

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

DHS Must Address Significant Security Vulnerabilities Prior To TWIC Implementation (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-06-47

July 2006



Homeland
Security

July 7, 2006

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) 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 by our office as part of our DHS oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report addresses our assessment of the adequacy of security controls implemented for the systems supporting the Transportation Worker Identification Credential (TWIC) program prototype. It is based on direct observations, security vulnerability assessments, and an analysis of applicable TWIC documents. We obtained additional supporting information through interviews with employees and officials in the TWIC Program Office and the Transportation Security Administration's (TSA) Office of the Chief Information Officer (OCIO), as well as personnel located at the [REDACTED]; TWIC contractor facilities; TSA's [REDACTED] Operations Center; TSA's Screening Gateway; and U.S. Customs and Immigration Services' (USCIS) card production facility. This report also includes an evaluation of the TWIC prototype systems against the Federal Information Security Management Act (FISMA) requirements.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	8
Security Vulnerabilities Jeopardize TWIC Program Implementation.....	8
Additional TWIC Program and Security-Related Concerns	12
Recommendations	16
Management Comments and OIG Analysis	16


Appendices

Appendix A: Purpose, Scope, and Methodology	19
Appendix B: Management’s Response.....	22
Appendix C: TWIC System Layout.....	26
Appendix D: Instances of Security Vulnerabilities Detected By Location & System.....	27
Appendix E: Number of Security Vulnerabilities Identified By Location	28
Appendix F: Summary of Significant Security Vulnerabilities Identified and Potential Threats.....	29
Appendix G: Major Contributors to this Report	31
Appendix H: Report Distribution.....	31

Abbreviations

CIO	Chief Information Officer
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ID	Identification
IDMS	Identification Management System
ISS	Internet Security Systems
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
POA&M	Plan of Action and Milestones
<hr/>	
ST&E	Security Testing and Evaluation
<hr/>	

Table of Contents/Abbreviations



TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	U. S. Coast Guard
USCIS	U. S. Customs and Immigration Services

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the information security management and access controls implemented for the systems supporting the Transportation Worker Identification Credential (TWIC) program prototype phase. TWIC is an important part of TSA's efforts to improve the security of the nation's transportation system. It establishes a system-wide, common credential that may be universally accepted across all transportation modes, for all personnel requiring unescorted physical access to secure areas and logical access to information and systems within transportation facilities.

Our audit objective was to determine whether adequate system security controls have been implemented on TWIC systems to protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. Our audit work was based on direct observations; vulnerability and wireless system security scans; and an analysis of applicable TWIC documents. In addition, we interviewed management officials and security personnel located at the TWIC Program Office; TSA's Office of Chief Information Officer (OCIO); [REDACTED]; TWIC contractor's main [REDACTED] offices and datacenter; [REDACTED] Operations Center; Screening Gateway; and, the USCIS facility. Fieldwork was conducted from November 2005 through March 2006.

We determined that significant security vulnerabilities existed relative to the TWIC prototype systems, documentation, and program management. Furthermore, we are raising a number of additional program and security-related concerns that we identified during the course of our fieldwork. Due to the number and significance of the weaknesses identified, TWIC prototype systems are vulnerable to various internal and external security threats.

The security related issues identified may threaten the confidentiality, integrity, and availability of sensitive TWIC data. Until remedied, the significant security weaknesses jeopardize the certification and accreditation of the systems prior to full implementation of the TWIC program.

We are recommending that the Assistant Secretary for TSA direct the Assistant Administrator and Chief Information Officer (CIO), Operational Process and Technology, to establish a formal structure for the oversight and management of security for the TWIC program. An effective security management structure, the timely remediation of system and configuration management vulnerabilities, and the revision and development of necessary security documentation and standard operating procedures are essential to attain a robust security posture for the TWIC program prior to full implementation. In response to our draft report, TSA concurred with and has already taken steps to implement the recommendations.

Background

The mission of TSA is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. The TWIC program is being developed in response to threats and vulnerabilities identified in our nation's transportation system, in accordance with the requirements of the *Aviation and Transportation Security Act of 2001* (Public Law 107-71),¹ and the *Maritime Transportation Security Act of 2002* (Public Law 107-295),² as well as other statutory mandates. TSA and the United States Coast Guard (USCG) are partnering to issue a joint regulation that will outline various requirements and applicability for TWIC to address the threats and vulnerabilities that have been detected in our nation's transportation system. The regulation will seek to achieve the security benefits that Congress expected when

¹ The *Aviation and Transportation Security Act* authorizes TSA to assess security threats to the transportation system and develop policies and programs to counter those threats, including background checks for transportation workers with unescorted access to secure areas.

² The *Maritime Transportation Security Act* requires increased security of the U. S. maritime domain, specifically ports, facilities, and vessels, including a requirement for the completion of background checks and issuance of biometric transportation security cards for all maritime personnel requiring access to secured areas of facilities and vessels. As the implementing agency of MTSA, the USCG implemented federal regulations to clearly outline the intent of the law and provide specific requirements to ensure compliance with the law. 33 C.F.R. §§ 101.100 *et seq.*

the *Maritime Transportation Security Act* was enacted without imposing unnecessary burdens on the regulated community. Initially, only seaports and airports will be covered by the regulation being developed.

The TWIC is a secure identification card that is about the size of a credit card. This card can be used by transportation workers³ for unescorted physical access⁴ to secure areas and logical (cyber) access to information and systems within transportation facilities. The TWIC verifies a transportation worker's identity by linking a person's claimed identity and background information to that person's stored physical characteristics. Figure 1 contains a TWIC prototype card example.

Figure 1

Source: [REDACTED] TWIC Program Brief

³ A transportation worker is defined as any owner, operator, or contractor assisting or engaged in the movement of cargo, sale of goods within a transportation facility, or the development and maintenance of information technology (IT) systems. Any person within the transportation industry whose job may require unescorted access to a secure area or transportation industry site might be eligible for a TWIC card.

⁴ Unescorted access is the permission granted to an individual to enter a facility or computer system without requiring an authorized individual to accompany them.

TWIC Program Objectives

The TWIC program is to design and field a common credential or standard for all transportation workers across the U.S. who require unescorted access to secure areas at seaport, airport, rail, pipeline, trucking, and other mass-transit facilities. A TWIC card is to serve as an integrated credential-based identity management system for all those transportation workers. The requirements for this credentialing include the verification of each TWIC holder's identity, a successful background/threat assessment, and the use of biometric technology to link each credential to its rightful holder.

The TWIC program goals are to: (1) improve security by reducing risks associated with fraudulent or altered credentials by using biometrics to positively match an individual to the credential; (2) enhance commerce by reducing the need for multiple credentials/vetting and leverage current security investments; and (3) protect personal privacy by collecting minimal personal data stored on a secure system and network. Additionally, the TWIC program is to serve as a model in meeting the mandatory requirements for a government-wide standard for a secure and reliable form of identification issued by the federal government to its employees, including contractor employees, as outlined in Homeland Security Presidential Directive 12 (HSPD-12).⁵

TWIC Program Phases

The TWIC program consists of five phases:

TWIC Program	
Phase I	Planning
Phase II	Technology Evaluation
Phase III	Prototype
Phase IV	Implementation
Phase V	Operations and Maintenance

⁵ HSPD-12, the Policy for a Common Identification Standard for Federal Employees and Contractors, mandated by the President, established a government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees) to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

Currently, the TWIC program is in a sustainment period, which is the time period between prototype and implementation. The scope of our audit was focused on the systems supporting the prototype, Phase III of the program, which began November 17, 2004 and ended June 30, 2005. Transportation worker and facility participation in the prototype was on a completely voluntary basis.⁶

The goals of the prototype system were to:

- Assess the performance of the TWIC identity management architecture and business processes.
- Assess performance of the TWIC credential as an access control tool.
- Assess the readiness of the TWIC system to be implemented.

Additionally, the “prototype phase” tested the conceptual TWIC identity management and business processes, which included enrolling workers, conducting security threat assessments, issuing TWICs, and daily usage of the credential. A TWIC Prototype Report, compiled by the TWIC contractor and issued August 29, 2005, documents the prototype testing results, lessons learned, and recommendations to be addressed prior to and during the full implementation of the TWIC program.

A major challenge during the prototype phase emerged because some participating ports did not have an infrastructure to support the program. Each facility must have an infrastructure to support the use of the TWIC card in order to participate in the program. Originally, 37 facilities were expected to participate during the prototype phase. Nine of the 37 sites opted out of the prototype due to the unavailability of an infrastructure to support card testing. Many of the remaining participating transportation facilities required installation of some physical access components; installing this infrastructure in places where none existed caused significant programmatic delays and increased costs.⁷ According to the TWIC Prototype Report, not only was the number of

⁶ Participants consisted of a broad array of transportation workers, such as truckers, longshoremen, and container terminal and airport personnel.

⁷ The 28 prototype site locations included the following: 15 ports, 2 airports, and 11 other transportation facilities including train stations, truck stops, and maritime exchanges.

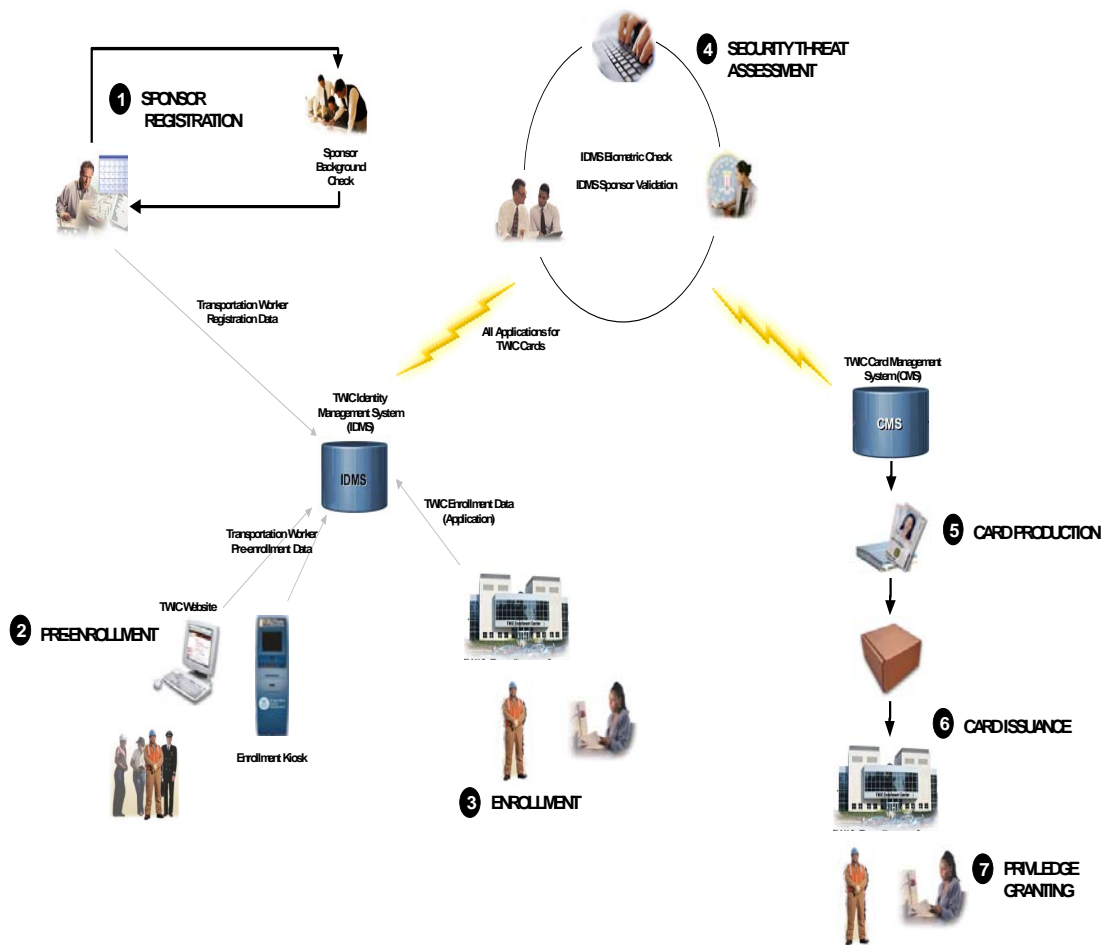
participating facilities lower than expected, the number of TWIC cards issued was also much lower than expected.

TWIC Process Overview

Figure 2 depicts the overall business processes associated with obtaining a TWIC card.

Figure 2

TWIC Overview



Source: [REDACTED]

The following processes are associated with the numbers in the overview in Figure 2:

1. **Sponsorship** – The process of confirming that an individual has a legitimate need for a TWIC.
2. **Pre-enrollment** – The process prior to enrollment for acquiring a TWIC where an individual provides [REDACTED] data on-line.⁸
3. **Enrollment** – The process of [REDACTED] information.
4. **Security Threat Assessment** - The process of checking various databases looking for a name or biometric match to determine a person’s eligibility to access secure areas and automated systems.⁹
5. **Card Production** – The manufacturing process performed to personalize a card; includes extracting data from databases, encoding the data, and printing the data onto a card.
6. **Card Issuance** – The process conducted at an enrollment center to validate an individual’s identity (matching a live biometric capture to the biometric data stored on the card), enable the card for use, and present the card to the authorized user.
7. **Privilege Granting** – The process of validating the status and possession of the TWIC and providing access rights within the TWIC infrastructure to each transportation facility or network that a transportation worker needs access to for the performance of their day-to-day duties.¹⁰

⁸ This [REDACTED] data is then used along with the information captured during an enrollment appointment to run the necessary security threat checks, encode, print, and issue a TWIC.

⁹ During the prototype testing, only name-based security threat assessments were done for most TWIC card applicants, with the exception of those workers applying for a TWIC card in Florida. Florida statute sets minimum statewide seaport security standards and requires that individuals accessing Florida’s active seaports undergo an annual criminal history records check . The criminal history background check was done by the State of Florida in accordance with its statutory authority, which included a requirement that all applicants be screened against the Federal Bureau of Investigation’s Integrated Automated Fingerprint Identification System.

¹⁰ TSA does not have control over who is granted access privileges at the ports. TSA only provides the security threat assessment for a worker, who may then be authorized for a TWIC card based on the results of the assessment. Local authorities decide which individuals get a TWIC card and where they have access based on the access privileges granted by the individual facility.

Card revocation and reissuance is also part of TWIC card processing too.¹¹ However, these processes, which were not fully established prior to testing, were not part of the prototype assessment.

Three datacenters are involved during TWIC card processing and production:

- Production Datacenter – Identification Management System (IDMS),¹² Card Management System,¹³ and other supporting systems (-----).¹⁴
- TSA’s ----- Operations Center – Name-based security threat assessments processed through TSA’s Screening Gateway in -----.
- USCIS’ Card Production Facility (-----) – Card production and printing.

Appendix C documents the TWIC Systems Layout and the specific data collected to support TWIC processing.

Results of Audit

Security Vulnerabilities Jeopardize TWIC Program Implementation

TSA faces numerous challenges ensuring that security vulnerabilities are remedied and key program policies, regulatory processes, and other work are completed to support system certification and accreditation and the full implementation of the TWIC program. The existing vulnerabilities can compromise the confidentiality, integrity, and availability of sensitive TWIC data. Further, beginning with maritime operations, as it moves forward

¹¹ Card revocation and reissuance are the processes involved in permanently ending the operational period of a card because the card has been reported as lost or stolen, or the cardholder has been identified as a threat to security.

¹² IDMS stores TWIC applicants’ enrollment records. -----

-----.

¹³ The Card Management System provides information on the status of cards throughout the TWIC system. Card information will be kept from the moment it is received into inventory to the time it is destroyed.

¹⁴ -----
-----.

with the implementation of the TWIC program, TSA faces other security-related issues, including resolving stakeholder concerns regarding the depth of security threat assessments, retaining and protecting individuals' sensitive information, and obtaining funding for full implementation at all transportation facilities.

We evaluated the TWIC program procedures and security requirements in place during the prototype phase. We also conducted system security vulnerability assessments on a variety of systems supporting the TWIC program prototype phase. We chose the specific systems tested to ensure coverage at all points in the TWIC prototype process. Prototype systems tested included the following: enrollment workstations in [REDACTED], and [REDACTED]; the contractor's datacenter databases and servers in [REDACTED]; and, the workstations and printers at the card production facility in [REDACTED]. Additionally, we conducted tests to detect [REDACTED] at the [REDACTED] [REDACTED] and the TWIC contractor's datacenter.

Significant System Security Vulnerabilities Identified

Over [REDACTED] instances of security vulnerabilities were detected during the security vulnerability assessments of the TWIC prototype systems.¹⁵ Excluding duplicate instances of vulnerabilities and false/positives, a total of [REDACTED] unique vulnerabilities were identified across the different sites assessed. Of those [REDACTED], [REDACTED] were classified as "high" risk vulnerabilities, and [REDACTED] were classified as "medium" risk vulnerabilities. The remaining vulnerabilities identified ([REDACTED]) were classified as "low" risk vulnerabilities. Appendix D lists the number of instances of vulnerabilities by location and system. Appendix E lists the number of high, medium, and low vulnerabilities identified.

Vulnerabilities identified were related to [REDACTED] [REDACTED] [REDACTED]. Specific examples include:

¹⁵ The number of instances includes the [REDACTED] detected during the OCIO's testing of the systems at TSA's Screening Gateway in [REDACTED].

¹⁶ [REDACTED].

¹⁷ Perimeter devices include routers, switches, and firewalls.

-
- [REDACTED] 18
 - [REDACTED]
 - [REDACTED]
 - [REDACTED] 19
 - [REDACTED]

Contractor IT services and operations must adhere to DHS IT security policies. These vulnerabilities may exist in part because a test environment was not developed prior to operations due to limited funding available for the prototype. These vulnerabilities were deemed to be significant since the prototype systems were tested at the participating sites using [REDACTED]. Furthermore, during the sustainment period, this type of data is still being collected and retained on the systems tested, which [REDACTED]. Appendix F contains a summary of the high vulnerabilities identified and the potential system security threats that exist if the vulnerabilities are not remedied.

We discussed our findings with the TWIC Program Office and contractor personnel at each of the audit locations assessed. We also provided the site system administrators with the technical vulnerability reports so that they could begin addressing the vulnerabilities identified. Additionally, we provided TSA’s Assistant Administrator and CIO, Operational Process and Technology, with the test results from each of the locations assessed so that a plan of action could be developed to address vulnerabilities identified that cannot not be remedied under the current funding restraints.

FISMA Issues

We determined whether systems, databases, and networks supporting the TWIC prototype complied with FISMA requirements, in addition to our system security vulnerability scans. FISMA requires an annual evaluation of agency information programs and systems, as well as an assessment of related security policies and procedures. An agency’s security program should provide security for the information and the

18 [REDACTED]
[REDACTED]

19 [REDACTED]
[REDACTED]

information systems that support the operations and assets of the agency, including those managed by another agency, contractor, or other source.

Based upon our analysis of the security documentation for the systems supporting the TWIC program, we identified the following deficiencies as they directly relate to FISMA:

- [Redacted]
- [Redacted]
- The Plan of Action and Milestones (POA&M) for TWIC is incomplete. Not all vulnerabilities have been included in the POA&M, nor have resources to address the vulnerabilities that are documented in the POA&M been determined. Furthermore, the milestone dates and responsible points of contact need to be updated.
- The Privacy Impact Assessment, dated November 5, 2004, is outdated and does not reflect accurately how the prototype was implemented and tested or what policies need to be in effect prior to implementation.
- Systems contingency plans have not been approved or tested.
- System and database administrators have not received specialized security awareness training.

The DHS 4300A Sensitive Systems Handbook requires that component CIOs establish and oversee the IT security program within their organizational component.²⁰ Specifically, component CIOs must ensure that an ISSM has been appointed. Information Systems Security Managers (ISSM) play a critical role in ensuring that the DHS IT security program is both implemented and maintained throughout the component. CIOs should also make certain that the ISSM and Information Systems Security Officer (ISSO) work closely with program officials to ensure a complete understanding of risks, especially increased system security risks, so that they are documented and managed. DHS IT policy outlines the structure and foundation for a secure DHS systems environment by focusing on the management and mitigation of inherent IT system security risks.

Overall, based on our vulnerability assessments and observations, we concluded that the greatest risks to system security and the privacy of TWIC data stem from

[REDACTED]

Ultimately, TWIC Program Office officials and the system owner are responsible for the successful operation of the IT systems within their program area and are accountable for the security of the systems and programs under their control. In addition, they are accountable for the security of the information systems in compliance with FISMA. A coordinated effort is needed between the TWIC Program Office and TSA's OCIO to strengthen security management controls and achieve the long-term vision of the TWIC program.

Additional TWIC Program and Security-Related Issues

TSA is developing TWIC to improve overall security at the nation's transportation facilities. In auditing TWIC, we identified a number of additional program and security issues that need to be considered prior to full implementation of the TWIC program.

²⁰ This handbook serves as a foundation for the components within DHS to develop and implement their IT security programs.

These concerns, regarding the security and privacy of the sensitive data being maintained, arose during discussions with TWIC program management officials, meetings with the TWIC contractor, and a review of the Privacy Impact Assessment and Lessons Learned in the TWIC Prototype Report. Issues include the following:

- The rules of behavior need to clearly delineate responsibilities and the expected behavior of all individuals with access to systems supporting TWIC. Assignment and segregation of system responsibilities must be clearly defined and documented for all DHS IT systems, including TWIC.

- [Redacted]

- [Redacted]

- [Redacted]

²¹ [Redacted]

-
- The TWIC Program Office has not established procedures for periodically re-running threat assessments on all individuals granted a TWIC card. Such procedures are needed to ensure that TWIC cardholders do not pose any security threats, such as having been placed on a “hotlist” after being granted a TWIC card.²²
 - With the exception of participating sites in Florida, which require a criminal history assessment based on an individual’s biographic and biometric information, the prototype testing did not address criminal history checks or the biometric vetting process prior to granting an individual a TWIC card. Running Federal Bureau of Investigation criminal history checks on TWIC applicants may be needed to ensure that TWIC cardholders do not pose security threats to the nation’s transportation system.
 - The TWIC program does not currently have a records retention schedule; therefore, TSA has not disposed of individuals’ applications or other information collected during the prototype. The administrative, technical, and physical controls for safeguarding TWIC records stored are to be documented in the Privacy Impact Assessment. TSA is working to develop a retention schedule for both prototype and full-scale implementation of TWIC for approval by the National Archives and Records Administration.

- [REDACTED]

²² [REDACTED]

²³ A Trusted Agent is a federal or state government employee, non-federal site employee, or a contractor who is granted the authority by the federal government to perform and administer the TWIC enrollment process along with issue TWICs.

[Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

We discussed these issues with TWIC program officials and they agreed these concerns needed to be addressed prior to full-scale TWIC implementation.

24 [Redacted]

Recommendations

Prior to full implementation of the TWIC program, we recommend that the Assistant Secretary for TSA direct the Assistant Administrator and CIO, Operational Process and Technology to:

1. Ensure the ISSM works closely with TWIC Program Office officials to ensure a complete understanding of the severity of the security risks that currently exist and help determine the funding and resources needed to remediate those risks.
2. Ensure that all system vulnerabilities related to [REDACTED].
3. Finalize system and security documentation, including the security plan, standard operating procedures, and user manuals.
4. Update the Privacy Impact Assessment to reflect the expectations for the protection, retention, confidentiality, integrity, and availability of sensitive TWIC data and the results of security threat assessments.
5. Update the POA&M to ensure that all vulnerabilities are included and a plan for remediating weaknesses is in place, and ensure that adequate funding for IT security is provided for systems.

Management Comments and OIG Analysis

TSA concurred with recommendation 1. Congress approved funding for TWIC, and TSA has been remediating the program weaknesses for the past several weeks. The Program Office meets at least weekly with the primary certifier from the ISSM office to continue remediation. The Program Office is in the process of determining the new cost, schedule, and performance requirements, and is working on required technical enhancements for the system so that the program is ready for production.

As a result, the Program Office will give the IT Security Office a justification memorandum requesting that all remediation on technical findings cease until the Program Office has finalized system enhancements. The Program Office will work with the contractor to ensure that all documentation is updated and in accordance with security policies and to have the system implemented and ready for Security Testing and Evaluation (ST&E). As part of this evaluation, TSA's CIO will review and update all documentation to ensure it is in alignment with the production system. The IT Security Office will work closely with the Program Office to ensure that all new technical implementations comply with TSA and DHS policies.

We accept TSA's response to work closely with the ISSM office, IT Security Office, and the CIO to determine the funding and resources needed to remediate the technical weaknesses, and to cease remediation of those vulnerabilities until system enhancements have been finalized and comply with TSA and DHS policies.

TSA concurred with recommendation 2. TSA acknowledged these vulnerabilities and they will be addressed when completing the technical enhancements to the TWIC prototype system, conducting the ST&E, and mitigating any findings.

We accept TSA's response to address these vulnerabilities when implementing the technical enhancements and the ST&E for TWIC.

TSA concurred with recommendation 3. Work is on going to reflect the changes in the TWIC technical enhancements. All system and security documentation, including the security plan, standard operating procedures, and user manuals, will be fully updated at the conclusion of the work.

We accept TSA's response to finalize all system and security documentation at the conclusion of work on the technical enhancements.

TSA concurred with recommendation 4. A revised Privacy Impact Assessment has been generated for the TWIC Notice of Proposed Rulemaking and has been submitted for review and signature within TSA. The Privacy Impact Assessment will be published on the DHS website concurrently with the publication of the Plan of Action and the Notice of the Proposed Rule Making. When TSA publishes a final TWIC rule, the final Privacy Impact Assessment will also be published.

We accept TSA's response in regard to updating the Privacy Impact Assessment.

TSA concurred with recommendation 5. Funding has been allocated within the program budget to complete system changes and the certification and accreditation. Long lead-time items, such as the computer hardware, will be procured and assembled under the Office of Transportation, Threat, and Credentialing operation at ----- . After setup and installation of the software, the system will be operationally tested, and certification and accreditation performed. The POA&M will be updated after the completion of the ST&E of the production system.

We accept TSA's response in regard to funding the remediation of vulnerabilities and updating the POA&M.

Purpose, Scope, and Methodology

The overall objective of this audit was to determine whether adequate system security controls have been implemented on TWIC prototype systems to effectively protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, we determined whether: (1) adequate management and internal controls have been developed and implemented to protect the sensitive and biometric data contained on TWIC systems; (2) adequate access controls have been implemented on TWIC systems to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction; and (3) TWIC prototype systems comply with FISMA requirements.

We analyzed documents provided by the TWIC Program Office and contractor personnel to identify that adequate management and internal controls have been developed and implemented to protect the sensitive and biometric data contained on TWIC systems. These materials included: the TWIC Prototype Report; Privacy Impact Assessment; Prototype Phase III Requirements document; Phase III Standard Operating Procedures; Phase III Transportation Worker User Manual, Phase III Operations/System Administration Manual, Inter-Agency Agreement between TSA and USCIS; and, pamphlet information on the TWIC Program. We also reviewed DHS, National Institute of Standards and Technology (NIST), and Defense Information Systems Industry policies and procedures; HSPD-12; the Aviation and Transportation Security Act; the Maritime Transportation Security Act; the Federal Information Systems Controls Audit Manual; and Office of Management and Budget requirements.

We interviewed employees and officials regarding prototype processes and procedures with the TWIC Program Office and TSA's OCIO, as well as security and system administrators located at the [REDACTED]; TWIC contractor facilities in [REDACTED] and [REDACTED]; TSA's [REDACTED] Operations Center; TSA's Screening Gateway in [REDACTED]; and the USCIS [REDACTED] facility. To assess the TWIC card issuance

processes, audit team members, sponsored by the TWIC contractor, enrolled and were granted TWIC cards.

During our audit, we conducted system security vulnerability assessments to determine whether adequate access controls have been implemented on TWIC systems. Assessments were completed at the two enrollment centers that were still actively processing individuals for TWIC cards – the [REDACTED] and the contractor’s [REDACTED] enrollment center. We also assessed security controls for the systems supporting TWIC operations located at the contractor’s production datacenter in [REDACTED] and at the USCIS card production facility in [REDACTED]. Additionally, we tested for [REDACTED] at the [REDACTED] and the TWIC contractor’s datacenter. Furthermore, we obtained and analyzed the results of system security vulnerability assessments conducted by TSA’s OCIO at the Screening Gateway in [REDACTED] in February 2006. We did not evaluate the security of the systems at TSA’s [REDACTED] Operations Center, as there is no direct connection from the systems supporting the TWIC program to the Operations Center; all traffic going to the Operations Center must first go through TSA’s Screening Gateway at [REDACTED].

We used Internet Security Systems’ (ISS) Internet Scanner to conduct the system security vulnerability assessments at all the audit locations visited.²⁵ TSA’s OCIO also used ISS’ Internet Scanner to test for system security vulnerabilities at the Screening Gateway in [REDACTED]. We used ISS’ Database Scanner to test the TWIC databases that are part of the IDMS at the contractor’s datacenter.²⁶ [REDACTED] was used to test [REDACTED] at the contractor’s datacenter and at the USCIS facility.²⁷ We used [REDACTED] to test for [REDACTED].

²⁵ ISS’ Internet Scanner provides an automated vulnerability assessment across servers, desktops, operating systems, routers/switches, firewalls, and applications to identify potential risks to an organization’s network.

²⁶ ISS’ Database Scanner is a database vulnerability scanner for Microsoft Structured Query Language (SQL) Server, Sybase, and Oracle databases.

²⁷ [REDACTED]

_____ at the _____ and the TWIC contractor's datacenter.²⁸

To determine whether TWIC prototype systems complied with the FISMA requirements, we reviewed FISMA requirements as well as DHS and NIST guidance. We also analyzed documents provided by the TWIC Program Office, ISSO, and contractor personnel, including: the Phase III System Security Plan, Preliminary Phase III Risk Assessment, NIST 800-26 Self-Assessment, POA&M matrix, Trusted Agent Training Manual, and the contingency/disaster recovery plan. In addition, we interviewed contractor personnel and the ISSO regarding the status of the certification and accreditation of TWIC systems, security awareness training, and specialized security training.

We conducted fieldwork at the TWIC Program Office in _____, and the following locations: the _____; _____; _____ and _____; and, _____. Audit work was completed from November 2005 through March 2006 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix G.

The principal OIG points of contact for the audit are Frank Deffer, Assistant Inspector General for IT Audit, at (202) 254-4100, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.

²⁸ _____

_____.

Appendix B
Management's Response

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

MAY 11 2006



Transportation
Security
Administration

INFORMATION

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security

FROM: Robert D. Jamison *Robert D. Jamison*
Deputy Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response
Department of Homeland Security (DHS) Office of Inspector
General (OIG) Draft Report, OIG-06-XX
"DHS Must Address Significant Security Vulnerabilities
Prior to TWIC Implementation," March 2006

Purpose

This memorandum is the TSA formal agency response to the DHS Office of Inspector General (OIG) Draft Report "DHS Must Address Significant Security Vulnerabilities Prior to TWIC Implementation," OIG-06-XX, March 2006. TSA thanks the DHS OIG for their work in planning, conducting, and issuing this study. The recommendations identified in this review will help facilitate the nationwide implementation of a common Transportation Worker Identification Credentialing (TWIC) system for increased security throughout the nation.

Background

The mission of the TWIC program is to field a common credential or standard for all transportation workers requiring unescorted physical and logical access to secure areas of the national transportation system. In achieving the TWIC Program's mission, three overarching goals must also be achieved:

- Improving security;
- Enhancing commerce; and,
- Protecting privacy.

TSA developed the TWIC program, beginning in December 2001, to review, identify, and mitigate deficiencies in the transportation system to ensure that only properly cleared and authorized personnel could gain access to secure areas of the nation's transportation system. A plan was devised soon thereafter to develop the TWIC in four phases: Phase I - Planning, Phase II - Technical Evaluation, Phase III - Prototype, and Phase IV - Production.

Appendix B
Management's Response

2

The TWIC Prototype phase was completed on June 30, 2005. Each component of the TWIC prototype system was evaluated as having met program requirements and is either ready, or conditionally ready, for implementation. Three components - sponsorship (eligibility), privilege granting, and, revocation - are evaluated as "conditionally ready" for implementation and were given this rating because the controlled, volunteer-oriented environment of the prototype did not allow testing under implementation conditions. Although the risk of encountering significant implementation problems in these areas is considered minimal, a gap analysis is underway to identify factors to enhance the system for the full scale production environment. After the prototype design and development efforts concluded, the program continued to provide enrollment and card issuance services until March 31, 2006, sustaining the three ports in the area.

TSA and the U.S. Coast Guard have prepared a Notice of Proposed Rulemaking (NPRM) that proposes standards for national implementation of TWIC, based on the information gathered during the prototype phase. The NPRM has been approved by Secretary Chertoff. We anticipate it will be released shortly. When the NPRM is completed, we will provide your office with a copy.

Discussion

The program continues production planning by focusing on lessons learned from the Prototype phase to further refine requirements and is also assessing enhancements needed to fully comply with Federal Information Processing Standards 201 and current Personal Identity Verification standards. It was acknowledged in discussions with the OIG that a prototype system will always need further enhancements and additional work to ready it for production. In finalizing the proposed rule for the TWIC program, all key program policies will be completed and system vulnerabilities in protecting privacy data will be addressed.

Our specific approaches to each of your recommendations are reflected in the responses to the report. The findings from the prototype effort along with your input are being used to improve the security and operation of the final TWIC production system. TWIC will be implemented on a fully certified and accredited system.

Attachment

Appendix B
Management's Response

Transportation Security Administration's (TSA) Response
Department of Homeland Security (DHS) Office of Inspector
General (OIG) Draft Report, OIG-06-XX
"DHS Must Address Significant Security Vulnerabilities
Prior to TWIC Implementation," March 2006

Recommendation 1: Ensure the Information System Security Manager (ISSM) works closely with TWIC Program Office officials to ensure a complete understanding of the severity of the security risks that currently exist and help determine the funding and resources needed to remediate those risks.

TSA Concur: Congress approved funding for TWIC and TSA has been remediating the program for the past several weeks. The program team meets at least weekly with the primary certifier from the ISSM office to continue remediation. The program office is in the process of determining the new cost, schedule, and performance requirements for the system. The program office is also working on required technical enhancements so that the program will be ready for production.

As a result, the program office will give the Information Technology (IT) Security Office a justification memorandum requesting that all remediation on technical findings cease until the program office has finalized the system enhancements. The program office will work with the contractor to ensure that all the documentation is updated and in accordance with security policies and plans to have the system implemented and ready for Security Testing and Evaluation (ST&E). As part of the ST&E process, the Chief Information Officer will review and update all documentation to ensure that it is in alignment with the production system. The IT Security Office will work closely with the program office to ensure that all new technical implementations comply with Transportation Security Administration and Department of Homeland Security policies.

Recommendation 2: Ensure that all system vulnerabilities related to default security settings and accounts and patch management are remedied.

TSA Concur: This is acknowledged and will be addressed when completing the technical enhancements to the prototype system, conducting the ST&E and mitigating any findings.

Recommendation 3: Finalize system and security documentation, including the security plan, standard operation procedures, and user manuals.

TSA Concur: This work is ongoing and will continue to reflect the changes in the technical enhancements. All system and security documentation, including the security plan, standard operation procedures and user manuals will be fully updated at the conclusion of the work.

Recommendation 4: Update the Privacy Impact Assessment to reflect the expectation for the protection, retention, confidentiality, integrity, and availability of sensitive TWIC data and the results of security threat assessments.

TSA Concur: A revised Privacy Impact Assessment has been generated for the TWIC Notice of Proposed Rulemaking and submitted for review and signature within TSA. This document addresses the protection, retention, confidentiality, integrity and availability of TWIC data and the results of security threat assessments. The Privacy Impact Assessment for the proposed rule will be published on the DHS website concurrently with the publication of the Plan of Action and the Notice of Proposed Rule Making. When TSA publishes a final TWIC rule, the final Privacy Impact Assessment will also be published.

Recommendation 5: Update the POA&M to ensure that all vulnerabilities are included and a plan for remediating weaknesses is in place, and ensure that adequate funding for IT security is provided for systems.

TSA Concur: Funding has been allocated within the program budget to complete system changes and complete certification and accreditation. Long lead time items such as the computer hardware will be procured and assembled under the Office of Transportation, Threat and Credentialing operation at [redacted]. After setup and installation of the software, the system will be operationally tested and Certification & Accreditation performed. Plan of Action & Milestones (POA&M) will be updated after Security Test and Evaluation of the production system is completed.

Appendix C
TWIC System Layout

Instances of Security Vulnerabilities Detected By Location & System

	High	Medium	Low	Total
	1	1	1	3
	1	1	1	3
	1	2	2	5
	2	2	1	5
	1	1	1	3
	1	1	1	3
	1	1	1	3
	1	1	1	3
Totals	10	10	10	30

*In addition to the above, which was based on our systems security vulnerability testing of the systems supporting the TWIC prototype, we obtained the results of the vulnerability testing conducted by TSA’s OCIO at the Screening Gateway in [REDACTED]. From our analysis of those results, we determined that there were [REDACTED] instances of security vulnerabilities identified on the systems in [REDACTED] that support the TWIC prototype.

Number of Security Vulnerabilities Identified By Location

	High	Medium	Low	Total
	1	1	1	3
	1	1	1	3
	2	2	2	6
	2	2	2	6
	1	1	1	3
	1	1	1	3
Totals	10	10	10	30

Appendix F
Summary of Significant Security Vulnerabilities Identified and Potential Threats

Appendix G
Major Contributors to this Report

Information Security Audit Division

Edward G. Coleman, Director
Barbara Bartuska, Audit Manager
Chelsea Pickens, Senior IT Auditor
Mike Horton, IT Specialist
Matthew Worner, Referencer

Advanced Technology Division

Jim Lantzy, Director
Karyn Higa, Information Assurance Computer Engineer (Space and Naval
Warfare Systems Command)

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary, Policy
CIO
Chief Information Security Officer
Assistant Administrator and CIO, Operational Process and Technology, TSA
Director and IT Security/Chief Information Security Officer, TSA
TWIC Program Director
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative and Intergovernmental Affairs
Director, Departmental Government Accountability Office/OIG Liaison
Director, Compliance and Oversight Program
TSA Audit Liaison
USCG Audit Liaison
USCIS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.