

January 2009

# INFORMATION SECURITY

## Further Actions Needed to Address Risks to Bank Secrecy Act Data



GAO

Accountability \* Integrity \* Reliability



Highlights of [GAO-09-195](#), a report to congressional requesters

## Why GAO Did This Study

The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, relies extensively on its own computer systems, as well as those at the Internal Revenue Service (IRS) and the Treasury Communications System (TCS), to administer the Bank Secrecy Act (BSA) and fulfill its mission of safeguarding the U.S. financial system from financial crimes. Effective information security controls over these systems are essential to ensuring that BSA data, which contains sensitive financial information used by law enforcement agencies to prosecute financial crime, is protected from inappropriate or deliberate misuse, improper disclosure, or destruction.

GAO evaluated whether security controls that effectively protect the confidentiality, integrity, and availability of the information and systems that support FinCEN's mission have been implemented. To do this, GAO examined security policies and controls for systems at three organizations.

## What GAO Recommends

GAO recommends that the Secretary of the Treasury direct the FinCEN Director to take several actions to fully implement an effective agencywide information security program. In commenting on a draft of this report, Treasury agreed to develop a detailed corrective action plan for each of the recommendations.

To view the full product, including the scope and methodology, click on [GAO-09-195](#). For more information, contact Nancy Kingsbury at (202) 512-2700 or [kingsburyn@gao.gov](mailto:kingsburyn@gao.gov), or Gregory C. Wilshusen at (202) 512-6244 or [wilshusen@gao.gov](mailto:wilshusen@gao.gov).

## INFORMATION SECURITY

### Further Actions Needed to Address Risks to Bank Secrecy Act Data

#### What GAO Found

FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission; however, significant information security weaknesses remain in protecting the confidentiality, integrity, and availability of these systems and information. The three organizations implemented many information security controls to protect the information and systems that support FinCEN's mission. For example, IRS controlled changes to a key application and FinCEN segregated areas of its network. Nonetheless, the organizations had inconsistently applied or not fully implemented controls to prevent, limit, or detect unauthorized access to this information and these systems. For example, the organizations did not always (1) implement user and password management controls for properly identifying and authenticating users, (2) restrict user access to data to only what was required for performing job functions, (3) adequately encrypt data, (4) protect the external and internal boundaries on its systems, and (5) log user activity on databases. Furthermore, weaknesses in which systems were insecurely configured and patches were not applied to critical systems also existed. As a result, sensitive information used by the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing is at an increased risk of unauthorized use, modification, or disclosure.

A key reason for many of the weaknesses was that FinCEN and IRS had not fully implemented key information security program activities. For example, FinCEN did not always include detailed implementation guidance in its policies and procedures and adequately test and evaluate information security controls. Furthermore, GAO has previously reported that IRS did not sufficiently verify whether remedial actions were implemented or effective in mitigating vulnerabilities and recommended that it implement a revised remedial action verification process.

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	2
	Background	3
	FinCEN, TCS, and IRS Had Not Fully Implemented Appropriate Security Controls and Practices to Protect Information and Systems Supporting FinCEN's Mission	9
	Conclusions	26
	Recommendations for Executive Action	26
	Agency Comments	27
<b>Appendix I</b>	<b>Objective, Scope, and Methodology</b>	<b>29</b>
<b>Appendix II</b>	<b>Comments from the Department of the Treasury</b>	<b>32</b>
<b>Appendix III</b>	<b>GAO Contacts and Staff Acknowledgments</b>	<b>33</b>
<b>Figure</b>		
	Figure 1: BSA Environment Operational Relationships and Data Flow	8

---

---

## Abbreviations

BSA	Bank Secrecy Act
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TCS	Treasury Communications System
Treasury	Department of the Treasury
WebCBRS	Web-based Currency and Banking Retrieval System

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

January 30, 2009

The Honorable Barney Frank  
Chairman  
The Honorable Spencer Bachus  
Ranking Member  
Committee on Financial Services  
House of Representatives

The Honorable William Lacy Clay  
House of Representatives

The Honorable Stephen F. Lynch  
House of Representatives

As the administrator of the Bank Secrecy Act (BSA),<sup>1</sup> the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury (Treasury), is tasked with the mission of safeguarding the U.S. financial system from money laundering, terrorist financing, and other abuses. In fulfilling this mission, FinCEN performs analysis in support of law enforcement; issues regulations and enforces compliance with the BSA; facilitates information-sharing of BSA data; and coordinates with foreign counterparts.

FinCEN relies extensively on its own information systems, as well as on systems located at the Treasury components of the Internal Revenue Service (IRS) and the Treasury Communications System (TCS) to manage, store, and disseminate the data that financial institutions are required to report under the BSA. These data contain sensitive information, including transaction amounts, account numbers, and social security numbers, and are used by law enforcement agencies investigating financial crimes, including terrorist financing and money laundering. The computer systems that support FinCEN's mission must be properly protected through strong

---

<sup>1</sup>Bank Secrecy Act, Titles I and II of Pub. L. No. 91-508, 84 Stat. 1114 (1970), as amended, codified at 12 U.S.C. §§ 1829b, 1951-1959, and 31 U.S.C. §§ 5311-5322.

---

information security controls<sup>2</sup> because a security breach could place sensitive financial and personally identifiable information at risk and allow criminals to subvert law enforcement's ability to detect illegal activity.

Our objective was to determine whether information security controls have been implemented that effectively protect the confidentiality, integrity, and availability of the information and systems that support FinCEN's mission. To accomplish this objective, we examined the information security controls at FinCEN and two organizations that operate systems or process and store data on its behalf—specifically, TCS and IRS. We concentrated our evaluation on the applications, databases, and network and mainframe infrastructure that support FinCEN's mission. We performed our review at FinCEN and TCS facilities in the Washington, D.C., metropolitan area and at an IRS computing center.

We conducted this performance audit from March 2008 to January 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. For more details on our objective, scope, and methodology, see appendix I.

---

## Results in Brief

Although FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission, significant weaknesses existed that impaired their ability to ensure the confidentiality, integrity, and availability of these information and systems. The organizations have implemented many security controls to protect the information and systems. For example, FinCEN employed controls to segregate areas of its network and restrict access to sensitive areas, and IRS controlled changes to a key application in its BSA processing environment. However, weaknesses existed that placed sensitive data at risk of unauthorized disclosure. The organizations did not always consistently apply or fully

---

<sup>2</sup>Information security controls include access controls, configuration management, patch management, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, that systems are configured appropriately, that systems are protected against known vulnerabilities, and that back-up and recovery plans are adequate to ensure the continuity of essential operations.

---

implement controls to prevent, limit, or detect unauthorized access to devices or systems. For example, the organizations had not consistently or fully (1) implemented user and password management controls for properly identifying and authenticating users, (2) restricted user access to data to permit only the access needed to perform job functions, (3) encrypted data, (4) protected external and internal boundaries, and (5) logged user activity on key systems. Shortcomings also existed in managing system configurations, patching systems, and planning for service continuity. As a result, increased risk exists that unauthorized individuals could read, copy, delete, add, and modify data and disrupt service on systems supporting FinCEN's mission.

A key reason for many of the weaknesses was that FinCEN and IRS had not fully implemented key information security program activities. For example, FinCEN did not always include detailed implementation guidance in its policies and procedures or adequately test and evaluate information security controls. Furthermore, IRS did not sufficiently verify whether actions taken to remedy or mitigate known vulnerabilities were fully implemented or effective.

To help strengthen information security controls over the information and systems supporting FinCEN's mission, we are making five recommendations to the Secretary of the Treasury to direct the Director of FinCEN to fully implement key information security program activities. We also are making 88 recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct the specific information security weaknesses at FinCEN, TCS, and IRS.

In commenting on a draft of this report, Treasury's Deputy Assistant Secretary for Information Systems and Chief Information Officer stated that securely maintaining BSA information contributes to the department's goal of promoting the nation's security through strengthened financial systems. He also stated that Treasury will provide a detailed corrective action plan for each of the recommendations and noted that many of the actions required to address the recommendations are already completed or under way.

---

## 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 the public's trust is essential. The dramatic expansion in computer

---

interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, they also pose enormous risks that make it easier for individuals and groups with malicious intent to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

Our previous reports, and those by inspectors general, describe serious and widespread information security control deficiencies that continue to place federal assets at risk of inadvertent or deliberate misuse, mission-critical information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,<sup>3</sup> a designation that remains in force today.<sup>4</sup>

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and systems within federal agencies.<sup>5</sup> FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risks; developing and implementing security plans, policies, and procedures; providing security awareness and specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

---

<sup>3</sup>GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

<sup>4</sup>GAO, *High-Risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

<sup>5</sup>FISMA was enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946 (Dec. 17, 2002).



---

## The BSA and FinCEN

The BSA, enacted by Congress in 1970, authorizes the Secretary of the Treasury to issue regulations requiring financial institutions to retain records and file reports useful in criminal, tax, and regulatory investigations. Following the September 11, 2001, terrorist attacks, Congress passed the USA PATRIOT Act, which, among other things, amended the BSA to expand the number of industries subject to BSA regulation and required financial institutions to establish proactive anti-money laundering programs to combat terrorist financing.<sup>6</sup> In addition, the USA PATRIOT Act expanded reporting requirements and allowed the records and reports collected under the BSA to be used in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

As the administrator of the BSA, FinCEN, a bureau within Treasury, is tasked with the mission of safeguarding the U.S. financial system from money laundering, terrorist financing, and other abuses. In fulfilling this mission, FinCEN plays four key roles: (1) performing analysis in support of law enforcement; (2) issuing regulations and enforcing compliance; (3) facilitating information-sharing of BSA data; and (4) coordinating with foreign counterparts. Providing analysis was FinCEN's original mission when it was established in 1990, a role that it continues to perform. In its capacity as regulator, FinCEN develops regulations and delegates authority to eight other federal agencies to perform compliance examinations for BSA reporting requirements for referral to FinCEN, which retains enforcement authority. In terms of information-sharing, sections 361 and 362 of the USA PATRIOT Act mandate that FinCEN create and maintain networks to enable electronic filing of BSA reports and facilitate dissemination of the data to law enforcement and regulatory agencies. In addition, FinCEN participates in and promotes international collaboration and information-sharing among its foreign counterparts to detect and deter illicit financial activities. Between fiscal years 2002 and 2007, FinCEN's budget grew from \$47.5 million to \$73.2 million. According to FinCEN, this growth has taken place primarily because of the expansion of its regulatory functions.

### Information That Supports FinCEN's Mission

FinCEN relies on information submitted under BSA reporting requirements to fulfill its mission. Specifically, FinCEN collects information submitted and disseminates it to law enforcement and regulatory agencies. The information primarily consists of Currency

---

<sup>6</sup>USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

---

Transaction Reports and Suspicious Activity Reports that are filed by financial institutions. Currency Transaction Reports must be filed for any account cash withdrawals and deposits, currency exchanges, and wire transfers purchased with cash exceeding \$10,000. Suspicious Activity Reports must be filed by financial institutions if a transaction involves or aggregates a minimum threshold<sup>7</sup> of funds or other assets and the institution knows, suspects, or has reason to suspect that the transaction is a violation of law. Law enforcement agencies use the information in these reports in combination with other information that they collect to link individuals and their activities, hinder activities, and prosecute criminals. Financial regulators, such as the Federal Deposit Insurance Corporation and the National Credit Union Administration, use the information to examine financial institutions for compliance with the BSA.

Currency Transaction Reports and Suspicious Activity Reports contain highly sensitive, detailed information about the financial activity of private individuals<sup>8</sup> that is intended to help federal, state, and local law enforcement agencies in their investigations and, thus, potentially hinder criminal activity. Inappropriate disclosure, modification, or misuse of this information could undermine the ability of the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing.

## Information Systems That Support FinCEN's Mission

Information systems located at FinCEN, TCS, and IRS comprise the overall computing environment where BSA information is collected, processed, stored, disseminated, and protected in support of FinCEN's mission. In its own computing environment, FinCEN maintains a Web portal by which law enforcement agencies, regulatory agencies, and FinCEN employees access BSA data. It also has an analysis tool that it uses to provide analyses to law enforcement customers and a database containing a copy of the BSA database maintained by IRS. These systems reside on FinCEN's

---

<sup>7</sup>31 U.S.C. § 5318(g)(1) and 31 C.F.R. §§ 103.15–103.21. Depending on the type of financial institution, the threshold amount may vary. For example, money services businesses generally must file a Suspicious Activity Report if a transaction involves or aggregates \$2,000 in funds or other assets. Suspicious Activity Report forms must be filed for certain suspicious transactions involving possible violations of law or regulation, including transactions that are broken up for the purpose of evading the BSA reporting and record-keeping requirements.

<sup>8</sup>In addition to the dollar amount of the cash transaction, these reports may record other sensitive information, including the name of the account owner; the name of the person actually conducting the transaction (if not the account holder); social security numbers; driver's license or identification numbers; and account numbers.

---

## Information Flow in the BSA Environment

network infrastructure. Additional systems are operated at TCS, including the electronic filing system and the supporting TCS network infrastructure. FinCEN's electronic filing system is operated on the TCS network under a hosting agreement. FinCEN also relies on systems operated by IRS, including the BSA database and the Web-based Currency Banking and Retrieval System (WebCBRS). WebCBRS and the database reside on a mainframe computer and supporting network infrastructure at an IRS computing facility.

The information in BSA reports submitted by financial institutions comprise the data that is stored in the BSA database at IRS. Most reports<sup>9</sup> are submitted electronically, either singly or in batch form, over the Internet to the electronic filing system; FinCEN moves this data through its network infrastructure and passes them to IRS. Reports submitted in paper form are mailed directly to IRS; they are then forwarded to a contractor, who converts the reports into digital format and returns them electronically. IRS personnel then manually upload the data to the database.

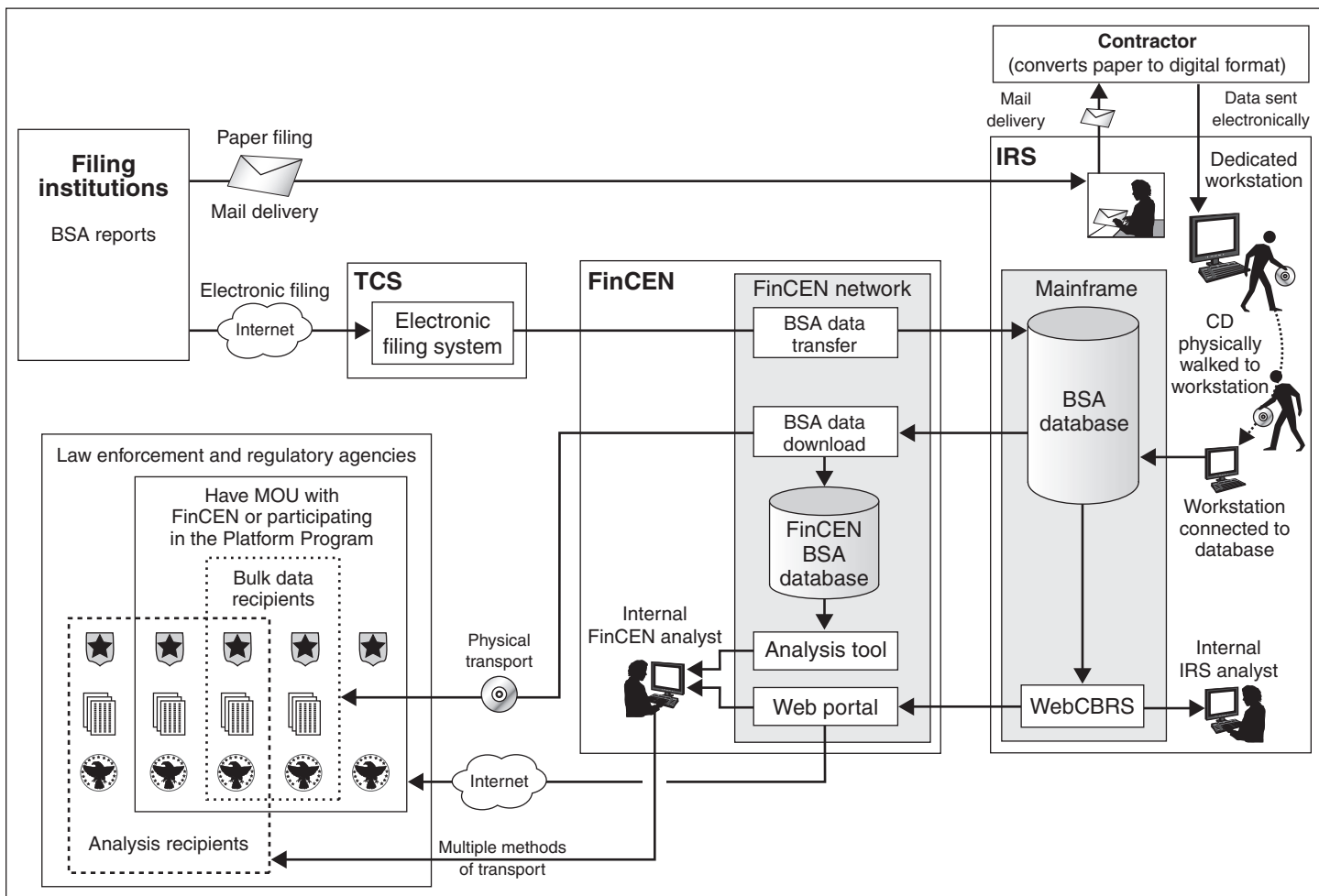
BSA data are provided to law enforcement and regulatory agencies in multiple ways. Organizations may access the data through FinCEN's Web portal, which provides access to the WebCBRS application. These organizations either have a memorandum of understanding with FinCEN, which allows them to access the portal remotely through the Internet, or participate in FinCEN's Platform Program, which allows them to access the portal on-site at FinCEN. In addition, certain federal agencies also periodically receive bulk downloads of BSA data for use at their agencies. FinCEN also has its own analysis tool that it uses to provide investigative leads to support financial criminal investigations and produce a variety of analytical products that can be used by law enforcement to more effectively target their investigations. Organizations may request that FinCEN analysts assist with their investigations by conducting queries or analyses on their behalf. Some internal IRS analysts and investigators also have direct access to WebCBRS to support compliance examinations for nonbank financial institutions and investigations of money laundering and other tax-related crime.

---

<sup>9</sup>According to FinCEN, approximately 71 percent of BSA submissions are made through the electronic filing system.

The flow of data through the overall BSA environment is illustrated in figure 1.

**Figure 1: BSA Environment Operational Relationships and Data Flow**



Source: GAO analysis of agency data.

## Security Responsibilities

Treasury’s Chief Information Officer is responsible for developing and maintaining a departmentwide information security program and for developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements. Each Treasury bureau, including FinCEN and IRS, is responsible for implementing Treasury-mandated security policies within its domain. In order to

---

implement departmentwide security policies, FinCEN and IRS are required to develop their own information security programs, including their own security compliance functions.

In addition, the organizations operating the systems that support FinCEN's mission have formalized agreements that define security responsibilities. For example, FinCEN's hosting agreement with TCS documents security prerequisites and the responsibilities of TCS as the host network. Additionally, FinCEN and IRS have an interconnection security agreement that identifies the technical requirements of the interconnection between the FinCEN network and the IRS systems that store and process the data. The agreement specifies that FinCEN owns the data and indicates that the environment where the data resides is to be logically isolated from the other systems at IRS.

---

## **FinCEN, TCS, and IRS Had Not Fully Implemented Appropriate Security Controls and Practices to Protect Information and Systems Supporting FinCEN's Mission**

Although FinCEN, TCS, and IRS had implemented many information security controls to protect the information and systems supporting FinCEN's mission, weaknesses existed in several critical areas. Specifically, the organizations did not consistently implement effective electronic access controls, including user accounts and passwords, access rights and permissions, encryption of sensitive data, protection of information system boundaries, audit and monitoring of security-relevant events, and physical security to prevent, limit, and detect access to their critical financial and sensitive systems. In addition, weaknesses in other information system controls, including managing system configurations, patching sensitive systems, and service continuity, further increase the risk to the information and systems that support FinCEN's mission. One key reason for these weaknesses was that FinCEN and IRS had not yet fully implemented key elements of their information security programs. As a result, BSA data—containing highly sensitive personal and financial information about private individuals that is used by the law enforcement community to identify and prosecute illegal activity—are at an increased risk of unauthorized use, modification, or disclosure.

---

## **Some Access Controls Had Been Implemented, but Significant Weaknesses Remained**

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 controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure,

---

Policies for Identifying and Authenticating Users Were Established, but Were Not Always Consistently Implemented

---

modification, and destruction of sensitive information and disruption of service. Access controls include those related to (1) user identification and authentication, (2) authorization, (3) cryptography, (4) boundary protection, (5) audit and monitoring, and (6) physical security. Weaknesses in each of these areas existed across the BSA environment, as the following sections in this report demonstrate.

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. FinCEN policy states that user IDs and passwords should not be shared. National Institute of Standards and Technology (NIST) guidance states that information systems should prohibit passwords from being reused for a specified number of generations and that complex passwords reduce the risk that a password could be guessed by an attacker. IRS requires that passwords not be shared, that each account have a unique user ID, and that default mainframe passwords be changed when information systems are installed.

Weaknesses in identification and authentication controls existed over the information and systems supporting FinCEN's mission at FinCEN, TCS, and IRS, including the following:

- Although FinCEN had established policies for identifying and authenticating users and required complex passwords on its databases, it allowed multiple users to share an account on the dedicated workstation used to download BSA data from IRS.
- TCS also had not consistently implemented effective password controls. For example, three accounts on a key database, including an administrative account, had passwords that were not complex, making them easily guessable. Additionally, the electronic filing application did not lock out user accounts after a specific number of unsuccessful log-in attempts.
- IRS did not always effectively control user identification and authentication. For example, it did not change easily guessable default passwords for two special purpose accounts that provided interactive

---

mainframe privileges, access to BSA data, and powerful processing capabilities.

As a result of these weaknesses, there is an increased risk that malicious individuals could gain inappropriate access to sensitive BSA applications and data.

### User Access to Sensitive Data Was Not Always Appropriately Authorized

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, directories, and special machine instructions that programs use to communicate with the operating system, an organization must give careful consideration to its assignment of rights and permissions.

FinCEN requires that access to resources be given only to users who need it, that managers re-evaluate the system privileges granted to users at least once every 6 months, and that all system privileges and access to information immediately cease when employees leave the organization. Additionally, IRS requires that information systems uniquely identify users that access sensitive information and that such access be given only to those employees with a valid need to know.

Weaknesses in authorization controls existed at FinCEN and TCS that could place the information and systems that support FinCEN's mission at risk, as the following examples indicate:

- FinCEN did not always adequately restrict access to sensitive files. The bureau had assigned rights and permissions to network users; however, it did not consistently protect all network resources. For example, it assigned excessive permissions to a shared network drive that stored BSA data received from IRS. In addition, FinCEN managers did not re-evaluate user privileges every 6 months. Further, two former employees retained access to the Web portal for at least 2 weeks after they left FinCEN.

- 
- Additionally, TCS did not consistently ensure that access to resources was appropriate. For example, it did not restrict access to log files and other operating system files associated with the electronic filing application to only those who needed the access to perform their jobs, increasing the risk that data could be accessed by unauthorized users or that malicious activity could potentially go undetected. In addition, it allowed users direct access to a shared administrative account, making it difficult to establish individual accountability for privileged activities.

More serious authorization control weaknesses existed over the information and systems supporting FinCEN's mission operated by IRS, including the following:

- IRS did not implement controls to restrict access to data and systems to only those who needed it. IRS and FinCEN created a memorandum of understanding and an interconnection security agreement in which IRS agreed to secure the systems and data supporting FinCEN by isolating them from other systems and controlling IRS user access to the systems and data through a dedicated network. However, IRS did not isolate the systems and data from its other systems and had not restricted user access to the systems and data via a dedicated network. Instead, other paths allowed any of its employees to gain access without detection, most of whom did not have a legitimate need for such access:
  - IRS allowed more than 600 IRS employees to have privileges on the mainframe supporting FinCEN's mission that they did not need in order to do their jobs; the privileges allowed them to interactively enter commands into the system and perform activities that are usually associated with programming and system administration.
  - Mainframe files had excessive permissions that could allow their contents to be read or copied by any user able to gain interactive access to the mainframe.
  - The systems supporting FinCEN's mission shared their data storage devices with other IRS systems, allowing users with interactive access to the mainframe the ability to view information about the BSA related datasets, including their location, even though most of them did not have a job-related need for this information.
  - Additionally, IRS did not maintain documentation of approved access privileges allowed to each system resource by each user group on its systems supporting FinCEN's mission, limiting IRS's ability to monitor and verify access privileges.



---

FinCEN Employed Encryption,  
but Sensitive Data Were Not  
Always Adequately Protected

By allowing access to information and systems to individuals who do not have a legitimate job-related need, FinCEN, TCS, and IRS are placing these data and systems at increased risk of unauthorized access or disclosure, which could hinder FinCEN's ability to fulfill its mission.

Cryptography<sup>10</sup> 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. FinCEN requires that sensitive information must be encrypted when it is transmitted or stored. In addition, IRS requires the use of insecure protocols to be restricted on its systems in order to protect passwords and other sensitive data.

Weaknesses in encryption controls over the information and systems supporting FinCEN's mission at FinCEN and IRS could place sensitive data at risk, as the following examples indicate:

- Although FinCEN employed encryption mechanisms to protect data on its network and workstations, not all sensitive data were encrypted. FinCEN employed software to encrypt data on removable flash drives. However, user IDs and passwords for a key system were transmitted unencrypted across the FinCEN network, making them vulnerable to being compromised and used to gain unauthorized access. Additionally, although FinCEN encrypted the hard drives on its laptop computers, the encryption software did not protect data after the computers had been booted to a running state.
- IRS did not always secure the transmission of information on its network. For example, user IDs and passwords for the mainframe were transmitted unencrypted over the network, making them vulnerable to being compromised. In addition, it did not use certificates to ensure that the encrypted communications path between its network and the BSA database could be trusted.

---

<sup>10</sup>Cryptography is the discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, nonrepudiation, and authenticity.

---

FinCEN and TCS Implemented Boundary Protection and Intrusion Detection Controls, but Weaknesses Remained

As a result, weaknesses in encryption increased the risk of exposing data at FinCEN and IRS to unnecessary disclosure or misuse by unauthorized individuals.

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 subnetworks with separate physical network interfaces and that key components within private networks are also adequately segregated as subnetworks. 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 also the risk of unauthorized access in a shared environment. NIST guidance states that information systems should establish a trusted communications path between remote users, that firewalls should control both outgoing and incoming network traffic, and that boundary mechanisms separate computing systems and network infrastructures. In addition, IRS requires that test and production environments be kept separate.

Although FinCEN and TCS had employed controls to segregate sensitive areas of their networks and protect them from intrusion, the organizations did not always adequately control the logical and physical boundaries protecting information and systems supporting FinCEN's mission, as the following examples indicate:

- FinCEN had not fully implemented controls to protect the boundaries of its network. For example, FinCEN did not configure its virtual private network<sup>11</sup> with controls to validate whether the systems that connected to it were secure. In addition, it did not employ host-based firewalls on its workstations.
- TCS also did not always control the logical and physical boundaries protecting the systems supporting FinCEN. For example, TCS stored sensitive files on a network segment that was less secure than other

---

<sup>11</sup>A virtual private network is a private network that is maintained across a shared or public network, such as the Internet, by means of specialized security procedures. Virtual private networks are intended to provide secure connections between remote clients, such as branch offices or traveling personnel, and a central office.

---

segments. In addition, the TCS e-mail server allowed spoofed e-mail messages<sup>12</sup> and potentially harmful attachments to be delivered to FinCEN.

- IRS did not restrict the processing of sensitive data on its systems that support FinCEN. For example, updates to libraries containing key control programs and source code and creation and deletion of datasets containing BSA information were submitted from areas of the mainframe that did not support FinCEN. In addition, some of this processing originated from a test environment.

As a result, there is an increased risk that individuals, internal and external to FinCEN, TCS, and IRS, could gain unauthorized access to the information and systems that support FinCEN's mission.

#### Audit and Monitoring Controls Were Implemented, but They Did Not Always Capture Key Events

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 process is managing audit logs.<sup>13</sup> Organizations should periodically review audit log design, review processes and procedures, and implement changes as needed to ensure that logs effectively detect security incidents.

FinCEN requires audit logs to be maintained for all information systems and for unsuccessful log-in attempts to be recorded; in addition, it requires intrusion detection systems<sup>14</sup> to be employed to protect the network from external threats. Similarly, IRS policy requires that audit records be

---

<sup>12</sup>E-mail spoofing occurs when a user receives e-mail that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

<sup>13</sup>Log management is the process for generating, transmitting, storing, analyzing, and disposing of log data.

<sup>14</sup>An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems.

---

created, protected, and retained to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

Weaknesses in audit and monitoring controls existed over the systems supporting FinCEN's mission at FinCEN and IRS, including the following:

- FinCEN logged user activity for two key applications; however, it did not always log security events on its databases. For example, the bureau did not enable auditing on the FinCEN BSA database and did not log failed log-in attempts to the database's error logs. In addition, its intrusion detection systems did not capture data from complete sessions or inspect outbound encrypted traffic.
- IRS did not effectively capture changes to datasets on its mainframe. Specifically, it did not configure its security software to log successful changes to key datasets that contain parameters and procedures used to support production operations of the operating system, system utilities, and user applications, including WebCBRS.

As a result of weaknesses in logging and monitoring controls at FinCEN and IRS, there is an increased risk that unauthorized activity would not be effectively detected or investigated.

#### FinCEN Controlled Physical Access to Sensitive Areas, but Did Not Control Laptop Computers Entering and Exiting Its Facility

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. FinCEN's physical security policy requires that access to sensitive areas be restricted to authorized personnel and that all information system-related items, including laptop computers, are to be monitored and controlled when they enter or leave FinCEN.

Although FinCEN controlled access to sensitive areas, it did not always implement a physical security control. FinCEN implemented an electronic badging system to control access to sensitive areas. However, at the time of our site visits, security guards at the FinCEN facility did not inspect laptop computers entering and exiting the facility. Controlling the entry and exit of laptop computers would reduce the risk that a malicious individual could introduce malware onto the FinCEN network or that sensitive data could be taken off site without authorization.

---

## Other Information Security Weaknesses Existed

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of an organization's information. These controls include policies, procedures, and techniques for (1) ensuring continuity of computer processing operations in the event of a disaster or unexpected interruption; (2) securely configuring information systems and preventing unauthorized changes to systems; and (3) protecting systems from known vulnerabilities. Weaknesses in these control areas increased the risk of unauthorized use, disclosure, modification, or loss of sensitive information and information systems supporting FinCEN's mission.

## FinCEN Documented Contingency Plans for Major Systems, but the Plans for High-Risk Systems Were Not Fully Tested

Continuity of operations planning, which includes contingency planning, is a critical component of information protection. Continuity planning controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and that critical and sensitive data are protected. These controls include (1) environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions and (2) a well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. NIST guidance states that contingency plans for high-risk systems should be tested at an alternate processing site. In addition, FinCEN policy requires contingency plans to be documented for each major system and tested at least annually.

FinCEN documented and tested contingency plans for each of the three major systems we reviewed, including two high-risk systems. For the high-risk systems, the plan for the network infrastructure had been tested with a table top exercise, and portions of the Web portal plan had been simulated in a functional exercise. Although the plans had not undergone a full functional test at FinCEN's alternate processing site, the bureau identified this as a weakness and planned to conduct tests at the alternate site once the infrastructure at the site was capable of supporting a full test. However, until FinCEN tests the plans at the alternate site, the risk that FinCEN may not be able to effectively recover these systems and resume normal operations after a disruption is increased.

---

---

IRS and FinCEN Implemented Configuration Management and System Change Controls, but Weaknesses Remained

The purpose of configuration management is to establish and maintain the integrity of an organization's systems. Organizations can better ensure that only authorized applications and programs are placed into operation by establishing and maintaining baseline configurations and by monitoring changes to these configurations. Organizations should ensure that changes to systems are necessary, work as intended, and do not result in the loss of data or program integrity by documenting, authorizing, testing, and independently reviewing changes. FinCEN's configuration management policy requires that change control procedures be developed and that documentation be created and retained for configuration changes. Additionally, NIST guidance states that change control procedures should address emergency changes. Further, IRS policy requires the establishment and maintenance of baseline configurations and inventories of organizational information systems and the establishment and enforcement of security configuration settings for IT products employed in organizational information systems.

Weaknesses existed in configuration management controls at FinCEN and IRS over the systems that support FinCEN's mission, including the following:

- FinCEN maintained an inventory for its network assets, established configuration management plans for its major systems, and established processes for documenting, authorizing, testing, and reviewing system changes. However, its configuration management plans were not fully documented and not all system changes included required documentation. For example, the Web portal plan did not describe the documentation that was required for system changes and the electronic filing system plan did not describe a key step in the change control process. In addition, the Web portal and network infrastructure plans did not include procedures for handling emergency changes. Moreover, although its network infrastructure configuration management plan required security assessments to be documented for changes, FinCEN did not document them for any of the eight infrastructure changes we reviewed.
- IRS did not always adequately manage the configuration of sensitive systems. IRS had adequately documented and tested the seven changes to the WebCBRS application that we reviewed. However, IRS did not maintain or enforce a baseline configuration on the mainframe system that supports the WebCBRS system and the BSA database, as well as other critical IRS systems.

---

---

FinCEN Established a Patch Management Program, but Key Systems Were Missing Critical Patches

Until FinCEN fully documents change control procedures and system changes, there is an increased risk that changes to its systems could be unnecessary, may not work as intended, or may result in the unintentional loss of data or program integrity. Moreover, without a baseline configuration, IRS is unable to adequately track and monitor changes to its mainframe, potentially placing sensitive BSA data at risk.

Patch management is a critical process that can help alleviate many of the challenges of securing computing systems.<sup>15</sup> As vulnerabilities in a system are discovered, attackers may attempt to exploit them, possibly causing significant damage. Malicious acts can range from defacing Web sites to taking control of entire systems, thereby being able to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. After a vulnerability is validated, the software vendor may develop and test a patch or workaround to mitigate the vulnerability. Incident response groups and software vendors issue information updates on the vulnerability and the availability of patches. FinCEN policy requires all of its systems to be patched on a monthly basis, that patches be tested on nonproduction systems before being loaded onto production systems, and a log be maintained of all patches applied to each system.

FinCEN did not always apply patches in a timely manner, and sensitive systems were missing critical patches. Although the bureau required all of its systems to be patched monthly, it was only applying patches to the Web portal application every 3 months. Furthermore, several systems that processed BSA data were missing critical patches or were running software that was out of date. Because the organization was not always applying patches in a timely manner, had not yet installed many critical patches, and had not upgraded software on all of its systems, data were unnecessarily vulnerable to compromise.

---

<sup>15</sup>For example, see GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, [GAO-04-706](#) (Washington, D.C.: June 2, 2004).

---

## FinCEN and IRS Had Not Fully Implemented Elements of Their Information Security Programs

A key reason for the information security weaknesses over the information and systems supporting FinCEN's mission is that FinCEN and IRS had not fully implemented information security program elements required by FISMA. FISMA requires agencies to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be 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; and
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices.

Although FinCEN made progress in implementing its information security program, it had not yet fully implemented key activities. Additionally, although we did not fully evaluate IRS's security program separately as a part of this review, in previous reports we have found that key elements of IRS's program have shortcomings. Until all key elements of its information security programs are fully and consistently implemented, FinCEN and IRS will not have sufficient assurance that new weaknesses will not emerge and that sensitive data and systems are adequately safeguarded



---

from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.<sup>16</sup>

**FinCEN Conducted Risk Assessments for Systems Transmitting and Storing BSA Data**

Identifying and assessing information security risks are essential steps in determining what controls are required to mitigate the risks. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. NIST guidelines state that the identification of risk for an information technology system requires an understanding of the system's processing environment, including data and information, system and data criticality, and system and data sensitivity. Furthermore, according to NIST, risk management should identify threats and vulnerabilities, set priorities for actions to reduce risks, identify new controls or countermeasures, and determine risks remaining after implementing the new control, also known as residual risk. FinCEN risk assessment policy requires that risk assessments be documented for all systems, conducted in accordance with NIST guidance, and updated at least every 3 years as part of the certification and accreditation process.

FinCEN documented risk assessments for all three of the major systems we reviewed; they were conducted in accordance with FinCEN policy and NIST guidance for risk assessments. The assessments were current, documented potential threats, and recommended corrective actions for mitigating or eliminating the vulnerabilities identified.

**FinCEN Made Progress Toward Developing and Documenting Information Security Policies and Procedures, but Lacked Detailed Implementing Guidance**

A key element of an effective information security program is establishing and implementing appropriate policies, procedures, and technical standards to govern security over an agency's computing environment. Moreover, such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local and wide area networks and interconnections to contractors and other federal agencies that support critical mission operations. Establishing and documenting security policies is important because they are the primary mechanism by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures

---

<sup>16</sup>The information and systems at TCS that support FinCEN's mission are subject to the information security program for Treasury; however, we did not evaluate Treasury's program as part of this review.

---

and controls. Otherwise, agency systems and information will not receive the protection that should be provided by the security policies and procedures.

Although FinCEN had made progress toward developing and documenting information security policies and procedures, the policies did not always include key information, and detailed implementing guidance for its policies did not always exist. FinCEN updated its policies and approved them in June 2008; the policies replaced older ones that had not been updated since 2003. However, shortcomings in the updated policies existed. For example, although FinCEN established a patch management policy, the implementing guidance for UNIX patches did not address prioritization of critical patches. In addition, its policy requiring that the network be protected by an intrusion detection system did not require that outbound network traffic be inspected. Further, the bureau did not have detailed implementation guidance for securely configuring its virtual private network. The weaknesses we identified in each of these controls demonstrate the need for such guidance.

**FinCEN and IRS Developed System Security Plans, but FinCEN Did Not Document All Required Controls**

An information system security plan should provide a complete and up-to-date overview of a system's security requirements and describe the controls that are in place or planned to meet those requirements. Office of Management and Budget (OMB) Circular A-130 specifies that agencies develop and implement system security plans for major applications and for general support systems and that these plans address policies and procedures for providing management, operational, and technical controls. Under FISMA, federal agencies are required to categorize information systems as low, moderate, or high impact; apply the appropriate set of baseline security controls in accordance with NIST guidance; and document the security controls in a system security plan. In addition, NIST recommends that security plans include, among other topics, existing or planned security controls, the name of the individual responsible for the security of the system, a description of the system and its interconnected environment, and rules of behavior for individuals accessing the system.

FinCEN also requires that its system security plans describe the system's security requirements, identify the security controls and whether they are planned or implemented for a system, and that they be reviewed, updated, and reapproved by management at least annually, or whenever a significant change to the system occurs. Additionally, IRS requires that system security plans document the security controls for systems, whether

---

planned or in place, as well as rules of behavior for individuals accessing the system.

Although FinCEN documented system security plans for each of its major information systems, it did not always consistently document controls. While the three system security plans we reviewed documented the status of almost all of the required management, operational, and technical controls, two plans for systems categorized as high impact did not document five required security controls. During our review, FinCEN provided updated versions of the plans; however, one of them still did not document one control or describe how another control was implemented.

IRS documented system security plans for each of its three major systems that support FinCEN's mission. The plans included information required by OMB; documented the management, operational, and technical controls in place; and mapped the controls directly to those prescribed by NIST.

#### FinCEN Employees Completed Security Awareness Training

An important component of an information security program is providing required training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. FISMA mandates that federal employees and contractors who use agency information systems be provided with periodic training in information security awareness. FISMA also requires agencies to provide appropriate training on information security to personnel who have significant security responsibilities. This training, described in NIST guidance,<sup>17</sup> should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and their roles and responsibilities to properly and effectively implement the practices that are designed to reduce these risks. Depending on an employee's specific security role, training could include specialized topics, such as incident detection and response, physical security, or firewall configuration. FinCEN also requires all of its employees and contractors to complete annual security awareness training and for individuals with significant security responsibilities to complete specialized security awareness training annually.

---

<sup>17</sup>NIST, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, SP 800-16 (Gaithersburg, Md., April 1998); and NIST, *Building an Information Technology Security Awareness and Training Program*, SP 800-50 (Gaithersburg, Md., October 2003).

---

FinCEN Conducted Periodic Vulnerability Scans, but the Scans Were Not Always Comprehensive or Timely

FinCEN implemented a security awareness training program and ensured that its employees and contractors completed it annually. The annual training given to all employees and contractors included topics that were consistent with NIST guidance, such as laws and regulations, e-mail security, procedures for handling sensitive information, and security threats such as viruses. The bureau reported that all of its 471 employees and contractors who were required to do so completed the training between June 2007 and July 2008. FinCEN provided certificates documenting that all 17 of the employees that we selected had completed required training and that all 8 of the employees holding significant IT responsibilities that we selected had completed the required specialized training.

An important element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies and controls that are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits of such activities will not be achieved unless the results improve the security program. Analyzing the results of monitoring efforts—as well as security reviews performed by external audit organizations—provides security specialists and business managers with a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls. NIST requires organizations to scan information systems for vulnerabilities; in addition, it states that vulnerability analysis for custom software and applications includes specialized approaches such as review of source code. In addition, according to commercial vendors, running scanning software in an authenticated mode allows the software to detect additional vulnerabilities. FinCEN policy also requires periodic scanning of its systems every 3 months to detect potential vulnerabilities.

Although FinCEN conducted periodic vulnerability scans of major systems, the scans were not always comprehensive or timely. FinCEN scanned its workstations and network infrastructure, but did not scan databases or applications; it also did not scan or conduct independent reviews of source code for its internally developed applications. Further, scanning had not been conducted quarterly; in June 2008, FinCEN officials told us that they had not conducted any scans since February 2008, a period of 4 months. As a result, FinCEN could be unaware of many

---

FinCEN Improved Its Process for Verifying Corrective Actions, but IRS's Corrective Actions Were Not Always Effective

undetected vulnerabilities in its applications, systems, and network in a timely manner.

In its guidance to agencies, OMB requires agencies to develop remedial action plans, also known as plans of action and milestones. A remedial action plan assists agencies in the identification, assessment, prioritization, and monitoring of the progress of corrective efforts for weaknesses found in systems and programs. FinCEN policy requires that the agency track vulnerabilities found during security assessments, together with planned and implemented mitigation actions to correct these weaknesses, in each system's respective remedial action plan. IRS has a similar policy, which requires that it track the status of resolution for all weaknesses and verify that each weakness is corrected.

FinCEN developed a new remedial action management process to manage and mitigate security weaknesses in its systems. FinCEN officials told us that the bureau did not have a process to document and validate remedial actions prior to March 2008 and that the new process was developed in order to address this. The process describes how the bureau plans to identify, prioritize, and track vulnerabilities as they are addressed. Among other things, the new process requires

- monthly meetings between key staff and the Information Security System Officer in order to review the status of new and existing vulnerabilities;
- vulnerabilities to be prioritized according to risk; and
- all information concerning remedial actions to be updated at least monthly.

FinCEN officials told us that they had collected supporting documentation when remedial actions were completed and provided us with examples. However, FinCEN's procedure for the new process did not specify that supporting documentation was required. Requiring supporting documentation in the procedure would better ensure that remedial actions are verified as effective.

---

As we have previously reported,<sup>18</sup> IRS's verification process for determining whether remedial actions were implemented was not always effective. In January 2009, we reported that IRS indicated that it had corrected or mitigated 65 previously reported weaknesses but that 16 still existed at the time of our review; 3 of these weaknesses affect the systems that support FinCEN's mission. We have identified a similar weakness in both our January 2008<sup>19</sup> and March 2007<sup>20</sup> reports; however, this condition continues to exist. Without a sound remediation process, IRS will not have assurance that the proper resources will be applied to known vulnerabilities or that those vulnerabilities will be properly mitigated. We have previously recommended that IRS implement a revised remedial action verification process that ensures actions are fully implemented.

---

## Conclusions

FinCEN, TCS, and IRS have taken important steps in implementing numerous controls to protect the information and systems that support FinCEN's mission. However, significant weaknesses in access controls and other information security controls existed at all three organizations that impaired their ability to ensure the confidentiality, integrity, and availability of the information and systems. FinCEN had made important progress in implementing its information security program; however, one key reason for many of the weaknesses was that FinCEN and IRS had not yet fully implemented elements of their information security programs. Further actions are needed to address the risk to the information and systems. Until (1) the organizations act to mitigate identified weaknesses and (2) FinCEN and IRS fully implement their information security programs, there is an increased risk that sensitive BSA information will not be adequately protected against unauthorized disclosure or modification and that systems could be disrupted.

---

## Recommendations for Executive Action

To better ensure the security of the overall BSA environment, we are recommending that the Secretary of the Treasury direct the Director of

---

<sup>18</sup>GAO, *Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS*, [GAO-09-136](#) (Washington, D.C.: Jan. 9, 2009).

<sup>19</sup>GAO, *Information Security: IRS Needs to Address Pervasive Weaknesses*, [GAO-08-211](#) (Washington, D.C.: Jan. 8, 2008).

<sup>20</sup>GAO, *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service*, [GAO-07-364](#) (Washington, D.C.: Mar. 30, 2007).

---

FinCEN to fully implement its information security program by taking the following five actions:

- Update information security policies and procedures to address key missing information such as patch prioritization and inspection of outbound network traffic, as well as to include detailed implementation guidance for issues such as securely configuring the virtual private network.
- Ensure that system security plans document all required controls and describe how all required controls are implemented.
- Conduct vulnerability scans on databases, applications, and network infrastructure on a quarterly schedule.
- Implement vulnerability scanning of custom source code or manual source code reviews.
- Update remedial action procedures to require that supporting documentation be provided to verify that corrective actions are fully implemented and effective.

In a separate report designated “Limited Official Use Only”, we are making 88 detailed recommendations to the Secretary of the Treasury to strengthen information security controls at FinCEN, TCS, and IRS over the systems supporting FinCEN’s mission.

---

## Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, Treasury’s Deputy Assistant Secretary for Information Systems and Chief Information Officer stated that the department is committed to promoting the nation’s security through strengthened financial systems and promoting safer and more transparent U.S. and international financial systems, noting that securely maintaining BSA information significantly contributes to this goal. He also stated that Treasury will provide a detailed corrective action plan for each of the recommendations and that many of the actions required to address the recommendations are already completed or under way.

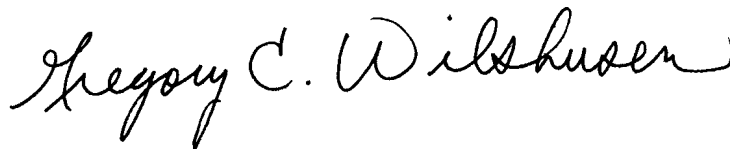
---

We are sending copies of this report to interested congressional committees, the Secretary of the Treasury, the Director of FinCEN, the Commissioner of Internal Revenue, the Treasury Inspector General, and the Treasury Inspector General for Tax Administration. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staffs have any questions regarding this report, please contact Nancy Kingsbury at (202) 512-2700 or Gregory C. Wilshusen at (202) 512-6244. We can also be reached by e-mail at [kingsburyn@gao.gov](mailto:kingsburyn@gao.gov) and [wilshuseng@gao.gov](mailto:wilshuseng@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 listed in appendix III.



Nancy R. Kingsbury  
Managing Director, Applied Research and Methods



Gregory C. Wilshusen  
Director, Information Security Issues



---

# Appendix I: Objective, Scope, and Methodology

---

The objective of our review was to determine whether information security controls have been implemented that effectively protect the confidentiality, integrity, and availability of the information and information systems supporting the mission of the Financial Crimes Enforcement Network (FinCEN).

To accomplish this, we tested the effectiveness of information security and information technology-based internal controls. We focused our evaluation on the controls for the applications, databases, and network infrastructure that directly or indirectly support the processing and storage of Bank Secrecy Act (BSA) data on behalf of FinCEN at the Department of the Treasury (Treasury), FinCEN, and the Internal Revenue Service (IRS). Specifically, we evaluated FinCEN's network infrastructure and Web portal used to access BSA data; the Web-based Currency and Banking Retrieval System (WebCBRS) and the mainframe and network infrastructure supporting it at IRS; and the electronic filing system and related network infrastructure at the Treasury Communications System (TCS).

Our evaluation was based on our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information. We also used FinCEN, IRS, and Treasury policies and procedures to evaluate the information system controls at the organizations. Additionally, where federal requirements or guidelines were applicable, such as the Federal Information Security Management Act of 2002 (FISMA) or National Institute of Standards and Technology (NIST) guidance, we used them to assess the extent to which the organizations had complied with specific requirements.

To determine whether TCS, FinCEN, and IRS had implemented access controls, contingency planning controls, and configuration controls over the information and systems that support FinCEN, we

- evaluated and reviewed the security software password settings to determine if users were appropriately identified and authenticated and if strong password management was enforced;
- examined application and system access lists and associated documentation to determine whether users were properly authorized or had more permissions than necessary to perform their assigned job functions;

- analyzed network and system configurations to determine if access paths were adequately controlled and if sensitive data were being encrypted;
- tested and observed physical access controls and environmental controls to determine if computer facilities and resources were being protected from intentional or unintentional loss or impairment;
- evaluated and reviewed backup and recovery procedures to determine if they adequately protected key systems against service interruptions;
- examined contingency plans and test results for key FinCEN systems to determine whether those plans were adequately documented, had been updated, or had been appropriately tested;
- inspected key servers, workstations, and network infrastructure devices to determine whether critical patches had been installed or were up-to-date; and
- evaluated and reviewed change request documentation to determine if system and application changes were appropriately authorized, tested, and approved.

To assess whether FinCEN had fully implemented an information security program to ensure that controls were established and maintained for its information systems, we used the requirements of FISMA, which establish key elements for an effective agencywide information security program. To evaluate FinCEN's implementation of these key elements, we

- analyzed risk assessments for key FinCEN systems to determine whether risks and threats were documented;
- examined security plans to determine if management, operational, and technical controls were in place or planned and whether these security plans were updated;
- analyzed FinCEN policies, procedures, practices, and standards to determine their effectiveness in providing guidance to personnel responsible for securing information and information systems;
- inspected training records for personnel with significant responsibilities to determine if they received training commensurate with those responsibilities;

- analyzed test plans and test results for key FinCEN systems to determine whether management, operational, and technical controls were adequately tested at least annually and were based on risk; and
- evaluated FinCEN's process to correct weaknesses to determine whether remedial action plans complied with federal guidance.

In addition, we examined IRS's security plans for WebCBRS and the related general support systems to determine if management, operational, and technical controls were in place or planned and whether these security plans were updated.

We also interviewed key security representatives and officials responsible for information security management at FinCEN, TCS, and IRS to help determine whether information system controls were in place, adequately designed, and operating effectively. We also reviewed a previous report issued by the Treasury Inspector General's Office on FinCEN information security and previous reports from GAO on IRS information security. Our work was conducted in the Washington, D.C., metropolitan area and at FinCEN, TCS, and IRS computing facilities in Virginia and Michigan.

We conducted this performance audit from March 2008 to January 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

# Appendix II: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

JAN 16 2009

Mr. Greg Wilshusen  
Director, Information Security Issues  
U.S. Government Accountability Office  
441 G Street N.W.  
Washington, D.C. 20515

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft reports entitled, *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data* (GAO-09-200SU and GAO-09-195). Treasury is committed to promoting the nation's security through strengthened financial systems and promoting safer and more transparent U.S. and international financial systems. The ability to securely maintain Bank Secrecy Act (BSA) information contributes significantly to this goal. Therefore, we appreciate GAO's efforts in reviewing BSA information security.

Although the Financial Crimes Enforcement Network (FinCEN) is the administrator of the BSA, your reports correctly note that three entities within Treasury have responsibilities associated with maintaining and safeguarding BSA information: FinCEN, the Department's Office of the Chief Information Officer (OCIO) which operates the Treasury Communications System (TCS), and the Internal Revenue Service Enterprise Computing Center in Detroit (IRS ECC-Detroit). Many of the actions required to address the recommendations are already completed or underway. Specifically, of the 41 recommendations addressed to FinCEN, 18 have already been completed; of the 21 recommendations addressed to the Department's OCIO, 12 have already been completed; and of the 11 addressed to IRS, 4 have already been completed. Treasury will provide a detailed corrective action plan for each of the recommendations with the response to the final reports.

If you have any questions, please feel free to contact Mr. Ed Roback, Associate Chief Information Officer for Cyber Security at 202-622-2593.

Sincerely,

A handwritten signature in black ink that reads "Michael D. Duffy".

Michael D. Duffy  
Deputy Assistant Secretary for Information Systems  
and Chief Information Officer

---

# Appendix III: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Nancy R. Kingsbury, (202) 512-2700 or [kingsburyn@gao.gov](mailto:kingsburyn@gao.gov)  
Gregory C. Wilshusen, (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

---

## Staff Acknowledgments

In addition to the contacts named above, Edward Alexander and Jeffrey Knott (Assistant Directors), Rebecca Alvarez, Angela Bell, Bruce Cain, William Cook, Neil Doherty, Denise Fitzpatrick, Myong Kim, George Kovachick, Rebecca LaPaze, Kevin Metcalfe, Nancy Glover, David Plocher, Zsaroq Powe, Matthew Snyder, and Christopher 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](http://www.gao.gov)). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://www.gao.gov) and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Ralph Dawn, Managing Director, [dawnr@gao.gov](mailto:dawnr@gao.gov), (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngcl@gao.gov](mailto:youngcl@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548