United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2007

INFORMATION SECURITY

Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program

GAO-07-870

July 2007

INFORMATION SECURITY

Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-870, a report to congressional requesters

Why GAO Did This Study

Intended to enhance the security of U.S. citizens and visitors, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program encompasses the pre-entry, entry, status management, and exit of foreign national travelers who enter and leave the United States at 285 air, sea, and land ports of entry.

GAO was asked to determine whether Department of Homeland Security (DHS) has implemented appropriate controls to protect the confidentiality, integrity, and availability of the information and systems used to support the US-VISIT program. To do this, GAO examined the controls over the systems operated by Customs and Border Protection (CBP) that support the US-VISIT program.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct CBP to fully implement information security program activities for systems supporting the US-VISIT program. In commenting on a draft of this report, DHS stated that it has directed CBP to complete remediation activities to address each of the recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-870.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov or Keith A. Rhodes, (202) 512-6412, rhodesk@gao.gov.

What GAO Found

The systems supporting the US-VISIT program have significant information security control weaknesses that place sensitive and personally identifiable information at increased risk of unauthorized and possibly undetected disclosure and modification, misuse, and destruction. Weaknesses existed in all control areas and computing device types reviewed. Deficiencies in access controls and other system controls exposed mainframe computer, network infrastructure, servers, and workstations to insider and external threats. For example, CBP did not implement controls to effectively prevent, limit, and detect access to computer networks, systems, and information. To illustrate, it did not (1) adequately identify and authenticate users in systems supporting US-VISIT; (2) sufficiently limit access to US-VISIT information and information systems; (3) ensure that controls adequately protected external and internal network boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. In addition, CBP did not always ensure that responsibilities for systems development and system production were sufficiently segregated and did not consistently maintain secure configurations on the application servers and workstations at a key data center and ports of entry.

These weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including personally identifiable information, and disrupt the operations of the US-VISIT program. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These risks are not confined to US-VISIT information. The CBP mainframe and network resources that support US-VISIT also support other programs and systems. As a result, the vulnerabilities identified in this report could expose the information and information systems of the other programs to the same increased risks.

A key reason for these weaknesses is that, although CBP has made important progress in implementing elements of the department's information security program, it did not effectively or fully implement essential program activities. For example, CBP did not fully characterize the risks facing critical systems, update interconnection security agreements in security plans, sufficiently test and evaluate security controls, incorporate required elements in remedial action plans, adequately implement incident detection and handling procedures, and consistently address privacy issues. Until DHS and CBP act to mitigate the weaknesses in CBP systems supporting the US-VISIT program and CBP effectively and fully implements its information security program, limited assurance exists that the US-VISIT program will achieve its goal of enhancing the security of U.S. citizens and its visitors.

Contents

Abbreviations

ADIS	Arrival and Departure Information System
CCD	Consular Consolidated Database
CBP	United States Customs and Border Protection
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
ICE	United States Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
INS	Immigration and Naturalization Service
ISA	Interconnection Security Agreement
IT	Information Technology
LAN	Local-area Network
NCIC	National Crime Information Center
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
SORN	System of Records Notice
TECS	Treasury Enforcement Communications System
TECS/IBIS	Treasury Enforcement Communications System/ Interagency Border Inspection System
USCIS	United States Citizenship and Immigration Services
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WAN	Wide-area Network

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 13, 2007

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

In the years since the 2001 terrorist attacks, the need to secure U.S. borders has taken on added importance and has received increasing attention from Congress and the public. In an effort to avoid repetition of such attacks, and improve overall national security, Congress and the Administration have sought better ways to record and track the entry and departure of foreign visitors who pass through U.S. ports of entry[1] by air, land, or sea; to verify their identities; and to authenticate their travel documentation. Pursuant to several statutory mandates, the Department of Homeland Security (DHS), in consultation with the Department of State, established the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program.

As the federal government strives to integrate information on the entry and exit from the United States of foreign nationals, it is critical that the computer systems that support US-VISIT are properly protected through strong information security controls since a security breach could have a direct impact on our homeland and the security of U.S. citizens. For example, if controls for systems supporting US-VISIT were inadequately implemented there is a risk that unauthorized individuals could (1) delete or alter visitor records used or processed by US-VISIT and allow a drug smuggler, terrorist, or convicted felon to illegally enter the United States or (2) mount denial of service attacks and cripple computer processing at

[1]A port of entry is generally a physical location, such as a pedestrian walkway and/or a vehicle plaza with booths, and associated inspection and administration buildings, at a land border crossing point, or a restricted area inside an airport or seaport, where entry into the country by persons and cargo arriving by air, land, or sea is controlled by U.S. Customs and Border Protection (CBP).

U.S. air, land, and sea ports of entry as well as the networks and infrastructure that support these ports of entry.

As agreed, our objective was to determine whether the Department of Homeland Security has implemented appropriate information security controls to protect the confidentiality, integrity, and availability of the information and systems used to support the US-VISIT program. To accomplish this objective, we examined the controls over the systems operated by the United States Customs and Border Protection (CBP) that support the US-VISIT program. We performed our review at CBP facilities in the Washington, D.C. metropolitan area and selected ports of entry on the East and West Coast of the continental United States from February 2006 through April 2007, in accordance with generally accepted government auditing standards.

In a separate report designated "Limited Official Use Only," we are providing a more detailed discussion of the information security weaknesses affecting US-VISIT applications and additional technical recommendations.

Results in Brief

Significant weaknesses in computer security controls threaten the confidentiality, integrity, and availability of critical CBP information and information systems used to support the US-VISIT program. CBP did not implement controls to effectively prevent, limit, and detect access to computer networks, systems, and information. For example, it did not (1) adequately identify and authenticate users in systems supporting US-VISIT; (2) sufficiently limit access to US-VISIT information and information systems; (3) ensure that controls adequately protected external and internal boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. In addition, CBP did not always ensure that responsibilities for systems development and system production were sufficiently segregated and did not consistently maintain secure configurations on the application servers and workstations at a key data center and ports of entry. As a result, increased risk exists that unauthorized individuals could read, copy, delete, add, and modify sensitive information—including personally identifiable information—and disrupt service on CBP systems supporting the US-VISIT program.

A key reason for these weaknesses was that, although CBP made important progress in implementing elements of the department's information security program, it did not effectively or fully implement key program activities. For example, CBP did not fully characterize the risks facing critical systems, update interconnection security agreements in security plans, sufficiently test and evaluate security controls, incorporate required elements in remedial action plans, adequately implement incident detection and handling procedures, and consistently address privacy issues.

We are making six recommendations to the Secretary of Homeland Security to effectively and fully implement key information security program activities for systems supporting US-VISIT.

In written comments on a draft of this report (which are reprinted in app. I), DHS' Director of the Departmental GAO/OIG Liaison Office stated that CBP concurred with our recommendations and that CBP has already taken a number of significant steps toward mitigating many of the reported weaknesses. The director also stated that the department has directed CBP to complete remediation activities to address each of the six recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have changed the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, systems are unprotected from individuals and groups with malicious intent to intrude and use the access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. This concern is well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Recognizing the importance of securing federal agencies' information and systems, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen the security of information and systems within federal agencies.[2] FISMA requires each agency to use a risk-based approach to develop, document, and implement a departmentwide information security program for the information and systems that support the operations and assets of the agency.

Overview of the US-VISIT Program

The Congress has long recognized the need for a border security system that collects information about foreign nationals entering and exiting the United States and identifies those who have overstayed their visits. Legislative efforts to create an entry exit control system to record and match arrival and departure records for foreign nationals traveling to the United States began as early as 1996 with the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA).[3] Among other things, Section 110 of the of IIRIRA directed the former Immigration and Naturalization Service (INS) to develop an automated entry exit control system to collect records of departure from every alien leaving the United States and match it with the alien's record of arrival. In 2000, the Immigration and Naturalization Service Data Management Improvement Act[4] amended section 110 of IIRIRA by replacing it in its entirety. This act, among other things, requires that the entry exit system integrate alien arrival and departure information contained in Department of Justice (including INS) and State Department databases.

Since September 11, 2001, additional laws address, among other things, the use of biometric technology in an alien entry exit control system. For example, the USA PATRIOT Act[5] mandates that this system be capable of interfacing with other law enforcement agencies, and that it uses biometric technology and tamper-resistant documents. In addition, the Aviation and Transportation Security Act[6] requires air carriers to

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

[3]Pub. L. No. 104-208 (Sept. 30, 1996), Div. C, sec. 110.

[4]Pub. L. No. 106-215 (June 15, 2000), sec. 2(a).

[5]Pub. L. No. 107-56 (Oct. 26, 2001), sec. 414. The official title of this act is the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001.

[6]Pub. L. No. 107-71 (Nov. 19, 2001), sec. 115.

electronically transmit manifest information for all international flight passengers and crew members to the Commissioner of Customs before landing at a U.S. airport. Furthermore, the Enhanced Border Security and Visa Entry Reform Act[7] further requires the use of biometrics in travel documents and expands the passenger arrival manifest requirements in the Aviation and Transportation Security Act to sea carriers and to air and sea departures.

With the passage of the Homeland Security Act of 2002,[8] 22 federal agencies and organizations merged into the Department of Homeland Security (DHS). Shortly after DHS assumed operational control, the Secretary of the Department of Homeland Security renamed the entry exit system US-VISIT. Most recently, the Intelligence Reform and Terrorism Prevention Act of 2004[9] calls for the Secretary of the Department of Homeland Security to accelerate the full implementation of an automated biometric entry and exit data system. Among other things, the act requires the biometric entry exit screening system to provide real-time updates on all information about entry exit history to relevant agencies.

Today, the US-VISIT program is a multi-agency initiative. From fiscal year 2002 through fiscal year 2007, total funding for the US-VISIT program has been about $1.7 billion dollars.

Since fiscal year 2002, Congress has directed GAO to review annual DHS plans, also called expenditure plans, describing how the agency plans to satisfy legislative conditions specified in the appropriations, including acting and complying with federal acquisition rules, requirements, guidelines, and systems acquisition management practices. These reviews have produced five reports, the latest being a review of the fiscal year 2006

[7]Pub. L. No. 107-173 (May 14, 2002), sec 302, 303, 401 & 402.

[8]Pub. L. No. 107-296 (Nov. 25, 2002).

[9]Pub. L. No. 108-458 (Dec. 17, 2004), sec. 7208.

US-VISIT expenditure plan.[10] These reports and other recent reports on US-VISIT contract and financial management[11] and US-VISIT operations at land ports of entry have identified fundamental challenges that DHS continues to face in meeting program expectations (i.e., delivering program capabilities and benefits on time and within cost).[12] We have made many recommendations over the last 4 years to DHS to define and justify US-VISIT's future direction, strengthen program management, and ensure the delivery of promised system capabilities on time and within budget.

Goals and Purpose

The goals of the US-VISIT program are to (a) enhance the security of U.S. citizens and visitors, (b) facilitate legitimate travel and trade, (c) ensure the integrity of the U.S. immigration system, and (d) protect the privacy of our visitors. Key US-VISIT functions include:

- collecting, maintaining, and sharing information on certain foreign nationals who enter and exit the United States;
- identifying foreign nationals who (1) have overstayed or violated the terms of their admission; (2) may be eligible to receive, extend, or adjust their immigration status; or (3) should be apprehended or detained by officials;
- detecting fraudulent travel documents, verifying traveler identity, and determining traveler admissibility through the use of biometrics; and

[10]GAO, *Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning*, GAO-03-563 (Washington, D.C.: June 9, 2003); GAO, *Homeland Security: Risks Facing Key Border and Transportation Security Program Need to Be Addressed*, GAO-03-1083 (Washington, D.C.: Sept. 19, 2003); GAO, *Homeland Security: First Phase of Visitor and Immigration Status Program Operating, but Improvements Needed*, GAO-04-586 (Washington, D.C.: May 11, 2004); GAO, *Homeland Security: Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program*, GAO-05-202 (Washington, D.C.: Feb. 23, 2005); and GAO, *Homeland Security: Planned Expenditures for U.S. Visitor and Immigrant Status Program Need to Be Adequately Defined and Justified*, GAO-07-278 (Washington, D.C.: Feb. 14, 2007).

[11]GAO, *Homeland Security: Contract Management and Oversight for Visitor and Immigrant Status Program Need to Be Strengthened*, GAO-06-404 (Washington, D.C.: June 9, 2006).

[12]GAO, *Homeland Security: US-VISIT Has Not Fully Met Expectations and Longstanding Program Management Challenges Need to Be Addressed*, GAO-07-499T (Washington, D.C.: February 16, 2007).

- facilitating information sharing and coordination within the immigration and border management community.

Information Systems Supporting the US-VISIT Program

The US-VISIT program is implemented via a "system-of-systems"[13] in that the program is composed of different systems that are used to capture and store traveler information. Traveler information captured by US-VISIT includes such information as air, land, and sea port of entry admission data, commercial passenger and crew data, visa application data, and travel document (passport and visa) data. The type of data captured includes the person's complete name, date of birth, nationality, travel document issuing country, travel document number and type, applicant photo, and finger scans.[14]

The scope of the program includes the pre-entry,[15] entry,[16] status management,[17] and exit[18] of foreign national travelers who enter and leave the United States at 285 air, land, and sea ports of entry, and the provision of new analytical capabilities across the overall process. The entry aspect of the program, and the systems that support entry, are described below.

US-VISIT Port of Entry Processing

When the applicant for admission arrives at a primary inspection booth, the CBP officer, using a document reader, scans the traveler's machine-readable travel documents or manually enters the information into a biographic system if the traveler is not in possession of machine readable documents. A biographic check is then made of the traveler to identify individuals who (1) are not known to pose a threat or is not suspected of

[13]A "system of systems" is a group of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole.

[14]A finger scan is an inkless capture of finger ridge pattern images.

[15]Pre-entry refers to processes designed to evaluate a traveler's eligibility for required travel documents, enroll travelers in automated inspection programs, and pre-screen travelers entering the U.S.

[16]Entry refers to the process of determining a traveler's admissibility to the U.S. at air, land, or sea ports of entry.

[17]Status management is the process of managing and monitoring the changes and extensions of the visits of lawfully admitted non-immigrant foreign nationals to ensure that they adhere to the terms of their admission and to notify appropriate government entities when they do not.

[18]Exit refers to the process of collecting information regarding persons departing the U.S.

posing a threat to the security of the United States; (2) have not violated the terms of their admission to the United States; or (3) are not wanted for commission of a criminal act in the United States or elsewhere. In addition, a photograph and summary biographical information of the individual is also displayed in cases where the individual has been issued a travel document by the Department of State or by DHS.

Following the biographic check of the traveler by the CBP officer at the primary inspection booth, the officer then switches to a second biometric system to capture information pertaining to each traveler. The officer scans the individual's fingerprints (left and right index fingers) and takes a photograph.

While the system is checking the finger scan, the officer questions the foreign national about the purpose of his or her travel and length of stay. If the officer determines the traveler is admissible, the officer enters the class of admission[19] and duration of stay information into the system and also annotates the class of admission and "admit until" date on the I-94 form.[20]

The officer in the primary inspection booth then receives either a red or green light from the system indicating the results of the query. For example, if the query from the biographic system returns derogatory information or if the document issuance information does not match the traveler, the officer gets a red light from the system and then refers the traveler to secondary inspection for further questioning or actions. If the individual is then determined to be inadmissible in secondary inspection, the person is processed for removal or other actions.[21] This information is then entered into the system by officers at the secondary inspection area and the appropriate actions are taken.

[19]A class of admission is a specific category to which an alien lawfully enters the United States, following inspection and authorization by an immigration officer.

[20]The I-94 form is used to track the arrival and departure of nonimmigrants. It is divided into two parts. The first part is an arrival portion, which includes, for example, the nonimmigrant's name, date of birth, and passport number. The second part is a departure portion, which includes the name, date of birth, and country of citizenship.

[21]Travelers are processed by US-VISIT at primary and secondary inspection at air and sea ports of entry. At land ports of entry, visitors are only processed by US-VISIT at secondary inspection.

A green light indicates that the traveler's biometrics did not match any records in the US-VISIT biometric watch list and, in cases of repeat travelers; there was no mismatch against the biometric data captured from the traveler's prior arrival(s).

Systems Supporting US-VISIT Biographic Checks

The biographic system referred to above for the biographic check is performed by a system called the *Treasury Enforcement Communications System/ Interagency Border Inspection Service* (TECS/IBIS).[22] The IBIS "service" serves as a centralized, shared database of textual enforcement and lookout information, containing well over 10 million subject records. It supports approximately two dozen federal and other agencies[23] and it resides on a CBP mainframe computer. IBIS keeps track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. The types of data contained on the IBIS "watch list" include information from a variety of federal, state and local sources, which contributes to effective national security and law enforcement. Personal information about these individuals includes, but is not limited to, name, alias, date of birth, address, physical description, details and circumstances of a search, arrest, or seizure, case information such as merchandise and values, and methods of theft.

Other Treasury Enforcement Communication System (TECS) systems besides IBIS that support US-VISIT are the

- *Advance Passenger Information System* (APIS), a system that returns current passenger and crew manifest records on individuals arriving into and departing from the U.S. APIS includes arrival and departure manifest information provided by air and sea carriers such as name, date of birth, travel document issuing country, gender, U.S. destination address, entry date, and departure date; and
- *I-94*, a system which has information derived from I-94 arrival and departure forms.

[22]Hereafter referred to as "IBIS."

[23]Some of these agencies are the Federal Bureau of Investigation, Interpol, Drug Enforcement Administration, Bureau of Alcohol, Tobacco, and Firearms, the Internal Revenue Service, the Coast Guard, the Federal Aviation Administration, the Secret Service, and the Animal Plant Health Inspection Service. Also, information from IBIS is shared with the Department of State for use by Consular Officers at U.S. Embassies and Consulates.

CBP officers also have access to other TECS watch lists that according to US-VISIT officials are not used in conjunction with US-VISIT but are used in the border management process. For example, two systems which CBP officers have access through IBIS are (1) the *National Crime Information Center* (NCIC) database which was established by the Department of Justice as a service to all criminal justice agencies, as well as federal, state, and local users; and (2) the *National Law Enforcement Telecommunication System* (NLETS), which allows queries on state criminal history, vehicle registration, driver's license information, and administrative messages.

In addition, the Automated Targeting System–Passenger is a module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crew members prior to arrival or departure. US-VISIT officials told us that, although the system is not used in support of US-VISIT, it is used in the CBP officer's decision-making process about whether a passenger or crewmember should receive additional screening prior to entry into or departure from the country.

Systems Supporting US-VISIT Biometric Checks

The biometric[24] system behind the finger scan processing described above is complex as well. For example, after the CBP officer at the port of entry scans the fingerprints and takes a digital photograph of the visitor, the finger scans and photograph are sent to a system called the Automated Biometric Identification System (IDENT) which is managed by the US-VISIT program office.

IDENT contains information on (1) known and suspected terrorists; (2) selected wanted persons (foreign-born, unknown place of birth, previously arrested by DHS); (3) deported felons and sexual registrants; (4) certain previous criminal histories; and (5) previous IDENT border crossing enrollments. Also included in IDENT is information on persons who have attempted illegal entry into the United States, persons who have applied for immigration and naturalization benefits, and persons who have applied for positions of public trust.

IDENT checks visitors at U.S. borders against a US-VISIT biometric watch list of individuals for whom biometrics have been collected. These individuals include:

[24]In the context of US-VISIT, biometrics consists of digital inkless finger scan images and a digital photograph of the visitor.

- known or suspected terrorists,
- wanted individuals,
- deported felons, and
- individuals related to gang activity.

Information on these individuals comes from a variety of sources, including

- the Federal Bureau of Investigation,
- Interpol,
- the California Department of Justice,
- the Los Angeles County Sheriff's Office,
- the Department of Defense, and
- Department of State visa application refusals.

Each of the above organizations has its own computer systems sending data to IDENT. For example, in the case of the Department of State, IDENT receives enrollment data and visa refusal data from Consular officers abroad who collect finger scans as part of the visa issuance process. When the visa applicant's finger scans are captured, they are electronically sent, along with a digital photo of the applicant and biographic data, to the Department of State's *Consular Consolidated Database* (CCD)[25] and from CCD the finger scans and photo are sent to IDENT.[26] Information about the photo is also sent from the CCD to a TECS database called US-VISA Datashare. Information from the FBI comes to IDENT from the FBI's Integrated Automated Fingerprint Identification System.

[25]U.S. consular offices supporting US-VISIT collect biographic information, to include a photo as well as biometrics from the foreign national seeking to enter the United States and send it to the Consular Consolidated Database.

[26]The Department of State CCD connects to both TECS and IDENT. CCD collects and sends finger scans to IDENT but does not store them. IDENT is the sole repository for finger scans collected on behalf of the US-VISIT program.

The IDENT system performs three basic biometric operations: identification, verification, and enrollment. Identification consists of searching databases, such as 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" individuals into the IDENT database. IDENT also stores finger scans collected during the inspection if they are of better quality than those already stored within the system.

IDENT in turn transmits the finger scan identification numbers associated with biometrics captured at arrival in the United States to the *Arrival Departure Information System* (ADIS). *ADIS*, which is "owned" by the US-VISIT program office,[27] is a database that stores traveler arrival, status management, and departure data. Arrival and departure data is received from (1) air and sea carrier manifests; (2) inspector data entries at ports of entry; (3) I-94 forms; and (4) biometric identifiers collected at arrival and certain departure locations. It matches entry, immigration status updates, and departure data to provide up-to date immigration status, including whether the individual has overstayed his/her authorized period of stay.

ADIS also receives information from a variety of other sources. For example, information on student change of status is received from the *Student and Exchange Visitor Information System (SEVIS)*. Schools and sponsors transmit information to SEVIS via the Internet throughout a foreign student's or exchange visitor's stay in the U.S.[28] SEVIS in turn provides this information to ADIS.

Another system called the *Computer Linked Application Information Management System (CLAIMS 3)* also sends information to ADIS.

[27]However, the ADIS contract is managed by CBP.

[28]SEVIS applies to F, J, and M visa nonimmigrants and their dependents only. F visa nonimmigrants are foreign students pursuing a full course of study in a college, university, seminary, conservatory, academic high school, private elementary school, other academic institution, or language training program in the United States that has been approved to enroll foreign students. J nonimmigrants are foreign nationals who have been selected by a sponsor designated by the Department of State to participate in an exchange visitor program in the United States. M nonimmigrants are foreign students who are pursuing a full course of study in a vocational school or other recognized nonacademic institution in the United States that has been certified to enroll foreign students.

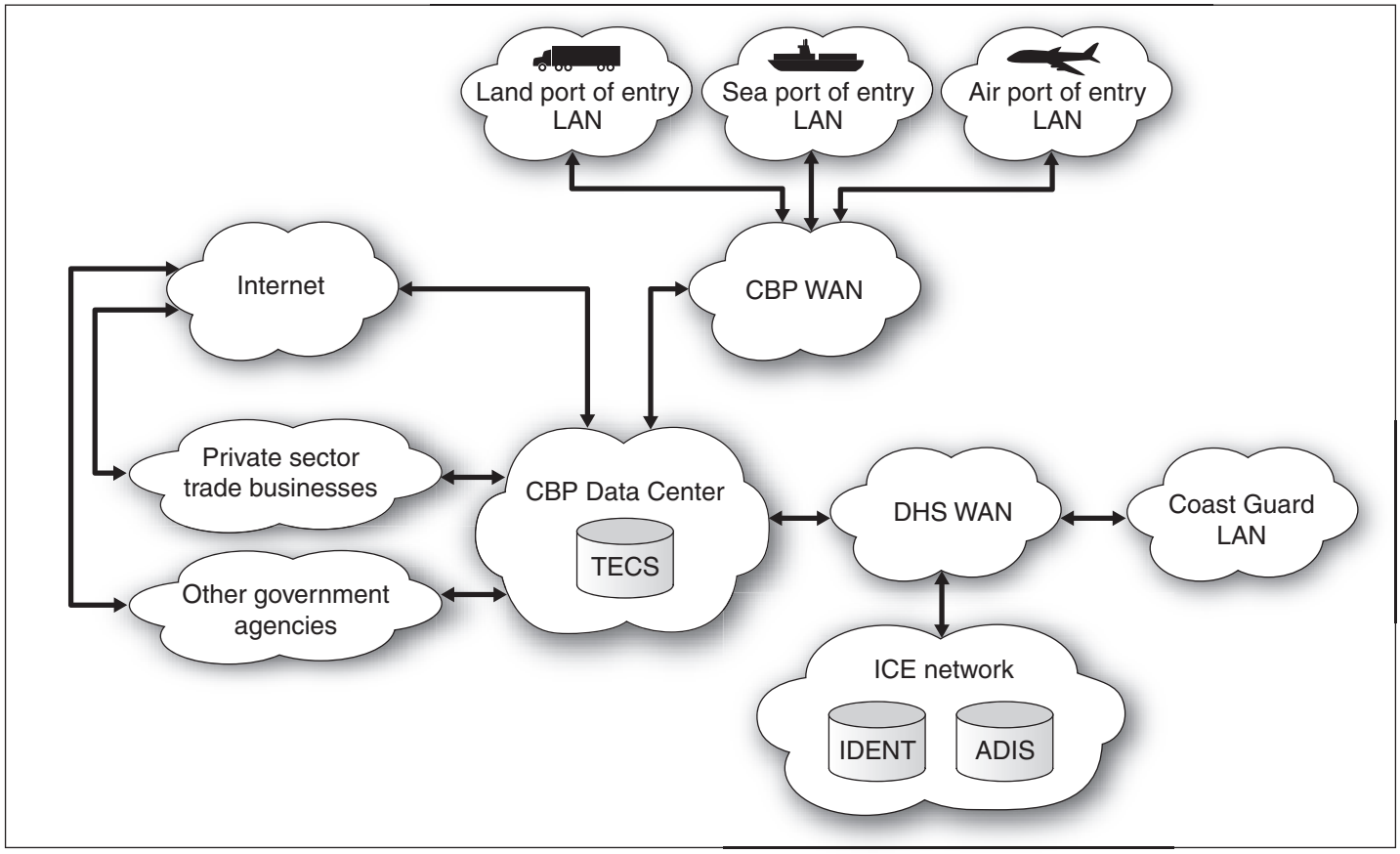
CLAIMS 3 is a system that contains information, including adjudication results on foreign nationals who request immigration benefits such as change of status, extension of stay, or adjustment to permanent resident status.

ADIS consolidates the biometric and biographic information and transmits information to TECS linking the travelers' biographic information to their biometrics. ADIS transmits this information to the TECS Biometric Information File, which includes the traveler's name, date of birth, travel document information and the associated biometric identification number.

As in the case of the biographic watchlists, the inspector has access to additional watchlists that are not part of the functionality of US-VISIT but are important in border management. For example, if a "match" is received from IDENT during primary inspection, the encounter data is stored as part of the US-VISIT process, and the traveler would be sent to secondary inspection for further action. During secondary inspection processing, the officer can access US-VISIT systems such as IDENT's Secondary Inspection Tool and ADIS to receive additional information, but the officer will also separately log into other CBP systems or interconnections such as NCIC, to retrieve the full case management information as part of the CBP border management and enforcement process.

Figure 1 is a simplified diagram of key computer systems and networks that support the US-VISIT program.

Figure 1: Simplified Diagram of Key Systems supporting US-VISIT



Source: GAO analysis.

As shown in the diagram, air, land, and sea ports of entry are connected to Customs and Border Protection local-area networks[29] which are connected to a wide-area network.[30] The wide-area network is in turn connected to a data center network which houses a mainframe computer supporting TECS. The Customs and Border Protection data center network is also connected to other networks, such as the Department's wide-area network

[29]A local area network is the cabling, hardware, and software used to connect workstations, computers, and file servers located in a confined geographical area (typically within one building or campus).

[30]A wide area network is a network that provides data communications to a large number of independent users and spans a large geographical area.

and the Immigration and Customs Enforcement network, where the IDENT and ADIS are located. Other government agencies such as the Department of State receive biometric and biographic data via the Customs and Border Protection data center network. Nongovernmental networks such as private sector trade business networks transmit passenger and crew manifest data to the data center network.

Roles and Responsibilities for Systems Supporting US-VISIT

The US-VISIT Program Office is the information system owner[31] for several of the systems that comprise US-VISIT functionality, such as the Automated Biometric Identification System and the Arrival and Departure Information System. However, the US-VISIT Program Office does not own all of the systems that support the program. For example, the

- U.S. Customs and Border Protection is the system owner for TECS,[32] the data center network, the wide-area network, and air, land, and sea port of entry local-area local-area networks;
- U.S. Immigration and Customs Enforcement is the system owner for the Student and Exchange Visitor Information System as well as the network that supports the Automated Biometric Identification System the Arrival and Departure Information System;
- U.S. Citizenship and Immigration Services is the system owner for the Computer Linked Application Information Management System;
- U.S. Coast Guard is the system owner for e-mail services; and
- The Department of State owns the Consular Consolidated Database system.

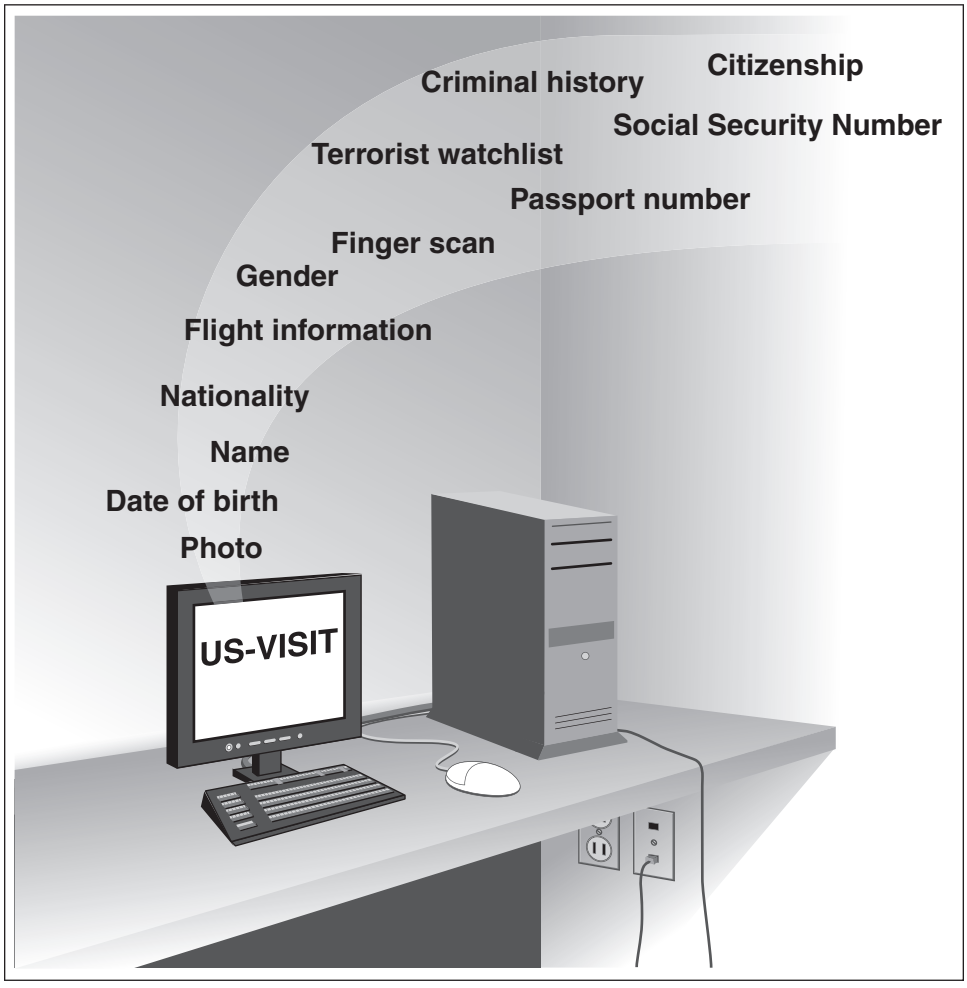
[31]The information system owner has overall responsibility for the procurement, development, integration, modification, operation, and maintenance of the information system.

[32]Some TECS components do not have a single system owner. For example, CBP officials stated that there is no one system owner for TECS/IBIS; rather it is a shared effort among all agencies that input data into it and use it.

Information and Information Systems Supporting US-VISIT Need Protection

The US-VISIT program relies extensively on computerized networks and systems to collect, access, or process a significant amount of personal and sensitive information on foreign visitors, immigrants, and legal permanent residents. Accordingly, effective information security controls are essential to ensuring that this information, depicted in figure 2, is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure or manipulation, and destruction. The compromise of this information could subject these citizens and visitors to financial crimes such as identity theft and could impede the Department of Homeland Security from achieving the goals of the US-VISIT program.

Figure 2: Types of information used by the US-VISIT program



Source: GAO analysis.

In addition, the US-VISIT program office has reported that threats to US-VISIT systems and information exist, not only because they are government assets, but also because they are a front line defense in the government's anti-terrorist identification effort. According to the program office, threats can fall into the broad categories of insiders, hackers, domestic/foreign terrorists, and other criminal elements. Because of their knowledge and access to systems, insiders are in a position to modify an individual computer system for personal gain, disrupt services, or embarrass the agency. Hackers, on the other hand, are a significant concern when connecting to the Internet. The specific attraction to US-VISIT might be to embarrass US-VISIT or gain notoriety by having defeated the security of an organization responsible for the Nation's border security. The program office also maintains that domestic or foreign terrorists are a threat since it is conceivable that these radical subversive groups could target US-VISIT to cause embarrassment to the program. Finally, other criminal elements such as international terrorists, organized crime, and foreign intelligence organizations could target US-VISIT systems to obtain US-VISIT data on various border programs.

Objective, Scope, and Methodology

The objective of our review was to determine whether DHS has implemented appropriate information security controls to protect the confidentiality, integrity, and availability of information and information systems used to support the US-VISIT program. To accomplish this, we used elements of our Federal Information System Controls Audit Manual to evaluate information system controls within the CBP control environment and concentrated our efforts on the evaluation of logical access controls over major systems, applications, and networks used by CBP in support of the US-VISIT program. Selected systems included the US-VISIT aspects of TECS, the data center mainframe that supports TECS, US-VISIT interface servers, US-VISIT client applications, and the supporting network and physical infrastructure such as servers, routers, firewalls, and workstations for CBP components supporting US-VISIT.

We reviewed results from other audits, assessments, and tests, conducted interviews, and obtained and reviewed technical documentation. In coordination with CBP officials, we identified control points and obtained detailed configuration data from selected devices. We then analyzed the output from each selected device and reviewed the results in context to the network and for impact on the mission.

In addition, we evaluated aspects of CBP's information security program. This program includes assessing risk; developing and implementing

policies, procedures, and security plans; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address security deficiencies; detecting, reporting, and responding to security incidents; and ensuring privacy for personally identifiable information. As part of this effort, we identified and examined pertinent CBP security policies, procedures, guidance, security plans, and relevant reports and reviewed corrective actions taken by CBP to address vulnerabilities identified in previous reviews and tests.

We discussed whether system controls were in place, adequately designed, and operating effectively with key security representatives, systems administrators, and management officials. Our work was performed at DHS offices, a data center, and selected air, land, sea ports of entry on the East and West coast of the continental United States in accordance with generally accepted government auditing standards.

Significant Weaknesses Place US-VISIT Data at Risk

Although CBP has implemented information security controls that are designed to safeguard US-VISIT data, its systems supporting US-VISIT have significant weaknesses in access controls and other controls designed to protect the confidentiality, integrity, and availability of its sensitive and personal information. CBP has implemented several important controls such as encrypting data transmitted between client and interface servers, deploying intrusion detection software, and performing daily backup procedures that synchronize the storage area network at a data center with its remote backup site. In addition, it controlled physical access systems for land and sea ports of entry and effectively secured some of its sensitive areas and computer equipment. However, CBP did not consistently implement effective access controls and other controls such as segregation of duties and configuration assurance for systems supporting US-VISIT. A key reason for these weaknesses was that CBP did not always effectively implement key program activities of the department's information security program for systems supporting the US-VISIT program. As a result, increased risk exists that unauthorized individuals could compromise systems that support US-VISIT.

Access Controls are Inadequate

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing access controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. These controls include identification and authentication, authorization,

boundary protection, physical security, cryptography, and audit and monitoring. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and the disruption of service.

Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. Users are also responsible for providing protection against loss or disclosure of passwords in their possession. DHS policy requires the implementation of automated identification and authentication mechanisms that enable the unique identification and authentication of individual users or processes acting on behalf of information system users.

DHS did not ensure that CBP adequately identified and authenticated users in systems supporting US-VISIT. For example, users shared passwords for accessing remote consoles, thereby diminishing CBP's ability to attribute system activity to specific individuals. Moreover, individuals with physical access to workstations could change settings without authentication. In addition, one application server owned by US-VISIT allowed logins using vendor default credentials from CBP port of entry workstations. As a result, increased risk exists that a malicious individual could gain network access to CBP systems and sensitive US-VISIT data.

Authorization

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of authorization and a basic principle for securing computer resources and data is the concept of "least privilege." Least privilege means that users are granted access to only those programs and files that they need in order to perform their official duties. To restrict legitimate users' access in this way, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that regulate which users have access to a particular file or directory and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, as well as special machine instructions which programs used

to communicate with the operating system, an organization must give careful consideration to its assignment of rights and permissions. DHS policy requires that each user or process be assigned only those privileges needed to perform authorized tasks.

CBP did not sufficiently limit access to US-VISIT information and information systems. For example, over one thousand users with command line access could put a program designed to bypass security rules into a special system library. CBP users also inappropriately had local administrator privileges on their workstations that could be used to intentionally or unintentionally load programs that may adversely affect security. In addition, CBP did not effectively use access control lists to control connectivity to sensitive applications and network devices such as firewalls.

As a result, the unnecessary level of access granted to CBP computer resources provided opportunities for individuals to circumvent security controls and deliberately or inadvertently read, modify, or delete critical or sensitive information relating to the US-VISIT program.

Boundary Protection

Boundary protections demarcate logical or physical boundaries between unknown users and protected information and systems. Best practices dictate that organizations allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces and that key components within private networks are also adequately segregated as sub-networks. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. NIST guidance states that organizations should control all remote access through a managed access control point. DHS requires that any connections to the Internet or to other external systems be through controlled interfaces. For example, DHS requires that any direct connection of DHS networks to the Internet or to extranets must occur through firewalls that have been certified and accredited.

However, DHS did not ensure that controls adequately protected external and internal boundaries. For example, internal network traffic was not segregated. Moreover, workstations and many servers did not have host based firewalls. Consequently, there is a heightened risk that security checkpoints at the boundaries of CBP's network may not inspect all traffic entering the network. As a result, increased risk exists that individuals could gain unauthorized access to sensitive information and systems.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed, and by periodically reviewing the access granted in order to ensure that it continues to be appropriate.

DHS policy requires (1) that physical access to rooms, work areas and spaces, and facilities containing departmental systems, networks, and data be limited only to authorized personnel and (2) the implementation of environmental controls that safeguard agency assets against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. CBP policy states that information assets are required to have consistent and documented protection, similar to a "defense-in-depth" concept, which means there are multiple layers of security protecting an asset.

However, CBP did not effectively implement physical security at several locations. For example, CBP did not control access to its restricted information technology spaces since its physical access systems were controlled by local authorities. In addition, sensitive information technology areas at CBP were not adequately secured and many rooms containing sensitive IT equipment had no environmental controls. As a result, these weaknesses increase the risk that unauthorized personnel could access sensitive CBP computing resources supporting US-VISIT and inadvertently or deliberately access, misuse, or destroy network resources.

Cryptography

Cryptography[33] underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. One primary principle of cryptography is encryption. Encryption can be used to provide basic confidentiality and integrity for data by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. DHS requires the encryption of highly sensitive system files.

[33]Cryptography is the discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity.

DHS did not consistently apply encryption to protect sensitive data traversing the communication network. For example, network routers, switches, and network management servers used unencrypted network protocols so that files traversing the network could be read. In addition, passwords were transmitted over the network in clear text and were stored using weak encryption. US-VISIT applications also used a single key to encrypt all communications between the clients and servers so that sensitive US-VISIT data could be compromised should the key be captured and decrypted. CBP also did not appropriately distribute its private certificate authority[34] and users relied on unknown certificates. In addition, CBP applications did not assign unique certificates and used the same certificate for both the client and the server. As a result, these weaknesses could allow an attacker to have unauthorized access to CBP network resources on the internal network and view or modify the messages between the servers and any client supporting US-VISIT.

Audit and Monitoring

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail of needed information in the desired format and locations so they can use it to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that the audit trails can provide. A key aspect of this is management of audit logs.[35] Organizations should periodically review audit log design, processes and procedures and implement changes as needed to ensure that logs effectively detect security threats.

DHS policy requires the enforcement of auditing and accountability by configuring information systems to produce, store, and retain audit records of system, application, network, and user activity. DHS also requires that audit records contain sufficient information to establish what

[34]A certificate authority is a provider that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure, a certificate authority checks with a registration authority to verify information provided by the requester of a digital certificate. If the registration authority verifies the requester's information, the certificate authority can then issue a certificate.

[35]Log management is the process for generating, transmitting, storing, analyzing, and disposing of log data.

events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome. CBP also developed and implemented a monitoring list that tracks access to key operating system libraries with programs allowed to execute restricted functions.

CBP did not provide adequate logging or user accountability for the mainframe, workstations, or servers. For example, monitoring lists for key operating system libraries on the mainframe did not capture needed data for all sensitive libraries in the desired locations. In addition, the monitoring list for key operating system libraries was out of date and irrelevant since it focused on 680 items that were no longer on the system. CBP also did not install central logging servers to ensure that key security-relevant events could be easily reviewed and safeguarded. As a result, CBP may allow unauthorized logical access to US-VISIT systems to go undetected.

Weaknesses in Other Information System Controls Increase Risks

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structures that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. DHS policy requires that segregation of duties be observed in order to eliminate conflicts of interest in the responsibilities and duties assigned to individuals.

CBP did not always ensure that responsibilities for systems development and system operations or production were sufficiently segregated. For example, development and test servers and a development code repository were on the production network. In addition, mainframe system programmers were allowed to access application production data and developmental staff could access mainframe operating system libraries. Moreover, developmental staff had update access to the application

production data. As a result, potential risk exists for these individuals to perform incompatible functions and increases the likelihood that they can corrupt critical processes.

Configuration Assurance

Configuration assurance is the process of (1) verifying the correctness of the security settings in the operating systems, applications, or computing and network devices and (2) maintaining operations in a secure fashion. Patch management is an important element in mitigating the risks associated with software vulnerabilities. When software vulnerabilities are discovered, the software vendor may develop and distribute a patch or work-around to mitigate the vulnerability. DHS patch management policy states that components shall manage systems to reduce vulnerabilities by installing patches. Both DHS and CBP policies state that security patches need to be installed on servers and desktops in a timely and expeditious manner. Outdated and unsupported software are more vulnerable to attacks and exploitation. NSA guidance also states that it is important to install periodic updates to the operating system, since these updates contain fixes to vulnerabilities.

CBP has taken steps to ensure that patches for the Windows operating systems were kept up-to-date. For example, CBP officials informed us that (1) CBP has documented its patch deployment process, manual patching procedures, and scan procedures for Windows and that (2) the Security Operations Center uses an automated tool to install patches on Windows devices within the ports of entry, the CBP wide-area network, and the CBP infrastructure.

However, CBP did not consistently maintain secure configurations on the mainframe, applications servers, and workstations we reviewed at the data center and ports of entry. For example, production servers and workstations were missing critical operating system and software application security patches. CBP also used outdated versions of software and products that were no longer supported by the vendor. Further, CBP could not implement critical security features because it had not deployed the appropriate software on some workstations.

As a result, increased risk exists that the integrity of the CBP mainframe, network devices, and administrator workstations supporting US-VISIT could be compromised and could lead to denial-of-service attacks or to individuals gaining unauthorized access to network resources.

Aggregate Effect of Weaknesses

The aggregate effect of inadequate access controls and weaknesses in other system controls place information and information systems supporting US-VISIT at increased risk of unauthorized disclosure, use, modification, or destruction, possibly without detection. These weaknesses increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information—including personally identifiable information—on systems supporting the US-VISIT program. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These acts could include tampering with data; browsing sensitive information; using computer resources for inappropriate purposes, such as launching attacks on other organizations; and disrupting or disabling computer-supported operations.

These risks are not confined to US-VISIT information. The CBP mainframe and network resources that support US-VISIT also support other programs and systems. As a result, the vulnerabilities identified in this report could expose the information and information systems of the other programs to the same increased risks.

Information Security Program Is Not Fully Implemented

A key reason for these weaknesses is that, although CBP has made important progress in implementing the department's information security program, it has not effectively or fully implemented key program activities for systems supporting the US-VISIT program.

CBP has taken several actions to implement elements of the department's information security program. For example, it has

- developed, documented, and disseminated information security policies, procedures, and plans. For example, CBP has (1) policies on security; (2) procedures for incident handling and patch management; and (3) configuration management plans;
- used Trusted Agent FISMA[36] as a tool to report component data for enterprise management and oversight of the departmentwide information security program;

[36]Trusted Agent FISMA is a DHS enterprise compliance and oversight tool used by CBP and other components to manage the collection and reporting of key information security practices and controls.

- established a central security group that monitors systems such as the ports of entry's regional local-area networks, and CBP's wide-area network;

- established a security awareness training program. CBP reported a 99 percent security awareness training completion rate for employees and contractors for fiscal year 2006;

- implemented a central data repository for its business continuity documents; and

- developed and tested continuity of operations and disaster recovery plans for recovering the production environment at CBP's data center which includes the TECS application.

DHS also requires its components to implement information security program activities in accordance with FISMA requirements, OMB policies, and applicable NIST guidance. Among other things, FISMA requires agencies to develop, document, and implement

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

- plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency;[37] and

[37]OMB requires agencies to address remedial actions through plans of action and milestones (POA&M) for all programs and systems where an information technology security weakness has been found. The plan lists the weaknesses and shows estimated resource needs, or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions.

- procedures for detecting, reporting, and responding to security incidents.

In addition, the E-Government Act of 2002 also requires agencies to conduct privacy impact assessments (PIA) for information systems to (1) ensure the system conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[38] Insofar as protecting personal privacy is an essential element of information security, the privacy impact assessment is an important means by which an agency can identify related risks and needed information security controls.

However, CBP did not fully or effectively implement these program activities. We identified risk assessments that did not fully characterize the risks facing critical systems, security plans that did not have updated interconnection security agreements, tests and evaluations of security controls that were inadequate, remedial action plans that lacked required elements, incident detection and handling procedures that had not been adequately implemented, and privacy issues that were not addressed in all cases.

Risk Assessment

Identifying and assessing information security risks are essential to determining what controls are required. By increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted. NIST guidelines state that identification of risk for IT systems require keen understanding of the system's processing environment, including data and information, system interfaces, system and data criticality, and system and data sensitivity.

CBP completed risk assessments for the CBP mainframe and the local area networks within the last 3 years and the risk assessments identify key information such as threat sources, threat actions, risk levels, and business impact as described in NIST guidelines. However, the risk assessments CBP performed for systems supporting the US-VISIT program did not always fully characterize risks to the systems. For example, the risk assessment for TECS was conducted without the benefit of (1) a

[38] *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22, Sept. 26, 2003.

completed privacy impact assessment and (2) a complete inventory of all interconnections between TECS and other systems. As a result, CBP has less assurance that risks associated with these interconnections have been properly identified and that privacy controls have been implemented to mitigate risks.

Security Plans

The purpose of an information system security plan is to provide an overview of the security requirements of the system and describe the controls that are in place or planned for meeting those requirements. According to NIST guidance, security plans should document all interconnected systems and describe the interaction among systems with regard to the authorization for the connection to other systems or the sharing of information. System interconnections, if not appropriately protected, may compromise connected systems and the data they store, process or transmit. DHS policy states that security protections for interconnected systems should be (1) documented in an interconnection security agreement approved and signed by both parties and (2) updated every three years or sooner whenever a significant change occurs to any of the interconnected systems. According to DHS policy, an interconnection security agreement is vital in protecting the confidentiality, integrity, and availability of data processed between interconnected systems.

However, 52 of the 57 interconnection security agreements listed in the TECS security plan were not current since they had not been updated within 3 years. Without updated interconnection security agreements, CBP has limited assurance that appropriate security controls have been identified and documented in system security plans. Without current and complete documentation on the interconnection of systems supporting US-VISIT, unintended access may be granted to connecting parties and there is heightened risk of compromise for connected systems and the data they store, process, or transmit.

CBP officials have acknowledged that many interconnection security agreements were not current and stated they are in the process of updating the interconnection security agreements.

Security Testing

Another key element of an information security program is testing and evaluating system controls to ensure that they are appropriate, effective, and comply with policies. FISMA requires that agencies test and evaluate the information security controls of their major systems, and that the frequency of such tests be based on risk, but occur no less than annually. NIST requires agencies to ensure that the appropriate officials are assigned roles and responsibilities for testing and evaluating controls over

systems. According to NIST, the security test results should be documented and that the objectives of testing are to (1) uncover design, implementation, and operational flaws that could allow the violation of security policy; (2) determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy; and (3) assess the degree of consistency between system documentation and its implementation. In addition, DHS has provided guidance to its component agencies on developing system test and evaluation plans, documenting the results, and using an automated tool to capture test requirements and test results. CBP test documentation did describe the vulnerabilities that we found during our audit such as the absence of one major application privacy impact assessment, the lack of the application's interconnection security agreements, and patch management problems at ports of entry's local-area networks.

However, CBP did not adequately test security controls. For example, CBP tests of a major application and the mainframe did not identify or discuss certain vulnerabilities that we identified during our audit. Moreover, its testing did not reveal problems with the mainframe that potentially allowed unauthorized users to read, copy, change, delete, and modify US-VISIT and mainframe data. In addition, although testing requirements were stated in test documentation, the breadth and depth of the test, as well as the results of the test, were not always documented. As a result, without comprehensive tests and evaluations of security controls, CBP has limited assurance that security mechanisms enforce the security policy for systems supporting US-VISIT.

CBP officials have acknowledged that there are deficiencies in how it documents, monitors, and reports test findings and stated that they are taking steps to resolve these deficiencies.

Remedial Actions

The development and implementation of remedial action plans are key components of an effective information security program. These plans assist agencies in identifying, assessing, prioritizing, and monitoring the progress in correcting security weaknesses that are found in information systems. FISMA states that agencies must develop a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies in the information security policies, procedures, and practices of the agency.

According to OMB guidance, a plan of action and milestones is a tool that identifies tasks that need to be accomplished and is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of

corrective efforts for security weaknesses found in programs and systems. The plan details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for those milestones. OMB also states that the resource estimates should include the anticipated source of funding and whether a reallocation of base resources or a request for new funding is anticipated.

DHS policy requires, among other things, that (1) all "significant" deficiencies be addressed by a remedial action plan; (2) components use the Trusted Agent FISMA tool to identify, track, and manage all IT system weaknesses and associated plans of action and milestones to closure; (3) components identify an action as completed only when a weakness has been fully resolved and the corrective action has been tested and approved; and (4) remedial action plans must identify the necessary resources to correct identified weaknesses.

However, CBP did not always address significant deficiencies in a remedial action plan as required by DHS policy. Several of these exceptions resulted in vulnerabilities or exposed US-VISIT information to increased risk of unauthorized disclosure and modification. For example, CBP patch management weaknesses that made workstations supporting US-VISIT vulnerable to attacks were not addressed in a corresponding remedial action plan. In addition, deficiencies found during security testing for the TECS application supporting US-VISIT were also not always entered in the Trusted Agent FISMA database. For example, 13 of the 19 exceptions found during security testing for one major application, were not entered in the Trusted Agent FISMA database.

CBP also did not always accurately report the status of remedial actions. Weaknesses that were only partially resolved were sometimes reported as closed on remedial action plans. For example, an Office of Inspector General recommendation that CBP perform penetration testing was marked as "completed" in the remedial action plan even though it was not addressed and penetration testing was not performed for a key port of entry application.

Furthermore, one application POA&M did not estimate the resources to correct deficiencies. For example, this application's POA&M stated that the requirement to authorize interconnections to all systems was funded in a budget but the list of required resources was described as "$0." As a result, without ensuring that remedial action plans meet established requirements, CBP has limited assurance that information system

weaknesses affecting systems supporting US-VISIT will be corrected in a timely manner.

Incident Detection and Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect and respond to them before significant damage is done. In addition, analyzing security incidents allows organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Incident reports can be used to provide valuable input for risk assessments, help in prioritizing security improvement efforts, and illustrate risks and related trends for senior management. FISMA requires that agency information security programs include procedures for detecting and reporting security incidents. Furthermore, NIST guidance prescribes network and host-based intrusion detection systems as a means of protecting systems from the threats that come with increasing network connectivity.

To ensure effective handling of incidents, DHS policy requires the establishment and maintenance of an incident handling capability that includes preparation, identification, containment, eradication, and recovery. Preparation includes developing policies and procedures, identifying supporting roles and responsibilities, and establishing and implementing tools and processes to ensure timely reporting of security incidents. Identification includes determining the cause of a suspicious event and notification to management. Containment includes mitigating the risks of continuing to operate the affected system by creating backups, keeping incident handlers informed, gathering logs for review and changing passwords. Eradication involves correcting the condition that caused the incident. Recovery involves testing and validating the system before bringing it back into production.

CBP has (1) established a Computer Security Incident Response Center which is responsible for investigating, analyzing, documenting, and resolving reported incidents; (2) implemented policies and procedures pertaining to the preparation and identification processes for handling incidents; and (3) described what should be included in interconnection security agreements such as the security policies that will be followed, how incidents will be handled, and audit trail responsibilities for interconnecting organizations.

However, CBP did not adequately establish and implement tools and processes to ensure timely detection of security incidents. For example,

the CBP data center and the ports of entry have not fully implemented host-based firewalls and intrusion detection systems on their servers and workstations that process US-VISIT information. CBP has not established centralized log collection for all CBP servers supporting US-VISIT. Moreover, CBP does not have fully documented policies and procedures for responding to security incidents. For example, at the time of our review, CBP officials stated that policies and procedures for the containment, eradication, and recovery of incidents were currently under development. As a result, without consistent detection and reporting, CBP cannot be assured that it is detecting and handling incidents in systems supporting US-VISIT in an effective manner.

Implementation of Policies Involving Personally Identifiable Information[39]

In addition to FISMA, federal agencies are subject to privacy laws aimed at preventing the misuse of personal information. The Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002 contain the major requirements for the protection of personal privacy by federal agencies. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records[40] and requires that when agencies establish or make changes to a system of records, they must notify the public by a system of records notice.[41] The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments. These privacy impact assessments include an analysis of how personal information is collected, stored, shared, and managed in a federal system.

[39]Personally identifiable information refers to any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, or biometric records, and any other personal information which is linked or linkable to an individual.

[40]The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also identifies "system of records" as a group of records under the control of any agency by the name of the individual or by an individual identifier.

[41]A system of records notice is a notice in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personal information.

According to OMB guidance, these privacy impact assessments must analyze and describe how the information will be secured including administrative and technological controls and should be current.[42] Further, DHS guidance requires them to describe how shared information is secured by the recipient and how the external system's security controls have been addressed to ensure the security of the information once it is shared. One goal of the US-VISIT program is to protect the privacy of our visitors.[43]

However, privacy documents for systems supporting US-VISIT were not current or complete. For example, DHS officials told us that the TECS system of records notice was out of date. In addition, privacy impact assessments have not been completed for other US-VISIT systems. For example, CBP did not complete assessments for two regional field local-area networks,[44] nor was an assessment approved for TECS.[45]

Without fully developing privacy impact assessments and protecting the confidentiality of personal information in its computer systems through adequate computer security controls, there is a heightened risk that disgruntled employees or malicious users could alter personal information and compromise the confidentiality, integrity, and availability of US-VISIT data, as well as the data of other applications on the mainframe.

Conclusions

CBP systems supporting the US-VISIT program were riddled with significant information security control weaknesses that place sensitive information—including personally identifiable information—at increased

[42]According to *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB Memo M-06-20, July 17, 2006, a privacy impact assessment or a system of records notice is current if that document satisfies the applicable requirements and subsequent substantial changes have not been made to the system.

[43]GAO, *Some Progress Made, but Many Challenges Remain on U.S. Visitor and Immigrant Status Indicator Technology Program*, GAO-05-202 (Washington, D.C.: Feb. 2005).

[44]CBP conducted an assessment for two of the field local-area networks and said that the local area networks did need privacy impact assessments since personal data was stored in logs; an assessment for another local area network said that no privacy impact assessment was needed because information was not stored on the network, to include audit logs.

[45]The lack of a TECS PIA was noted in the TECS risk assessment. The DHS Privacy Office determined that the mainframe on which TECS resides did not need a PIA.

risk of unauthorized and possibly undetected disclosure and modification, misuse, and destruction, and place program operations at increased risk of disruption. Weaknesses existed in all control areas and computing device types reviewed. Deficiencies in identification and authentication controls, authorization controls, boundary protection measures, physical security, use of cryptography, audit and monitoring practices, segregation of duties, and configuration assurance controls exposed CBP's mainframe computer, network infrastructure, servers, and workstations to insider and external threats. While CBP has made important progress in implementing the department's information security program, it has not taken all the steps necessary to ensure the confidentiality, integrity, and availability of the information and information systems supporting the US-VISIT program. Consequently, such information may have been disclosed to or modified by unauthorized individuals.

These weaknesses require immediate attention. Ensuring that weaknesses affecting CBP's computing resources are promptly mitigated and that controls are effective to protect US-VISIT information require senior management support and leadership, disciplined processes, effective coordination between CBP and other government organizations, and consistent oversight. Until DHS and CBP act to mitigate the weaknesses in CBP systems supporting the US-VISIT program and CBP effectively and fully implements its information security program, limited assurance exists that sensitive information will be sufficiently safeguarded against unauthorized disclosure, modification, and destruction, and that the US-VISIT program will achieve its goals.

Recommendations for Executive Action

To help the Department effectively and fully implement information security program activities for CBP systems supporting the US-VISIT program, we are recommending that the Secretary of Homeland Security direct the Commissioner, U.S. Customs and Border Protection to

1. fully characterize risks in risk assessments for systems supporting US-VISIT program;

2. update the interconnection security agreements in the TECS security plan;

3. enhance the procedures and documentation for testing and evaluating the effectiveness of security controls;

4. ensure remedial action plans address all significant security vulnerabilities, accurately report status of remedial actions, and identify necessary resources for completing actions;

5. fully develop and implement policies and tools for the timely detection and handling of security incidents; and

6. update and complete privacy documents for systems supporting the US-VISIT program.

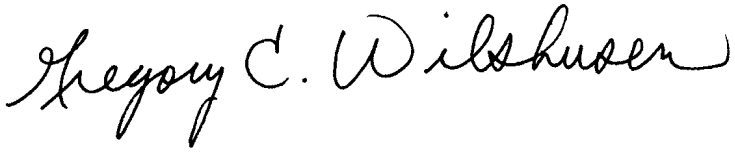
In a separate report designated limited official use only, we are making 54 detailed recommendations to the Secretary of Homeland Security to strengthen information security controls over CBP systems supporting the US-VISIT program.

Agency Comments

We received written comments on a draft of our report from DHS' Director of the Departmental GAO/OIG Liaison Office (these are reprinted in app. I). The director stated that CBP concurs with our six recommendations and that it has already taken a number of steps toward mitigating many of our findings. The director also stated that the department has directed CBP to complete remediation activities to address each of the recommendations.

As we agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Secretary of the Department of Homeland Security; the Commissioner of Customs and Border Protection; the Director of the United States Visitor and Immigrant Status Indicator Technology Program; the DHS Inspector General; and other interested congressional committees. We will also make copies available to others on request. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Keith A. Rhodes at (202) 512-6412. We can also be reached by e-mail at wilshuseng@gao.gov or rhodesk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are acknowledged in appendix II.



Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes
Chief Technologist

Appendix I: Comments from the Department of Homeland Security

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

Homeland Security

June 28, 2007

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Mr. Keith Rhodes
Chief Technologist
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen and Mr. Rhodes:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report GAO-07-870 entitled *INFORMATION SECURITY: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program.*

The draft report identified security weaknesses in information security controls for the Customs and Border Protection (CBP) systems supporting the US-VISIT program. CBP has already taken a significant number of steps toward mitigating many of GAO's findings. The weaknesses identified in the GAO report included: 1) passwords and access controls; 2) wide-area network (WAN) issues; 3) patches and updates; and 4) local-area networks (LANs).

CBP is currently in the process of upgrading its networks, systems and workstations. Once these implementations are completed, many of the GAO findings will be closed. CBP expresses its commitment to making the necessary improvements that have been identified in this draft report and concurs with GAO's six recommendations.

The Department has directed CBP to complete remediation activities to address each of the six recommendations. An initial response to the recommendations is provided in an enclosure to this letter.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Enclosure

RESPONSE TO GAO RECOMMENDATIONS

Recommendation 1: Fully characterize risks in risk assessments for systems supporting US-VISIT program.

Response: US-VISIT will review their Risk Assessments (RA) and work with CBP to understand their remediation plans. Should any residual risks remain, CBP and US-VISIT will document for review by the US-VISIT mission owner.

Recommendation 2: Update the interconnection security agreements in the Treasury Enforcement Communications System (TECS) security plan.

Response: CBP will update the TECS System Security Plan to include all interconnection security agreements.

Recommendation 3: Enhance the procedures and documentation for testing and evaluating the effectiveness of security controls.

Response: CBP will review its compliance with the Department's policy and procedures for annual testing of 800-53 controls. CBP will additionally review its scan requirements for high impact systems and address compliance monitoring.

Recommendation 4: Ensure remedial action plans address all significant security vulnerabilities, accurately report status of remedial actions, and identify necessary resources for completing actions.

Response: CBP will review all security vulnerabilities identified in the GAO report to ensure that Plans of Actions and Milestones (POA&M) are opened for each recommendation and remedial actions tracked to completion.

Recommendation 5: Fully develop and implement policies and tools for the timely detection and handling of security incidents.

Response: CBP will continue to improve its incident detection, incident reporting and incident handling procedures. CBP currently leverages a variety of tools to assist with security incident handling to include intrusion detection systems, anti-virus software, and event correlation systems. Process documentation will be updated to reflect the required improvements.

Recommendation 6: Update and complete privacy documents for systems supporting the US-VISIT program.

Response: US-VISIT will work with their Privacy Points of Contact (PPOC) to update any US-VISIT privacy impact assessments (PIAs) which have not been completed.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov
Keith A. Rhodes, (202) 512-6412, rhodesk@gao.gov

Staff Acknowledgments

In addition to the individuals named above, William F. Wadsworth; Bruce E. Cain; Jason A. Carroll; Lon C. Chin; West E. Coile; Kirk J. Daubenspeck; Neil J. Doherty; Patrick R. Dugan; Denise E. Fitzpatrick; Edward M. Glagola Jr.; Kory W. Godfrey; Mustafa S. Hassan; David B. Hayes; Kaelin P. Kuhn; Vernetta Y. Marquis; Kevin C. Metcalfe; Jennifer U. Mills; Tammi L. Nguyen; Ronald E. Parker; David F. Plocher; John A. Spence; Henry I. Sutanto; Amos A. Tevelow; and Christopher J. Warweg, made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548