 depicts ports of entry visited and specific TTP subprograms present at these ports.

| Port of Entry | FAST | SENTRI | NEXUS |
|---|---|---|---|
| Rainbow Bridge (New York) | X | | X |
| Whirlpool Bridge (New York) | | | X |
| Peace Bridge (New York) | X | | X |
| Peace Arch (Washington) | X | | X |
| Pacific Highway (Washington) | X | | X |
| San Ysidro (California) | X | X | |
| Calexico (California) | X | X | |
| Otay Mesa (California) | X | X | |

**Figure 4. Ports of Entry Visited and TTP Subprograms**

While CBP had taken actions to secure travelers' PII, including safeguards to lessen the risks of using RFID technology, we identified deficiencies in other areas of TTP that need improvements. Specifically, we identified deficiencies in CBP's implementation of Department of Homeland Security's (DHS) Baseline Configuration settings, and personnel overseeing TTP systems have not received the required specialized training annually.[4]

## Improvements Needed on System Security Controls

CBP had not implemented all the required DHS security configuration settings on its Windows and Oracle-Linux servers, which may allow unauthorized individuals to gain access to sensitive data used to support the TTP.[5] To assess the effectiveness of controls implemented on TTP servers and database, we interviewed selected information technology and program management personnel. In addition, we reviewed the configuration settings on selected servers for compliance with applicable DHS baseline configuration guidance. We also reviewed the configuration settings on the Oracle database that stores the PII used to verify traveler records.

DHS established baseline configuration settings that provide the guidelines and parameters for ensuring a minimum baseline of security when installing or

[4] Baseline configuration settings provide system and database administrators with procedures that will ensure a minimum baseline of security in the installation and configuration of the hardware and software.
[5] Oracle-Linux is the server operating system that is used to host the database to store traveler's PII.

configuring operating systems. The guidelines include controls for user access, password management, auditing, and services. These settings help secure the confidentiality, integrity, and availability of the information and system.

The results of our audit revealed that CBP had implemented 85 percent of the selected security controls outlined in the DHS baseline configuration guidance for Oracle databases. CBP management had either obtained a waiver from DHS not to implement the settings or documented the configuration management deviations we identified in plans of action and milestones.[6] However, we identified the following configuration setting deficiencies that may be exploited on the Windows and Oracle-Linux servers if not addressed timely:

- Minimum password age on Windows and Oracle-Linux servers was set to permit users to change their password more frequently than required, which may allow the user to change to a favorite password quicker. This would allow a user to use a favorite password repeatedly and for a longer period of time, which increases the possibility of compromised passwords. DHS requires the password age be set for a minimum of 7 days on Linux servers, and 1 day for Windows servers. According to the Windows administrators, the deviation is essential for password management and CBP has implemented password history to prevent users from reusing old passwords.[7]

- The audit trail was set to record only unsuccessful system events (e.g., system shutdown, time changed). Recording the correct type of system event is important to reconstruct security incidents. DHS requires only successful system events be recorded.

- DHS requires the use of Windows NT LAN Manager version 2, to authenticate the identity of users and other systems. However, CBP used an older and less secure version of authentication protocol.

- DHS prohibits the use of an unrestricted user account (i.e., root) to log into systems through an encrypted connection. When the root account is shared between different administrators actions taken through an encrypted connection, such as modification of files, cannot be tracked.

[6] A plan of action and milestone is a tool identifying tasks that need to be accomplished.
[7] Password history sets how frequently old passwords can be reused. This setting can be used to discourage users from changing back and forth between a set of common passwords.

CBP configured its Linux operating systems to allow root users to login on encrypted connections.

Without implementing the required configuration settings, CBP cannot ensure that the system that supports its TTP is secured and protected from unauthorized access. Further, RFID systems operating without the required configuration settings increases the possibility that malicious users can circumvent the security controls protecting CBP systems.

**Recommendation**

We recommend that the Assistant Commissioner and Chief Information Officer:

**Recommendation #1:**

Implement the required DHS sensitive systems configuration settings on Windows and Oracle-Linux servers that support the TTP or accept the risk by documenting the deviations in the system security plan.

**Management Comments and OIG Analysis**

CBP concurred with recommendation 1. CBP will evaluate the current settings on Windows and Linux and determine the need to implement the required settings. CBP estimates the corrective actions will be completed by February 28, 2015.

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until CBP provides supporting documentation that all planned corrective actions are completed.

**<u>Specialized Training Needed To Ensure Sensitive TTP Data is Secured</u>**

The administrators, who are responsible for managing the global enrollment system and its subsystems, have not received the required specialized training within the past year. Since the global enrollment system holds TTP participants' PII, it is critical that administrators obtain the required training to properly secure the data. Our audit of training records for 14 technical personnel (e.g., Information Systems Security Officers, system administrators) revealed that while all had taken the required DHS security awareness and privacy awareness training, only 2 had taken specialized training within the required timeframe.

DHS requires that personnel, contractors, and others working on behalf of DHS with significant security responsibilities shall receive initial specialized training and thereafter refresher training annually specific to their security responsibilities. CBP must provide senior managers, system owners, and information technology project managers specialized security-related training.

Due to a lack of funding and the Department's discontinuation of the specialized, technical training courses, CBP could not send its personnel with significant responsibilities to training, such as the DHS INFOSEC Introductory Information System Security Officer and the DHS INFOSEC System Administrator courses. CBP officials told us that DHS had not developed any new technical training to replace discontinued courses and there were no indications to do so. Further, CBP does not have sufficient resources to provide these courses but will continue to access the technical training available within the CBP Virtual Learning Center and develop replacement training courses.

Without specialized training, technical personnel may not possess the skills necessary to perform their assigned security responsibilities to safeguard PII data. Specialized training is of particular importance to those with access to the global enrollment system because this system contains PII used in the production of TTP cards.

**Recommendation**

We recommend that the Assistant Commissioner and Chief Information Officer:

**Recommendation #2:**

Provide technical staff with the required specialized trainings and skills necessary to properly secure the global enrollment system and the sensitive information residing within the system.

CBP concurred with recommendation 2. CBP plans to augment its role-based security program over the next several months to include additional courses by March 31, 2015.

**Management Comments and OIG Analysis**

We agree that the steps CBP is taking, and plans to take, begin to satisfy this recommendation. This recommendation will remain open and resolved until CBP provides supporting documentation that all planned corrective actions are completed.

## Appendix A
## Objectives, 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*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objective of our audit was to determine whether CBP has effectively managed the implementation of RFID technology. Specifically, we determined whether CBP has accomplished the following:

- Developed adequate policies and procedures to ensure the confidentiality, integrity, and availability of data contained on RFID tags, readers, and databases.

- Implemented effective security controls on its RFID devices to protect the sensitive data collected, processed, and generated.

- Developed effective policies and procedures to protect the PII collected by and stored on the RFID system.

- Complied with applicable DHS information security program requirements on RFID systems.

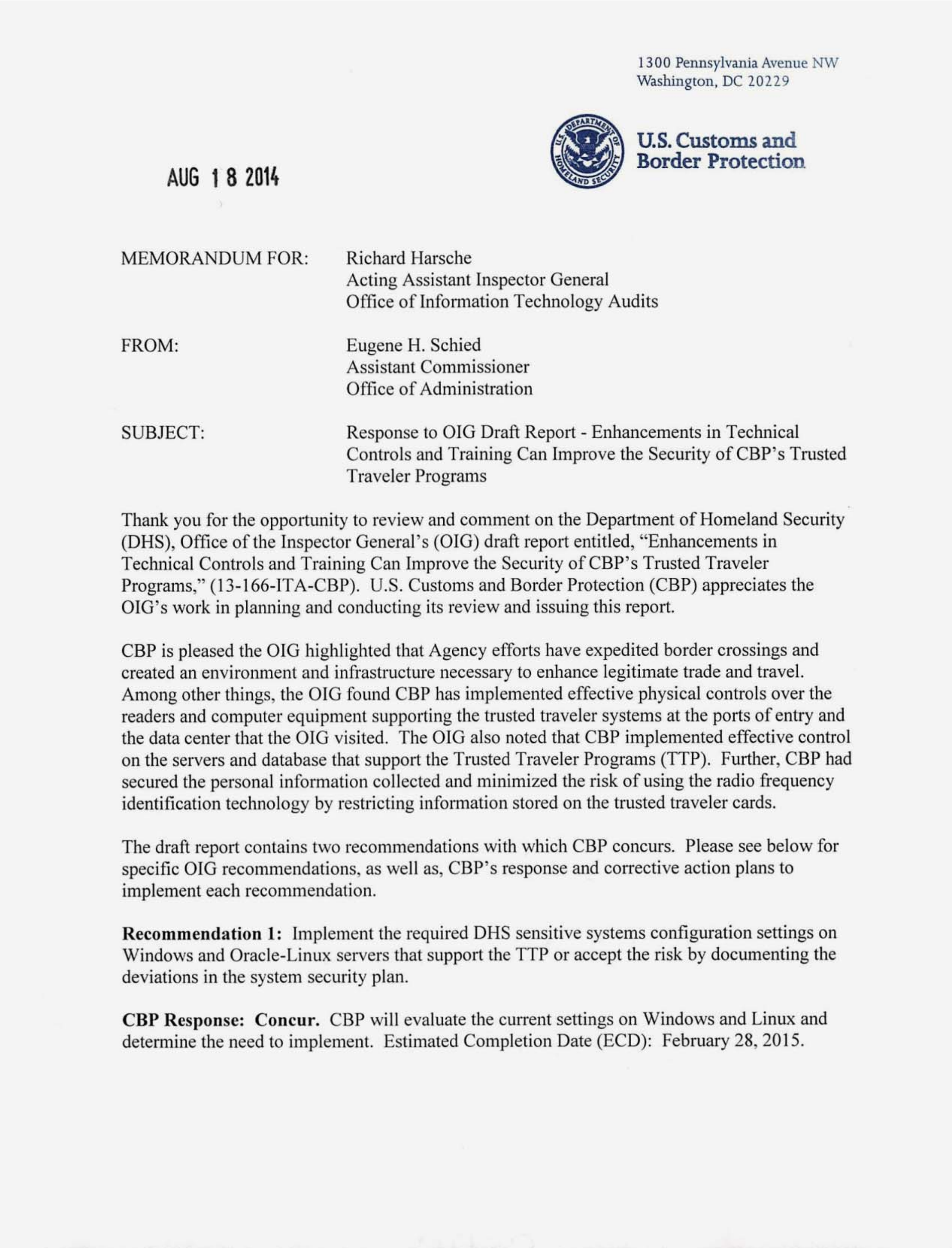
Our audit focused on CBP's use and management of RFID technology for land border management in compliance with applicable criteria and requirements outlined in the *DHS 4300A Sensitive Systems Handbook* (July 2012), *DHS 4300A Sensitive Systems Policy* (May 2013), *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* (March 2012), DHS Baseline Configuration Guidance, and National Institute of Standards and Technology Special Publication 800-98, *Guidelines for Securing RFID Systems* (April 2007), and Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013). We interviewed selected program officials and technical staff to discuss the TTP, technical testing, and any privacy incidents involving RFID.

We conducted our work at the program level and visited land border crossings in Buffalo, New York, and Blaine and Lynden, Washington, on the Northern border, and Calexico, Otay Mesa, and San Ysidro, California, on the Southern border. We visited the

Government Test Lane Facility in Virginia to obtain an overview of the RFID lanes and test our equipment. We performed technical testing to check security controls, identify known security vulnerabilities, and evaluate whether CBP configures its RFID devices in accordance with applicable policies and standards. We conducted vulnerability assessments and analysis using Tenable Nessus and Application Detective on supporting servers and databases that support the TTP.

We conducted this performance audit between November 2013 and March 2014 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
## Management Comments to the Draft Report



1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and
Border Protection

AUG 1 8 2014

MEMORANDUM FOR: Richard Harsche
Acting Assistant Inspector General
Office of Information Technology Audits

FROM: Eugene H. Schied
Assistant Commissioner
Office of Administration

SUBJECT: Response to OIG Draft Report - Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs

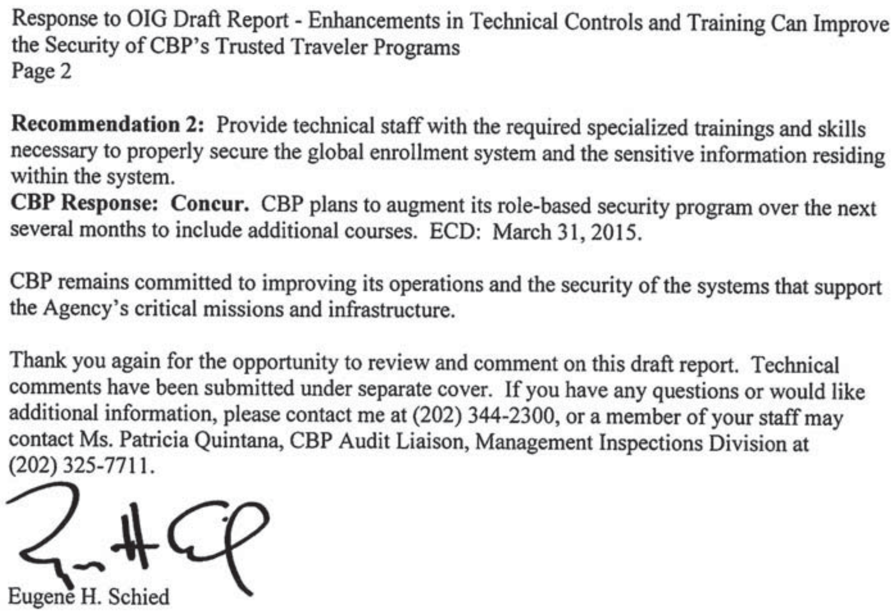
Thank you for the opportunity to review and comment on the Department of Homeland Security (DHS), Office of the Inspector General's (OIG) draft report entitled, "Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs," (13-166-ITA-CBP). U.S. Customs and Border Protection (CBP) appreciates the OIG's work in planning and conducting its review and issuing this report.

CBP is pleased the OIG highlighted that Agency efforts have expedited border crossings and created an environment and infrastructure necessary to enhance legitimate trade and travel. Among other things, the OIG found CBP has implemented effective physical controls over the readers and computer equipment supporting the trusted traveler systems at the ports of entry and the data center that the OIG visited. The OIG also noted that CBP implemented effective control on the servers and database that support the Trusted Traveler Programs (TTP). Further, CBP had secured the personal information collected and minimized the risk of using the radio frequency identification technology by restricting information stored on the trusted traveler cards.

The draft report contains two recommendations with which CBP concurs. Please see below for specific OIG recommendations, as well as, CBP's response and corrective action plans to implement each recommendation.

**Recommendation 1:** Implement the required DHS sensitive systems configuration settings on Windows and Oracle-Linux servers that support the TTP or accept the risk by documenting the deviations in the system security plan.

**CBP Response: Concur.** CBP will evaluate the current settings on Windows and Linux and determine the need to implement. Estimated Completion Date (ECD): February 28, 2015.



Response to OIG Draft Report - Enhancements in Technical Controls and Training Can Improve the Security of CBP's Trusted Traveler Programs
Page 2

**Recommendation 2:** Provide technical staff with the required specialized trainings and skills necessary to properly secure the global enrollment system and the sensitive information residing within the system.
**CBP Response: Concur.** CBP plans to augment its role-based security program over the next several months to include additional courses. ECD: March 31, 2015.

CBP remains committed to improving its operations and the security of the systems that support the Agency's critical missions and infrastructure.

Thank you again for the opportunity to review and comment on this draft report. Technical comments have been submitted under separate cover. If you have any questions or would like additional information, please contact me at (202) 344-2300, or a member of your staff may contact Ms. Patricia Quintana, CBP Audit Liaison, Management Inspections Division at (202) 325-7711.

Eugene H. Schied

# Appendix C
# Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Shannon E. Frenyea, Senior Program Analyst
Thomas Rohrback, Senior IT Specialist
Megan Ryno, Program Analyst
Referencer, Philip Greene

## Appendix D
## Report Distribution

**Department of Homeland**

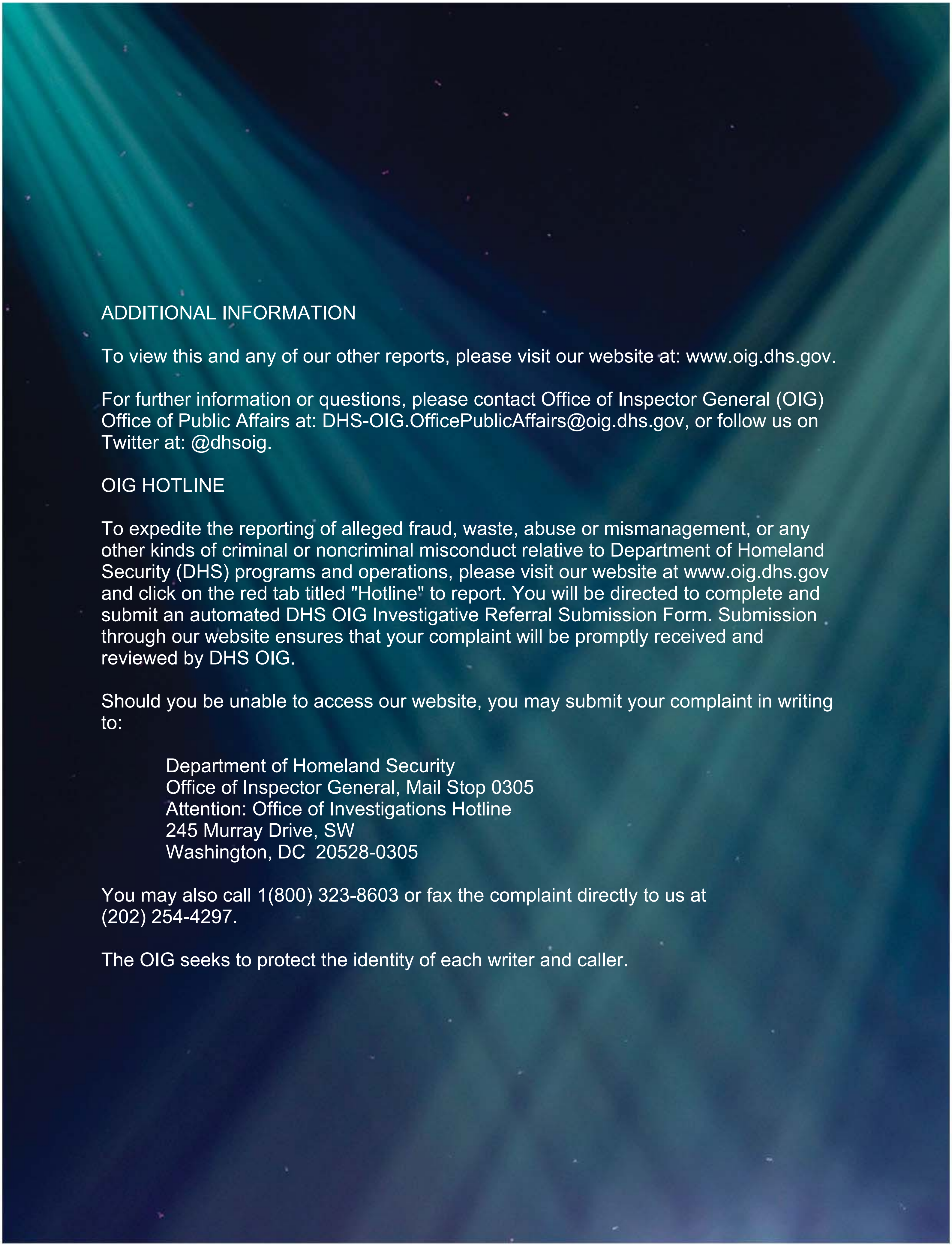
Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CBP Audit Liaison
Chief Privacy Officer
Commissioner, CBP
Assistant Commissioner and Chief Information Officer, CBP
Chief Information Security Officer, CBP
Assistant Commissioner, Office of Field Operations, CBP

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate



ADDITIONAL INFORMATION

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 (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: @dhsoig.

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

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

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.