

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

US-VISIT System Security Management Needs Strengthening (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-06-16

December 2005



**Homeland
Security**

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 information security controls implemented on the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program. It is based on direct observations, security vulnerability assessments, an analysis of applicable security documents, a review of physical security controls, and interviews with employees and officials in the US-VISIT Program Office, U.S. Customs and Border Protection (CBP), and U.S. Immigration and Customs Enforcement (ICE). This report also includes an evaluation of US-VISIT 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.....	3
Results of Audit	8
Existing Security Vulnerabilities Can Compromise Sensitive US-VISIT Data.....	8
Recommendation.....	12
Management Comments and OIG Analysis.....	12
FISMA Issues Need To Be Addressed.....	12
Recommendations	15
Management Comments and OIG Analysis.....	15
The Current Program Management Structure Increases US-VISIT Security Risks.....	17
Recommendations	19
Management Comments and OIG Analysis.....	19

Appendices

Appendix A: Purpose, Scope, and Methodology	21
Appendix B: Management’s Response	24
Appendix C: Map of US-VISIT Site Visits	35
Appendix D: Key US-VISIT Participants.....	36
Appendix E: US-VISIT Entry Procedures.....	37
Appendix F: -----)	38
Appendix G: Digital Fingerprint Scanning	39
Appendix H: Summary of System Security Vulnerabilities By Location	40
Appendix I: Major Contributors to this Report	41
Appendix J: Report Distribution.....	42

Abbreviations

ADIS	Arrival and Departure Information System
BTS	Border and Transportation Security
CBP	United States (U.S.) Customs and Border Protection
CCD	Consular Consolidated Database
CIO	Chief Information Officer
DAA	Designated Accrediting Authority
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
ICE	U.S. Immigration and Customs Enforcement

Table of Contents/Abbreviations

IDENT	Automated Biometric Identification System
ISS	Internet Security Systems
ISA	Interconnection Security Agreement
ISSM	Information Systems Security Manager
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
POE	Port of Entry
<hr/>	
TECS	Treasury Enforcement Communication System
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the information security controls of the three major systems that make up the “backbone” and current framework of the US-VISIT Program: Arrival and Departure Information System (ADIS), Automated Biometric Identification System (IDENT), and Treasury Enforcement Communication System (TECS). In addition, we determined whether these systems comply with Federal Information Security Management Act (FISMA) requirements.

Our audit objective was to determine whether adequate system security controls have been implemented on US-VISIT systems to protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. Our assessment of the adequacy of information security controls on US-VISIT systems is based on direct observations; vulnerability and wireless system security scans; an analysis of applicable security documents; a review of physical security controls at the data centers in Newington, VA, Rockville, MD, and six other audit site locations; and interviews with employees and officials in the US-VISIT Program Office, CBP, and ICE.

Overall, information security controls, including physical access controls, have been implemented and provide an effective level of security on the systems, which comprise the backbone of US-VISIT. However, vulnerabilities exist relative to -----

----- too. These security related issues could compromise the confidentiality, integrity, and availability of sensitive US-VISIT data if they are not remediated.

In addition, we identified that neither memorandums of understanding (MOU)¹ nor interconnection security agreements (ISA)² have been established between CBP and ICE, or with the US-VISIT Program Office, to govern the connection of the systems owned by these organizations. Also, weaknesses are present within the MOUs created to manage the business requirements for non-DHS systems connected to US-VISIT. Furthermore, ISAs between CBP for TECS, one of the key US-VISIT backbone systems, and non-DHS organizations have expired. Because MOUs and ISAs have not been developed, do not specify the security safeguards that should be in place for systems that will be interconnected, or have expired, US-VISIT systems may be vulnerable to [REDACTED]

Further, the security management of the US-VISIT Program needs strengthening. Overall, there is little communication and coordination regarding the security of existing US-VISIT systems between the US-VISIT Program Office, the DHS component Chief Information Officers (CIO), and program officials in CBP and ICE. Though the position includes a significant oversight role, the US-VISIT CIO does not have the necessary authority over DHS component CIOs and program officials in CBP and ICE to ensure adequate security controls are implemented on the systems that will be integrated for the US-VISIT Program. The US-VISIT CIO currently relies on the Information Systems Security Managers (ISSM) in ICE and CBP to ensure that the security controls for existing US-VISIT systems are adequate. However, the CBP and ICE ISSMs report to their respective CIOs. The US-VISIT CIO does not have the ability to direct the component ISSMs, CIOs, and program officials in CBP and ICE to inform the US-VISIT Program Office of the status of US-VISIT system security, which may hinder or limit the processes and mechanisms needed to

¹ A MOU defines the responsibilities of the organizations involved in establishing, operating, and securing an interconnection between two computer systems. The MOU is used to document business and legal requirements of an interconnection. The following should also be considered in developing a MOU: aspects of behavior expected from users who will have access to the interconnection and the implementation of security controls to protect against intrusion, tampering, and viruses (among others), as necessary, to support business relations between the organizations.

² The purpose of an ISA is to support a separate MOU establishing the exchange of data between two organizations. An ISA is a distinct security-related document that outlines the technical and security requirements for a system-to-system connection.

ensure that information security controls for the US-VISIT systems effectively protect US-VISIT data. A coordinated effort is needed to achieve the long-term, comprehensive vision of a secure, integrated entry and exit program.

We are recommending that the Assistant Secretary for Strategic Planning, Office of Policy, establish a formal structure for the oversight and management of the security for the US-VISIT Program. We are also recommending that US-VISIT's CIO be provided with the authority to oversee all elements, including the system security, of the future architecture of the US-VISIT Program. An effective security management structure, the [REDACTED] [REDACTED] and the revision and development of MOUs and ISAs with US-VISIT participants are needed to attain a robust security posture for the US-VISIT Program.

Fieldwork was conducted from January through June 2005 at the US-VISIT Program Office; Newington Data Center, Newington, VA; Rockville Data Center, Rockville, MD; several U.S. ports-of-entry (POE); and U.S. consulates [REDACTED] [REDACTED]. See Appendix A for our purpose, scope, and methodology. Appendix C contains a detailed map of our fieldwork locations.

In response to our draft report, Border and Transportation Security (BTS), the US-VISIT Program Office, and CBP management generally concurred with our findings and recommendations. Where appropriate, changes were made to more accurately present the issues in this report. The integrated management response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The Immigration and Naturalization Service Data Management Improvement Act of 2000 mandated the creation of an automated entry and exit system that integrates electronic arrival and departure information for travelers who need a visa or passport to visit the U.S.³ In accordance with these requirements, the

³ Public Law 106-215.

US-VISIT Program was established and has become a top priority for DHS. While the US-VISIT Program will facilitate the implementation of these requirements, it will help secure U.S. borders as well.

Securing U.S. air, land, and sea borders is a difficult task. The U.S. has more than 7,000 miles of land border with Canada and Mexico and 95,000 miles of shoreline. Additionally, the U.S. has more than 300 air, land, and sea POEs, where travelers are inspected and required to enter and exit the U.S. in accordance with applicable laws and regulations. Each year there are more than 500 million entries into the U.S. through those POEs; some 330 million of those individuals entering are non-U.S. citizens. This volume is projected to rise steadily, intensifying the need to improve the U.S. government's ability to manage its borders.

US-VISIT Process

The US-VISIT process begins overseas, at U.S. embassies and consulates, where individuals who want to travel to the U.S. apply for a visa. The application process involves collecting biographic and biometric (two fingerprints and digital photo) information for the individual. After filling out the required paperwork, a consular officer interviews the individual regarding the purpose of the visit, and the biographic and biometric information collected is checked against databases of known criminals and suspected terrorists.

When a visitor arrives at the POE, travel documents, such as a passport and visa, are reviewed by a CBP officer, who asks specific questions regarding the visitor's stay in the U.S. Most visitors traveling on a visa will then have two fingerprints scanned by an inkless device and a digital photograph taken; these are the same biometrics collected when issuing the person a visa during the application process. (See Appendix E for the US-VISIT entry procedures and Appendix G for a picture of the digital fingerprinting process.)

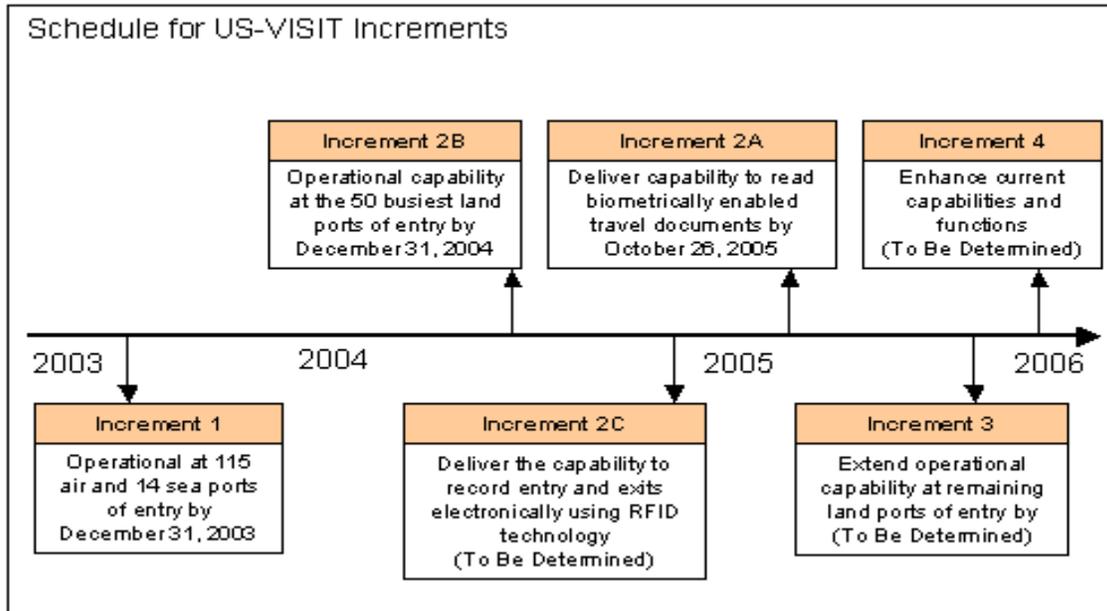
In an effort to tighten security at the U.S. borders, the US-VISIT initiative involving the collection of biographic and biometric information from visitors assists CBP officers in making critical admissibility decisions. With the use of biometrics, the verification process can go more quickly and be conducted with more certainty than by searching databases by name alone.

US-VISIT Timeline

The US-VISIT Program was established to comply with the Data Management Improvement Act’s mandate to create an automated entry and exit system that integrates electronic arrival and departure information for travelers who need a visa or passport to enter the U.S. The program, under the direction of the US-VISIT Program Office, is being implemented using a multi-layered approach to enhance border security. This approach splits the implementation of the US-VISIT Program into four increments. (See Figure 1, Schedule for US-VISIT Increments)

US-VISIT capabilities were first implemented at airports and seaports. Then, these capabilities were extended to U.S. land POEs. The long-term, comprehensive vision of a secure, integrated entry and exit program is not expected to be realized until some time in 2007.

Figure 1



Systems Comprising US-VISIT's Backbone

The ADIS system associates biographical data on travelers who enter and exit the U.S., primarily through airport and seaport POEs.⁴ ADIS currently interfaces with passenger arrival and departure information in TECS. ADIS performs a match or correlation operation to associate arrival and departure records for a particular traveler.

The IDENT system performs three basic biometric operations: identification, verification, and enrollment. Identification consists of searches of databases, such as the terrorist watch lists, to ensure that known or suspected terrorists are not admitted into the U.S. In verification, the claimed identity of a foreign visitor is confirmed by comparing the biometrics of an individual with stored biometrics associated with a travel document, such as a passport or visa. Enrollment “registers” passengers in the US-VISIT IDENT database. IDENT passes required biographic data and fingerprint identification numbers, if any, to be used to perform necessary biometric checks; the same data is used by CBP officers, who “enroll” arriving passengers into the US-VISIT database.⁵

The TECS information system is used to identify individuals and businesses suspected of or involved in violation of federal law. TECS provides CBP officers with controlled access to large databases of law enforcement information.

Data Flow

When the consular offices capture foreign travelers’ biographic and biometric information before issuing a U.S. visa, that information is “enrolled” into the IDENT database and captured in the Department of State’s Consular Consolidated Database (CCD).⁶ If a visa is granted to the traveler, the biographical visa issuance data is transmitted to DHS’ passenger component of TECS, while the biometric data is transmitted to IDENT through the US-VISIT interface with CCD.

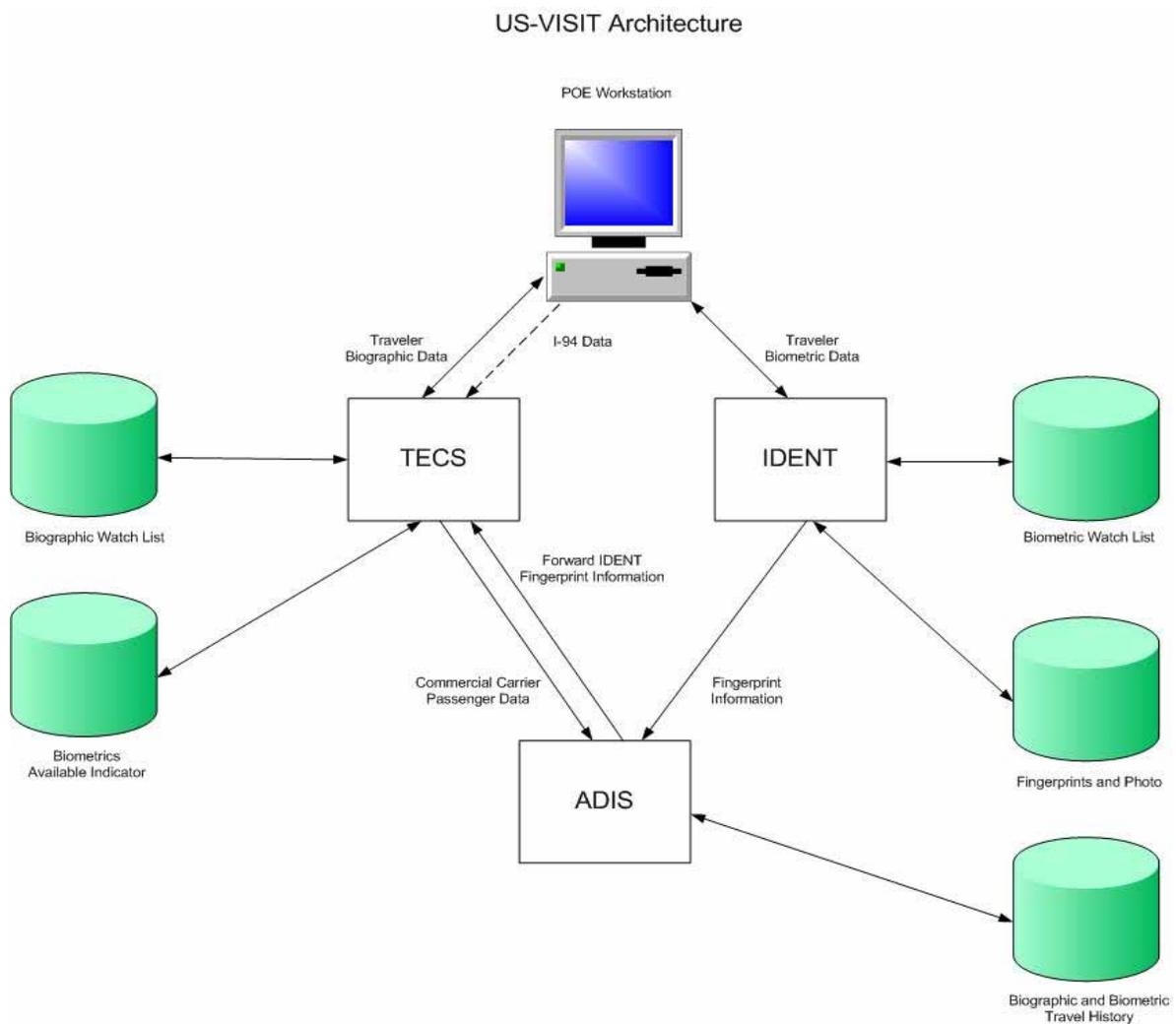
⁴ The exit process is in the piloting phase.

⁵ Enrollment time averages about 30 seconds.

⁶ Consular officers abroad oversee fingerprint enrollment of visa applicants with fingerprint scanners at the visa interview windows. As soon as the fingerprints are captured, they are electronically sent, along with a digital photo of the applicant and biographic data, to CCD.

At U.S. POEs, CBP officers at either or both a primary and secondary “processing station” review foreign travelers’ visa information. Computers with the appropriate software at these processing stations are connected to the systems and databases that comprise US-VISIT’s backbone. The computer workstations are used to facilitate the data input and retrieval from the US-VISIT databases. In addition to the primary and secondary stations, there are laptops, printers, routers, and switches specifically devoted to facilitate data flow from the POEs to the repositories (databases) at the Newington Data Center in Newington, VA. Figure 2 below illustrates the current architecture for US-VISIT operations.

Figure 2



Data on foreign travelers is entered into the systems (ADIS, IDENT, and TECS) that make up US-VISIT at each POE, whether it is an air, sea, or land port. Currently, at the 50 busiest land ports, CBP officers use the [REDACTED] [REDACTED] to capture biographic information from travel documents and biometric data from foreign visitors for enrollment in the US-VISIT Program. The [REDACTED] interacts directly with IDENT to facilitate the processing of travelers through the US-VISIT process at U.S. land ports. This process consists of taking digital fingerscans of the traveler's left and right index fingers, as well as a digital photograph of the traveler's face. These biometrics along with the biographical information contained in the traveler's passport or visa, are compared, and in some cases, entered into the US-VISIT Program if the traveler has not been processed through the program previously. (Appendix F contains [REDACTED] and explains what data is collected on Form I-94.)

Results of Audit

Existing Security Vulnerabilities Can Compromise Sensitive US-VISIT Data

We determined whether the organizational components responsible for US-VISIT systems have implemented adequate security controls to protect the data from unauthorized access, use, disclosure, disruption, modification, or destruction. To make this determination, we conducted system security vulnerability scans of those workstations, servers, and databases solely dedicated to US-VISIT, as well as the associated network devices that facilitated access to US-VISIT systems, at Newington Data Center, Rockville Data Center, and POEs included in our audit. In addition, we reviewed physical security controls at all audit locations, and interviewed system security and administration personnel regarding the user access controls implemented on US-VISIT systems.

We used Internet Security Systems' (ISS) Internet Scanner to conduct vulnerability scans at most of the audit locations we visited.⁷ We did not conduct vulnerability assessment scans at the

⁷ ISS Internet Scanner is a network vulnerability scanner that can be used to scan a pre-defined range of Internet Protocol addresses to identify hosts and selected vulnerabilities. Templates are used to customize

Vancouver or Juarez Consulates, as those systems are owned by the Department of State. ISS' Database Scanner⁸ and Nessus Vulnerability Scanner⁹ were used to detect vulnerabilities on the ADIS and IDENT systems, which reside at the Rockville Data Center. We evaluated physical access controls based on DHS' Sensitive Systems Policy Directive 4300A and best practices.

We determined that:

- 1) "Backbone" US-VISIT systems have been certified and accredited.
- 2) Configuration policies for all US-VISIT workstations are in place.
- 3) The performance of the systems that comprise US-VISIT's backbone is routinely monitored and evaluated.
- 4) Adequate physical controls were present at the Newington, VA and Rockville, MD, data centers, as well as the six audit site locations we visited.

System security vulnerabilities, however, were detected.

The vulnerabilities identified were classified into high, medium, and low categories, based on the severity of the vulnerabilities and damage they could inflict on the systems. These existing vulnerabilities can compromise the confidentiality, integrity, and availability of sensitive US-VISIT data. (See Appendix H for a summary of the numbers and severity of the system security vulnerabilities detected at each location.)

For US-VISIT, we did not identify any significant vulnerabilities at the Newington Data Center. However, the Newington Data Center

----- Further, for US-VISIT at the Rockville Data Center, we identified vulnerabilities relating to -----

scan characteristics, allowing for the inclusion or exclusion of any vulnerability that the software is capable of testing for.

⁸ ISS Database Scanner is a database vulnerability scanner that can be used to scan Microsoft SQL Server, Sybase, and Oracle databases for vulnerabilities. It does not require the installation of code on target systems to scan databases; all that is required is Database Administrator-level network access to the database so that queries and scripts can be executed to perform the scan.

⁹ Nessus Vulnerability Scanner is a security vulnerability product, similar to ISS Internet Scanner, but focuses on vulnerabilities related to Unix and Unix-based systems. Nessus checks for over 1,200 individual industry known vulnerabilities.

[Redacted]

Many of the vulnerabilities identified at the POE locations were related to [Redacted] Other vulnerabilities fell into two groups: [Redacted]

[Redacted] The security posture of US-VISIT operations at the POEs relies heavily on security management at the Newington Data Center.¹⁰ Most of the local area networks at POEs are owned by CBP and connected to CBP's wide area network.¹¹ Therefore, the system administrators at the Newington Data Center can only remedy many of the vulnerabilities at the POEs. A lack of communication between the Newington Data Center and the local system administrators at the POEs is a major factor and an underlying reason as to why a majority of the vulnerabilities existed at the POEs. Figure 3 shows examples of high and medium vulnerabilities identified and prevalent at more than one of the POE locations scanned.

In addition to the security assessment scans, we conducted wireless scans at the POEs [Redacted]. Overall, no authorized or unauthorized wireless access points were identified; however, multiple wireless signals were identified from surrounding businesses. Furthermore, at one of the locations, the point of origin of a wireless access point could not be identified. We suggested that further investigation be performed at this location to identify the origin of the access point and determine whether it poses any security threat to US-VISIT operations.

¹⁰ Newington Data Center [Redacted]

¹¹ Some of the workstations used for US-VISIT operations at one of the POEs were connected to servers owned and administered by ICE. This hardware was previously owned and operated by the Immigration and Naturalization Service prior to being transferred to DHS. A process is in place to turn the administration of all US-VISIT operations at those POEs over to CBP.

Figure 3

Vulnerability	[Redacted]	[Redacted]	Potential Threat
[Redacted]	X		[Redacted]
[Redacted]		X	[Redacted]
[Redacted]		X	[Redacted]
[Redacted]	X		[Redacted]
[Redacted]		X	[Redacted]
[Redacted]	X		[Redacted]

We discussed our findings with US-VISIT 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 CBP's ISSM with the results from each of the POEs assessed so that the system administrators at the Newington Data Center could begin addressing vulnerabilities that could not be remedied by the local administrators.

Recommendation

We recommend that the Assistant Secretary for Strategic Planning, Office of Policy, direct CBP's CIO to:

1. Ensure that CBP's ISSM follows up with the local system administrators at the POEs to ensure that the security vulnerabilities identified for the US-VISIT systems are remediated.

Management Comments and OIG Analysis

Both the US-VISIT Program Office and CBP management concurred with this recommendation. Based on the vulnerability scanning results, the US-VISIT Program Office will independently determine whether US-VISIT information or assets are at risk. CBP Technology Operations will organize a team of local administrators to generate a plan for the recommendation of identified POE vulnerabilities and for addressing subsequently identified vulnerabilities by March 31, 2006.

We accept the US-VISIT Program Office and CBP management's responses to this recommendation.

FISMA Issues Need To Be Addressed

In addition to our system security vulnerability scans, we determined whether US-VISIT's backbone systems, databases, and networks complied with FISMA requirements. 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 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 that comprise US-VISIT's backbone, we identified the following deficiencies as they directly relate to FISMA:

- Neither MOUs nor ISAs have been established between CBP and ICE, or with the US-VISIT Program Office, to govern the connection of the systems owned by these organizations. Organizations that own and operate information technology systems that will be connected should develop an ISA to document the technical requirements of the interconnection to support a MOU that establishes the requirements for data exchange between the organizations.
- A MOU developed between DHS and the Department of State does not document the terms and conditions for the sharing of data and information resources in a secure manner, specify the expected behavior from users who will have access to the interconnection, or contain a reference to the specific security requirements in the ISA. Additionally, neither the MOU nor the ISA were signed by the US-VISIT CIO prior to connecting with US-VISIT systems. Both MOUs and ISA should be submitted to the appropriate Designated Accrediting Authority (DAA) for each organization for approval before the interconnection should be declared operational.¹² As the DAA for the US-VISIT Program, the US-VISIT CIO should formally approve the MOU and ISA between the Department of State and ICE.
- MOUs for accessing the systems containing US-VISIT data have not been developed between DHS and other key agencies, such as the Department of Transportation, that may connect to US-VISIT systems. (Appendix D contains a list of key agencies participating in US-VISIT.)

¹² The DAA is a senior government official with the authority to assume responsibility for operating an information technology system at an acceptable level of risk using prescribed set of safeguards. The DAA is normally the individual who controls the operation of a system and who also influences personnel assignments, system budgets, and system maintenance. Therefore, the DAA is in the position to redirect resources as necessary in order to remedy security deficiencies. A DAA can be responsible for more than one general support system or major application.

-
- Although the certification and accreditation letters were current for TECS, ISAs for the exchange of TECS information between CBP and non-DHS organizations have expired. One of the ISAs expired in January 2003. Organizations should review the security controls for interconnections at least annually, or whenever a system change occurs, to ensure that the controls are operating properly and are providing appropriate levels of protection.
 - While system security plans had been developed for US-VISIT's backbone systems, only TECS contained documentation that it had been reviewed and approved. After making numerous requests for signed copies of both the ADIS and IDENT security plans, ICE personnel were not able to provide them. Therefore, we could not determine whether key management and program personnel from ADIS and IDENT approved the security plans.

We also determined that information security controls, including physical access controls, have been implemented and are operating effectively on the systems that comprise US-VISIT's backbone. For example, we noted the following:

- Adequate physical security controls have been implemented at the POEs and data centers visited. We observed CBP officers displaying their photo identification at all times; entrance barriers and fences were in place to prevent unauthorized entry into the facilities; and, in some locations, closed-circuit televisions had been installed to monitor the POE's perimeter and interior.
- The network performance of the ADIS, IDENT, and TECS system is routinely monitored. Automated tools are used to monitor and evaluate system and network performance and any changes that would be needed for improvement.
- Configuration management policies and procedures have been established for ADIS, IDENT, and TECS to ensure that only authorized system and security changes are implemented. For each system, a formal system change request must be submitted and approved by management before the change can be implemented.

Recommendations

We recommend that the Assistant Secretary for Strategic Planning, Office of Policy, direct the US-VISIT Program Office to:

2. Establish MOUs and ISAs between CBP, ICE, and the US-VISIT Program Office for the interconnections to the US-VISIT backbone systems.
3. Revise the MOU with the Department of State to ensure that it defines the responsibilities for establishing, operating, and securing the interconnection between US-VISIT and the Department of State's systems. Additionally, the US-VISIT CIO should formally approve the MOU and ISA with the Department of State.
4. Establish MOUs with key US-VISIT participants to ensure that security requirements are documented and agreed to before non-DHS systems are connected to US-VISIT's backbone.
5. Ensure that ISAs for the systems comprising US-VISIT's backbone and external organizations are current and formally approved by the US-VISIT CIO.

Management Comments and OIG Analysis

The US-VISIT Program Office concurred with recommendation 2. As a matter of best practices, the US-VISIT Program Office agreed that formal recognition of security agreements should be established between any two organizations in exchange for data, and will ensure that the appropriate documentation is developed. Because the US-VISIT Program Office is not the system owner for TECS, the appropriate signatories for connections between TECS and other systems are the DAAs for those organizations. The US-VISIT Program Office will ensure that program security requirements are appropriately enumerated in these documents.

We accept the US-VISIT Program Office's response to develop the appropriate documentation to support security agreements between DHS and other organizations for the exchange of US-VISIT related data and the assurance that the appropriate

requirements will be incorporated into such agreements in exchange for TECS data.

The US-VISIT Program Office partially concurred with recommendation 3. The Program Office responded that the current ISA between ICE and the Department of State outlines the security that is in place and agreed upon between the two agencies. The MOU will be reviewed and revised to ensure that it properly references the existing US-VISIT/Department of State ISA.

We accept the US-VISIT Program Office's response to review and revise the MOU with the Department of State to ensure that it properly references the existing ISA between ICE and the Department of State for IDENT. However, we continue to recommend that the US-VISIT CIO formally approve the US-VISIT/Department of State ISA prior to referencing it in the MOU and also formally approve the MOU.

The US-VISIT Program Office partially concurred with recommendation 4. As previously mentioned, the Program Office responded that all external connections to the US-VISIT backbone are documented in appropriate ISAs.

We accept the US-VISIT Program Office's response that all current external connections to the US-VISIT backbone systems are documented in appropriate ISAs. We recommend that, in the future, the US-VISIT Program Office continue to ensure that MOUs are established and security requirements are agreed upon with external agencies prior to connecting non-DHS systems to the US-VISIT backbone.

The US-VISIT Program Office concurred with recommendation 5 in regard to connections to external agencies, and agreed to ensure that all external connections are documented in appropriate ISAs. Additionally, although current DHS policy does not require ISAs for systems that interconnect within DHS, the US-VISIT Program Office recognized the need to formally address and document security requirements surrounding the exchange of data as a matter of best practices.

We accept the US-VISIT Program Office's response to address and document security requirements in ISAs with agencies both

within and external to DHS regarding the exchange of US-VISIT data.

The Current Program Management Structure Increases US-VISIT Security Risks

There is little communication or coordination regarding the security of existing US-VISIT systems between and among the US-VISIT Program Office, the DHS component CIOs, and program officials in CBP and ICE. For example, the US-VISIT CIO was unaware of the results of a November/December 2004 security risk assessment of four field offices in the Miami area conducted by CBP's Information Systems Security Branch. Additionally, because neither CBP nor ICE management reported or discussed the results of the system security assessments that we conducted with the US-VISIT Program Office, US-VISIT's CIO did not know what vulnerabilities we had detected at the Newington Data Center, Rockville Data Center, and the POEs. As a result, the US-VISIT CIO lacked an overall awareness of the current security posture of the US-VISIT Program or the vulnerabilities that exist with the legacy CBP and ICE systems that comprise the US-VISIT Program.

The US-VISIT CIO has a significant oversight role in the implementation of the US-VISIT Program, which includes serving as the DAA for the US-VISIT Program. As the DAA, the US-VISIT CIO is responsible for assuming security risks associated with the US-VISIT systems. With a staff of only 17 full time employees, the US-VISIT CIO currently relies on the ISSMs in CBP and ICE to ensure that the controls of US-VISIT systems are adequate, but they do not directly report to him. Additionally:

- There is no clear accountability of ownership for both the ADIS and IDENT systems. In February 2005, the former Under Secretary, BTS, signed a memorandum transferring the ownership of ADIS to the US-VISIT Program Office (IDENT was previously moved to the Program Office). However, as of May 2005, US-VISIT personnel, including the CIO, were still unclear as to who actually owned, and thus was responsible for securing these systems.

-
- The US-VISIT CIO lacks any authority with other DHS component CIOs and program officials in CBP and ICE to guide them in assuring adequate security controls are implemented on the legacy systems that make up US-VISIT's backbone. Furthermore, US-VISIT's CIO does not have the authority over the ISSMs or system owners in CBP or ICE to ensure that system vulnerabilities are remediated.

DHS' Sensitive Systems Policy Directive 4300A requires that component CIOs establish and oversee the information technology security program within their organizational component. Specifically, component CIOs must ensure that an ISSM has been appointed. CIOs should also make certain that the ISSM works closely with program officials to ensure a complete understanding of risks, especially the increased security risks resulting from the interconnectivity with other programs and systems over which the CIO may have little or no control.

Ultimately, the CIOs and program officials are accountable for the security of the information systems in compliance with FISMA. However, DHS has not established guidelines to support multiple owners and users of systems or data, making it difficult for the US-VISIT CIO to report on the security of the US-VISIT systems in compliance with the FISMA requirements. Additionally, the US-VISIT CIO does not have the authority to direct the component ISSMs, CIOs, and program officials in CBP and ICE to report to the US-VISIT Program Office on the status of US-VISIT system security, which may hinder or limit the processes and mechanisms needed to ensure that information security controls for the US-VISIT systems effectively protect US-VISIT data. A coordinated effort is needed to strengthen security management controls and achieve the long-term, comprehensive vision of having a secure, integrated entry and exit program.

Recommendations

We recommend that the Assistant Secretary for Strategic Planning, Office of Policy:

6. Establish a formal structure for the oversight and management of the security for the US-VISIT Program.
7. Provide US-VISIT's CIO with sufficient authority to oversee all elements, including the system security, of the future architecture of the US-VISIT Program.

Management Comments and OIG Analysis

The US-VISIT Program Office partially concurred with recommendation 6, but disagreed with the finding that there is little communication or coordination regarding the security of US-VISIT systems. The Program Office agreed that a formal structure for the oversight and management of the security for US-VISIT is needed. However, as documented in the response to the recommendation and additional comments, the US-VISIT Program Office stated that it has been actively engaged in providing oversight and management by establishing security working groups, creating a formal US-VISIT life-cycle development plan and the oversight of the system assurance testing of the plan, and developing a security strategy within the blueprint being crafted as a guide for future development efforts.

The Program Office also noted that US-VISIT program functions are implemented via systems, owned and operated by CBP and ICE, that are modified or enhanced according to the functional and security requirements developed by the US-VISIT Program Office. As such, technical solutions meeting these requirements are often developed, in concert, or at a minimum in consultation, with the other organizations. Furthermore, the Program Office initiated regular security team meetings, attended by the security principals from each organization, to discuss a wide range of security issues. While these meetings are essentially conducted “worker to worker” and may not always have high visibility, they nonetheless directly and positively impact the security posture of the systems comprising US-VISIT.

We accept the US-VISIT Program Office's response; however, we continue to recommend that the Program Office develop a formal structure to oversee and manage the security of the current legacy systems that comprise the US-VISIT backbone. During a meeting in May 2005, the US-VISIT CIO agreed that there is little communication or coordination among the components (CBP and ICE), the US-VISIT Program Office, and POE personnel regarding the existing structure and security vulnerabilities associated with the main, legacy systems that comprise US-VISIT. During our audit, we observed that Program Office efforts are focused on the security of the future US-VISIT program, while the US-VISIT CIO relied upon the oversight and management of the CBP and ICE ISSMs to ensure that current system security controls are effectively protecting US-VISIT data. Additionally, based upon our audit site visits, we determined that the system administrators at the POEs have little control over the implementation of security controls or remediation of security weaknesses associated with US-VISIT systems.

The US-VISIT Program Office concurred with recommendation 7 to provide the US-VISIT CIO with additional authority over the future architecture of US-VISIT.

We accept the US-VISIT Program Office's response; however, there should be formal documentation outlining the role and authority of the US-VISIT CIO with regard to the future architecture of the US-VISIT Program.

Purpose, Scope, and Methodology

The overall objective of this audit was to determine whether adequate system security controls have been implemented on US-VISIT systems to protect sensitive and biometric data from unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, we evaluated whether (1) controls have been implemented to effectively manage access to US-VISIT systems and protect the data contained on those systems; (2) the US-VISIT Program Office and organizational components have implemented adequate access controls to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction; and (3) US-VISIT systems comply with FISMA requirements.

To identify whether controls had been implemented to manage access to US-VISIT systems, we analyzed documents provided by US-VISIT personnel including: concepts of operations for Increments 1 and 2B, system administrator and password issuance user manuals; interface control documents, MOUs; ISAs; TECS' configuration management plan; ICE's Enterprise Systems Assurance Plan; audit trails; change control policies; and system change requests. Also, we reviewed DHS and National Institute of Standards and Technology (NIST) policies and procedures; the Federal Information Systems Controls Audit Manual; and Office of Management and Budget requirements. In addition, we interviewed US-VISIT Program Office officials, the CBP and ICE ISSMs, system administrators and management officials at the POEs, and personnel at U.S. Consulates [REDACTED]. Furthermore, we attended a demonstration of CCD at the Department of State in Washington, DC and observed the visa issuance process at two U.S. Consulates.

In determining whether the US-VISIT Program Office and organizational components coordinated, established, and implemented adequate access controls, we used two software tools to conduct security vulnerability assessment scans on CBP and ICE systems, databases, and networks that make up the US-VISIT

backbone.¹³ Only those components (servers, workstations, routers and switches, Intrusion Detection Systems, firewalls, anti-virus tools, and other network devices) specifically designated to support US-VISIT were scanned. We did not assess the security vulnerabilities of the mainframe system at Newington Data Center, nor did we evaluate the security of the CBP or ICE networks. US-VISIT system components were evaluated against a set of objective questions based on DHS and NIST guidance and criteria. Our testing methodology consisted of a standards-based vulnerability assessment and security controls review designed to imitate real-world information security testing in a controlled manner. Also, we conducted wireless scans at the POEs located in [REDACTED] to identify any authorized and unauthorized wireless access points. Additionally, we evaluated physical access security controls at the locations visited.

To assess whether US-VISIT systems complied with the FISMA requirements, we reviewed DHS and NIST guidance, as well as Federal Information Processing Standards 199. We also analyzed documents provided by US-VISIT, CBP and ICE personnel, including systems certification and accreditation packages; risk assessments; system security plans; Federal Information Processing Standards 199 assessments; self-assessments; and contingency plans. We also identified whether security costs were integrated into each life cycle increment for the US-VISIT backbone systems, and whether Plans of Actions and Milestones had been developed for ADIS, IDENT, and TECS. We interviewed CBP and ICE personnel regarding security awareness and specialized training.

We conducted fieldwork at the US-VISIT Program Office in Arlington, VA, and the following locations:

¹³ ISS Internet Scanner, version 7.0, was used to conduct scans of servers, computer workstations, printers, and other network devices specifically dedicated to US-VISIT operations for vulnerabilities. Nessus Vulnerability Scanner, version 2.2.4, was used to scan the ADIS and IDENT operating systems.

Location	Airport	Land Port	Seaport	Data Center	U.S. Consulate
[REDACTED]		X			
[REDACTED]					X
[REDACTED]	X		X		
Newington, Virginia				X	
[REDACTED]		X			
Rockville, Maryland				X	
[REDACTED]	X				
[REDACTED]	X		X		
[REDACTED]	X				X

We chose the specific audit locations based on geographic location, to ensure coverage for perimeter of the U.S. borders, and ranking for busiest POEs. We conducted our audit from January 2005 through June 2005 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 I.

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

[REDACTED]

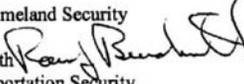
Appendix B
Management's Response

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

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

FROM: Randy Beardsworth 
Border and Transportation Security

SUBJECT: Response to the Office of Inspector General's Draft Report
"US-VISIT System Security Management Needs
Strengthening."

Thank you for providing the Border and Transportation Security Directorate (BTS) with a copy of your draft report entitled "US-VISIT System Security Management Needs Strengthening" and the opportunity to comment on the issues in this report.

BTS has reviewed the replies from both Customs and Border Protection (CBP) and US-VISIT and concurs with their responses. An integrated response is attached. BTS recognizes the importance of the recommendations made by the Inspector General in the report, and calls attention to both CBP's and US-VISIT's willingness to take corrective action concerning these issues.

CBP, US-VISIT and DHS security teams work diligently to minimize risks and provide adequate system security controls. The OIG came to this same basic conclusion during this audit, and provided valuable information for further improvement. As BTS is always striving to achieve stronger security, BTS welcomes the OIG recommendations and will implement them in a timely manner.

CBP and US-VISIT have also offered additional comments, attached as well.

If you have any questions regarding this response, you or your staff may contact Daniel Newell, BTS audit liaison, at (202) 282-8429.

Attachments

www.dhs.gov

US-VISIT System Security Management Needs Strengthening

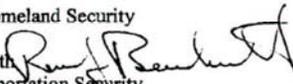
Appendix B
Management's Response

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

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

FROM: Randy Beardsworth 
Border and Transportation Security

SUBJECT: Protection of the Office of Inspector General's Draft Report
"US-VISIT System Security Management Needs
Strengthening."

BTS concurs with CBP's assessment that the information in the audit does warrant protection and designates the documents as "For Official Use Only (FOUO)." CBP believes that the report identifies weaknesses of CBP systems and classification of the report as FOUO is clearly justified due to the sensitive nature of the information contained therein. Please consider CBP's concerns prior to releasing information that has been determined to be sensitive.

If you have any questions regarding this response, you or your staff may contact Daniel Newell, BTS audit liaison, at (202) 282-8429.

www.dhs.gov

Appendix B
Management's Response

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

MEMORANDUM FOR: James A. Williams
Director, US-VISIT

FROM: Randy Beardsworth 
Border and Transportation Security

SUBJECT: Draft OIG Report: "United States Visitor and Immigrant
Status Indicator Technology (US-VISIT) System Security
Management Needs Strengthening"

Thank you for providing the Border and Transportation Security Directorate(BTS) with your detailed response to the OIG draft report entitled "US-VISIT System Security Management Needs Strengthening." BTS recognizes the commitment of US-VISIT to a robust security of its systems in the performance of its mission.

BTS concurs with the US-VISIT response and directs US-VISIT to implement the draft report's recommendations in the manner outlined in your response. The timely implementation of the OIG recommendations in the manner specified herein will serve to enhance the security controls already in place to protect the US-VISIT backbone.

Please contact BTS for any assistance and/or expertise in accomplishing this goal. BTS is committed to supporting US-VISIT in the secure accomplishment of its mission, and supports the dedication of US-VISIT personnel in working to secure our nation.

If you have any questions regarding this memo, you or your staff may contact Daniel Newell, BTS audit liaison, at (202) 282-8429.

www.dhs.gov

US-VISIT System Security Management Needs Strengthening

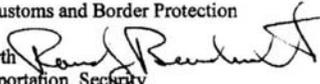
Appendix B
Management's Response

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

MEMORANDUM FOR: Robert C. Bonner
Commissioner, Customs and Border Protection

FROM: Randy Beardsworth 
Border and Transportation Security

SUBJECT: Draft OIG Report: "United States Visitor and Immigrant
Status Indicator Technology (US-VISIT) System Security
Management Needs Strengthening"

Thank you for providing the Border and Transportation Security Directorate(BTS) with your detailed response to the OIG draft report entitled "US-VISIT System Security Management Needs Strengthening." BTS recognizes the commitment of Customs and Border Protection(CBP) to a robust security of its systems in the performance of its mission.

BTS concurs with the CBP response and directs CBP to implement the draft report's recommendations in the manner outlined in your response. The timely implementation of the OIG recommendations in the manner specified herein will serve to enhance the security controls already in place to protect the US-VISIT backbone.

Please contact BTS for any assistance and/or expertise in accomplishing this goal. BTS is committed to supporting CBP in the secure accomplishment of its mission, and supports the dedication of CBP personnel in working to secure our nation.

If you have any questions regarding this memo, you or your staff may contact Daniel Newell, BTS audit liaison, at (202) 282-8429.

www.dhs.gov

**Comments on OIG Draft Report: United States Visitor and Immigrant Status Indicator
Technology (US-VISIT) System Security Management Needs Strengthening**

Recommendation No. 1: We recommend that the Acting Under Secretary, BTS, direct CBP's CIO to ensure that CBP's ISSM follows up with the local system administrators at the POEs to ensure that the security vulnerabilities identified for the US-VISIT systems are remediated.

CBP concurs with the recommendation. The Director, Technology Operations, was given responsibility and authority to ensure CBP IT infrastructure is protected against malicious code intrusions and to respond to any such intrusions. Personnel performing infrastructure software updates were transferred to Technology Operations, where they are in the chain-of-command responsible for handling preventative maintenance and action responses.

CBP Technology operations will organize a team of local administrators to generate a plan for the recommendation of identified POE vulnerabilities and for addressing subsequently identified vulnerabilities by March 31, 2006.

US-VISIT also concurs with the recommendation that CBP's Information Systems Security Manager (ISSM) follow up with local system administrators to ensure that security vulnerabilities identified in the audit are addressed. We have also requested a copy of the vulnerability scanning results to independently determine whether US-VISIT information or assets are at risk; we are awaiting receipt of the information.

Recommendation No. 2: We recommend that the Acting Under Secretary, BTS, direct the US-VISIT Program Office to establish MOUs and ISAs between CBP, ICE, and the US-VISIT Program Office for the interconnections to the US-VISIT backbone systems.

US-VISIT concurs with this recommendation. As a matter of best practices, US-VISIT agrees that formal recognition of security agreements should be established between any two organizations that exchange data, and we will ensure that appropriate documentation is developed. Because US-VISIT is not the system owner for TECS, the appropriate signatories for connections between TECS and other systems are the DAAs for those organizations. US-VISIT will ensure that program security requirements are appropriately enumerated in those documents.

Recommendation No. 3: We recommend that the Acting Under Secretary, BTS, direct the US-VISIT Program Office to revise the MOU with the Department of State to ensure that it defines the responsibilities for establishing, operating, and securing the interconnection between US-VISIT and the Department of State's systems. Additionally, the US-VISIT CIO should formally approve the MOU and ISA with the Department of State.

US-VISIT partially concurs with this recommendation. The current ISA between ICE and the Department of State outlines the security that is in place and agreed upon between the two agencies. The MOU will be reviewed and revised to ensure it properly references the existing US-VISIT/Department of State ISA.

Appendix B Management's Response

Recommendation No. 4: We recommend that the Acting Under Secretary, BTS, direct the US-VISIT Program Office to establish MOUs with key US-VISIT participants to ensure that security requirements are documented and agreed to before non-DHS systems are connected to US-VISIT's backbone.

US-VISIT partially concurs with this recommendation. As previously mentioned, all external connections to the US-VISIT backbone are documented in appropriate ISAs.

Recommendation No. 5: We recommend that the Acting Under Secretary, BTS, direct the US-VISIT Program Office to ensure that ISAs for the systems comprising US-VISIT's backbone and external organization's are current and formally approved by the US-VISIT CIO.

US-VISIT agrees with this recommendation in regard to connections to external agencies, and we work to ensure that all external connections are documented in appropriate ISAs. Although current DHS policy does not require ISAs for systems that interconnect within DHS, US-VISIT recognizes the need to formally address and document security requirements surrounding the exchange of data as a matter of best practices.

Recommendation No. 6: We recommend that the Acting Under Secretary, BTS, establish a formal structure for the oversight and management of the security for the US-VISIT Program.

US-VISIT partially concurs with this recommendation. We agree that a formal structure for the oversight and management of the security for US-VISIT is needed. However, it should be noted that US-VISIT has been actively engaged in providing oversight and management by establishing security working groups, creating a formal US-VISIT life-cycle development plan, and developing a security strategy within the blueprint being crafted as a guide for future development efforts.

Recommendation No. 7: We recommend that the Acting Under Secretary, BTS, provide US-VISIT's CIO with the authority to oversee all elements, including the system security, of the future architecture of the US-VISIT Program.

US-VISIT agrees with the recommendation to provide the US-VISIT CIO with additional authority over the future architecture of US-VISIT and we look forward to working with the appropriate officials to implement this recommendation.

US-VISIT Additional Comments

1. We are in complete agreement that increased authority for the US-VISIT CIO would better enable us to provide stronger security for US-VISIT component systems. US-VISIT has an Information Systems Security Manager (ISSM) who reports directly to the US-VISIT CIO. The US-VISIT ISSM works with both DHS headquarters and component (ICE and CBP) ISSMs and staff to coordinate security for US-VISIT. Though there are coordinated efforts between all components involved in US-VISIT, like the US-VISIT CIO, the US-VISIT ISSM does not have any authoritative power over the component ISSMs. As a result, the US-VISIT ISSM relies on component ISSMs to provide security policy, guidance, and enforcement. As ICE and CBP do not always follow the same processes, policies, or requirements, the oversight roles played by the current US-VISIT ISSM and CIO are difficult.
2. Though we agree that additional authority would benefit the US-VISIT CIO role, the proposed reorganization will remove the Border and Transportation Security Management layer.
3. We disagree with the finding that there is "little communication or coordination regarding the security of existing US-VISIT systems..." US-VISIT program functions are implemented via systems, owned and operated by CBP and ICE, that are modified or enhanced according to the functional and security requirements developed by US-VISIT. Technical solutions meeting these requirements are often developed in concert, or at a minimum in consultation, with the other organizations. Furthermore, US-VISIT is directly involved in the oversight of system assurance testing and has established a life-cycle process that coordinates the involvement of CBP and ICE. In addition, we have initiated regular security team meetings, attended by the security principals from each organization, that meets to discuss a wide range of security issues. These meetings are essentially conducted "worker-to-worker" and may not always have high visibility, but they nonetheless directly and positively impact the security posture of the systems comprising US-VISIT.
4. Any audit of the security posture of a system is likely to identify weaknesses that may need to be addressed. US-VISIT, CBP, and ICE conduct risk assessments and self-assessments that result in plans of action and milestones (POA&Ms) to address those weaknesses. To make effective use of scarce budgetary resources, weaknesses are prioritized for remediation. The information provided by the OIG report identifies additional weaknesses that may need mitigation. Overall, however, US-VISIT, CBP, and ICE have all developed security programs that effectively secure the information and assets supporting US-VISIT. We do not wish to minimize the importance of continuing to examine the security posture of all of the systems involved in the program, but do want to emphasize the significant steps that have been taken to enhance security.
5. Finally, we offer the following comments to ensure the accuracy of the reported information:

Appendix B Management's Response

Page 5, Figure 1: The description of Increment 2C should be changed to read "Deliver the capability to record entry and exits electronically using RFID technology (to be determined.)"
[Change made.](#)

Page 12, first paragraph: The report states that findings were discussed with US-VISIT personnel at each audit location. As the audit locations consisted of CBP ports of entry (POEs) and ICE and CBP Data Centers, it is likely the findings were shared with CBP and ICE personnel, and not with those of US-VISIT. We would appreciate receiving copies of all findings in order to immediately improve our coordination efforts with the components.
[Results were provided to CBP and ICE ISSMs during fieldwork.](#)

Page 9, first paragraph: US-VISIT was informed by the OIG that the mainframe system, also known as TECS, was out of the scope of this audit because it is undergoing a separate assessment as part of the DHS financial statement audit. As the mainframe system is an integral component of the US-VISIT backbone, we look forward to obtaining the results of the security assessment to ensure that the overall security for the US-VISIT backbone is adequate.

Page 9, first full paragraph: We are pleased that the OIG was able to confirm that adequate security controls are in place for the main criteria audited.



Page 13, second bullet: ISAs have been established for all external connections to the US-VISIT backbone. US-VISIT systems do not directly interface with Department of Transportation systems or those of other agencies listed in the diagram in Appendix D. The diagram is intended to be a programmatic diagram to show the various benefits other government agencies (OGAs) might receive from US-VISIT. In no way does it depict direct connections to US-VISIT backbone systems. All internal interfaces are documented in system security plans and interface control documents, and external connections are documented in ISAs. (Currently the third bullet)

Page 13, third bullet: Without knowing the exact document being referenced, the expiration date is consistent with the stand-up of DHS. As a result, some of the ISAs which were established for previously external connections (i.e., ICE and CBP prior to DHS being stood up) would no longer be appropriate as ISAs document external connections, not internal ones. The TECS C&A document undergoes constant modifications to reflect its most current state. The information in the referenced expired ISA is probably included in the TECS System Security Plan (in the interconnection section) or in an appropriate interface control document (between TECS and the system in question). However, as mentioned in the response to Recommendation No. 2, we agree that formal recognition of security agreements

Appendix B Management's Response

should be established between any two organizations that exchange data, and we will ensure that appropriate documentation is developed and maintained. (Currently on Page 14)

Page 14, first bullet: Requiring the signing of actual documents for approval is not part of the current life cycle process within ICE. The documents go through several review cycles and must have final approval before they can enter the enterprise library repository. During the release readiness reviews, the security team is called upon to state whether the C&A documents were received, found to be adequate, and approved prior to system release. The signature of the ISSM (or delegate) at the RRR indicates approval of C&A documents. (Currently the second bullet)

Page 16, first bullet: The memorandum referenced did not refer to IDENT. It did refer to ADIS; however, the memorandum has never been officially recognized throughout the Department, and only selectively recognized within various components. DHS headquarters has worked with Price Waterhouse Coopers (PWC) to establish a complete and accurate inventory of general support systems and major applications in order to assign appropriate accountability for Federal Information Security Management Act (FISMA) implementation and reporting. These efforts were completed in mid-August 2005 and have made US-VISIT the responsible component for both ADIS and IDENT. (Currently on Page 17)
Sentence revised.

Page 16, second bullet: We agree that the US-VISIT CIO lacks formal authority over CBP and ICE in guiding the implementation of security controls. However, US-VISIT does establish security requirements for development efforts and ensures that these requirements are met through a rigorous systems assurance process. (Currently on Page 18)
Added "legacy" before systems.

Page 23, Appendix D: This diagram is intended to be a programmatic diagram designed to show the various benefits OGAs might receive from US-VISIT. In no way does it depict direct connections to US-VISIT backbone systems. (Currently Page 36)

Appendix B
Management's Response

CBP Technical Comments

Page 6, 2nd paragraph, last sentence: Since program dates have recently changed, the phrase in the last sentence of the paragraph should be changed to "until some time in 2007." (Currently on Page 5)
[Change made.](#)

Page 6, Figure 1: For sensitivity consideration, delete the "To Be Determined" phrase from the Increment 2C and Increment 4 boxes. (Currently on Page 5)

Page 9, Figure 2: Clarification points:

- (1) What is the significance of the dashed line for the I-94 Data?
 - (2) Is the Biometrics Available Indicator a database?
 - (3) Is Biographic and Biometric Travel History part of the US-VISIT charter?
- (Currently on Page 7)

Page 12, last paragraph: Recommend deleting the 2nd, 3rd, and 4th sentences and rewording the final sentence to remove reference to "access point," i.e., "... further investigation be performed to determine additional possible wireless threats to US-VISIT operations." This removes specificity of threat yet leaves the vulnerability referenced. (Currently on Page 10)

Page 14, recommendation 1: The assumption is that CBP OIT will work through the appropriate OIT chain of command in order for the local system administrator, in the field, to remediate security vulnerabilities identified for the US-VISIT systems. Maintaining the chain of command will ensure proper communications between the National Data Center and the local system administrators in the field.

Additionally, while the Corrective Action Plan may fix an isolated incident, it does not address an enterprise solution for correcting vulnerabilities. Any enterprise wide solution regarding these vulnerabilities should be addressed through collaborative efforts of the US-VISIT Program Office and OIT Headquarters (Technology Operations, Passenger Systems, Program Integration, and any other contributing areas.) Without a top-down solution, only pockets of issues will be addressed, thus leaving an enterprise-wide vulnerability.

All personnel responsible for CBP IT infrastructure software updates have been transferred to the OIT Technology Operations Division. This ensures a centralized chain-of-command for making decisions regarding preventative maintenance and response actions on CBP IT infrastructure. (Currently on Page 12)

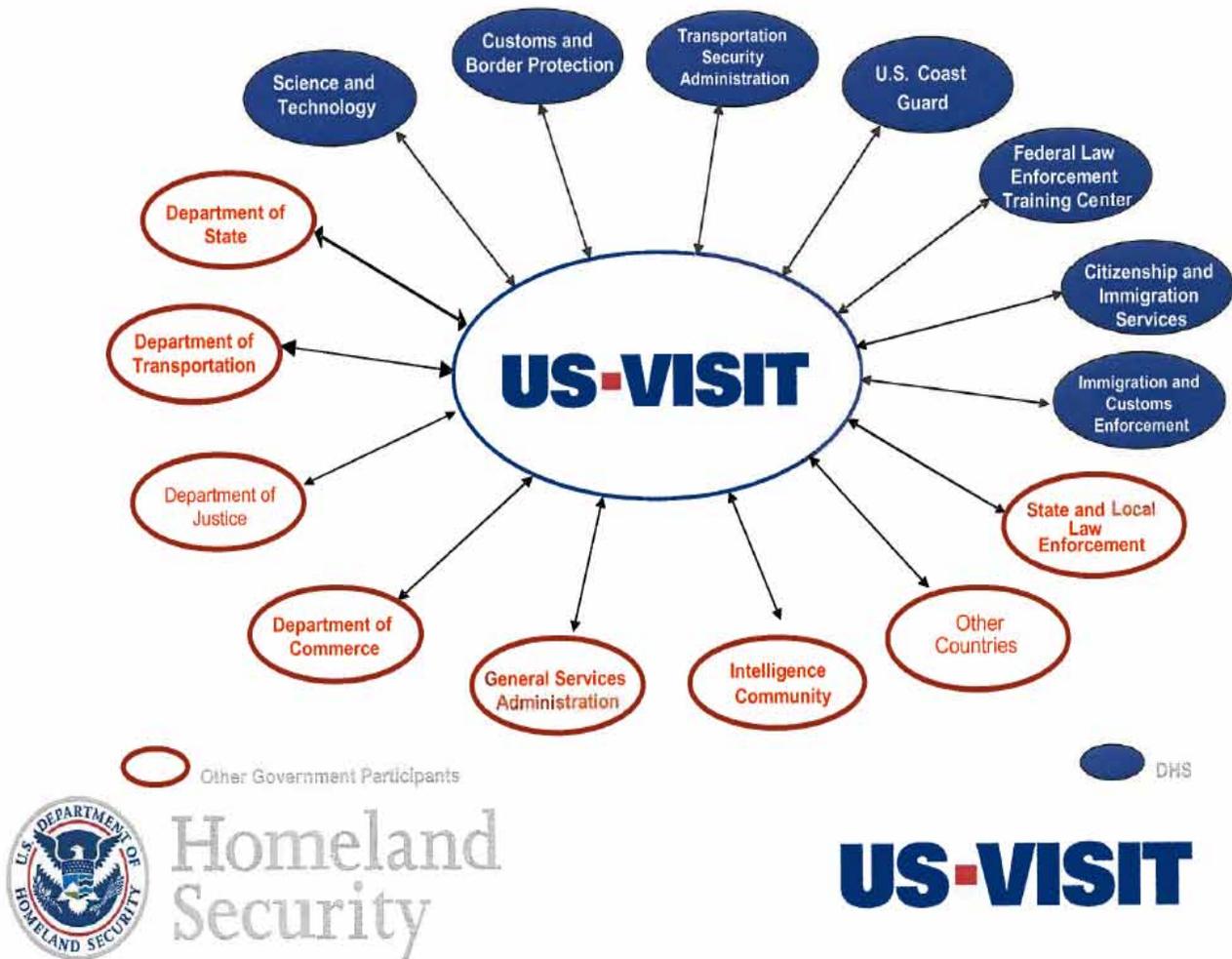
Page 17, paragraph under "The Current Program Management ... Security Risks," 2nd sentence: The sentence indicates that an example would be that the US-VISIT CIO was unaware of the results of a November/December 2004 security risk assessment performed by CBP OIT Security. CBP OIT Security did not perform any risk assessment in 2004. The sentence should be corrected.
[Added Miami - Risk assessment was conducted 11/29 through 12/9/2004.](#)

Page 19, recommendations 6 and 7: CBP believes that an Interagency Security team be established to collaboratively address US-VISIT security issues. This is the same approach that has been effective with the functional aspects of US-VISIT (i.e., requirements, development, deployment). CBP believes that it is impractical to give the US-VISIT CIO operational authority over CBP security processes. CBP agrees that the US-VISIT CIO needs to be informed of activities and events associated with the CBP security, just as the CIOs of other entities with whom CBP provides services (CIS, ICE, DOS, IRS, ATF, etc.). The US-VISIT components that were developed by CBP and operate in the CBP technical environment are very important components of TECS; but they are a small component of the overall system. Giving an external CIO authority over the CBP security program does not make sense.

Page 29, Appendix H: A reference would be helpful to a document that would provide details on the listed vulnerabilities so that CBP OIT Security could track their remediation. For sensitivity considerations, the reference should be password protected and not available to the public. (Currently Page 40)
[CBP system administrators and CBP's ISSM were provided with technical vulnerability reports.](#)

Appendix C
Map of US-VISIT Site Visits

Key Participants



Welcome

US-VISIT Procedures: For All International Visitors

1: Left Index Finger
Indice Izquierdo
왼손 검지손가락
左手食指
Indicador Esquerdo



2: Right Index Finger
Indice Derecho
오른손 검지손가락
右手食指
Indicador Direito



3: Look at Camera
Mire la Cámara
카메라를 보십시오
注视相机
Olhe para a Câmera



If you have privacy concerns or questions about the safekeeping of your personal information, please contact the US-VISIT privacy officer at usvisitprivacy@dhs.gov



**Homeland
Security**

US-VISIT
www.dhs.gov/us-visit

Keeping America's Doors Open and Our Nation Secure

¹⁵ Foreign nationals traveling on non-immigrant visas are issued Form I-94, Arrival/Departure Record. This form shows the traveler's date of arrival, POE, and date the authorized period of admission expires. Non-immigrant travelers issued an I-94 are enrolled in the US-VISIT Program during the primary inspection process at airports and seaports. At land ports, non-immigrant travelers are enrolled in the US-VISIT Program during the secondary inspection process.

Appendix G
Digital Fingerprint Scanning



Source: <http://www.whitehouse.gov/omb/budget/fy2006/dhs.html>

Summary of System Security Vulnerabilities By Location

Location	Severity of Vulnerability			Total
	High	Medium	Low	
-----	6	2	1	9
-----	3	2	18	23
-----	0	0	2	2
-----	0	0	3	3
-----	8	9	12	29
-----	0	0	1	1
-----	14	6	11	31
-----	5	1	3	9
Totals	36	20	51	107

Information Security Audit Division

Edward G. Coleman, Director

Barbara Bartuska, Audit Manager

Chelsea Pickens, Senior Information Technology Auditor

Scott Binder, Information Technology Auditor

Pedro Calderon, Information Technology Auditor

William Matthews, Information Technology Auditor

Jason Bakelar, Referencer

Karen Nelson, Referencer

Advanced Technology Division

Jim Lantzy, Director

Michael Goodman, Security Engineer

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

Lane Melton, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Executive Secretary
General Counsel
CIO
Chief Information Security Officer
Commissioner, CBP
CBP CIO
Assistant Secretary, ICE
ICE CIO
US-VISIT Program Director
US-VISIT CIO
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative Affairs
Assistant Secretary, Policy
Director, Government Accountability Office/OIG Liaison Office
Director, Compliance and Oversight Program
CIO Audit Liaison
CBP Liaison
ICE Audit Liaison
US-VISIT Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

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.