

April 2005

INFORMATION
SECURITY

Internal Revenue
Service Needs to
Remedy Serious
Weaknesses over
Taxpayer and Bank
Secrecy Act Data



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-05-482](#), a report to the Committee on the Judiciary, House of Representatives

Why GAO Did This Study

The Internal Revenue Service (IRS) relies extensively on computerized systems to support its financial and mission-related operations. In addition, IRS provides computer processing support to the Financial Crimes Enforcement Network (FinCEN)—another Treasury bureau. As part of IRS's fiscal year 2004 financial statements, GAO assessed (1) the status of IRS's actions to correct or mitigate previously reported weaknesses at one of its critical data processing facilities and (2) the effectiveness of IRS's information security controls in protecting the confidentiality, integrity, and availability of key financial and tax processing systems.

What GAO Recommends

GAO recommends that the Secretary of the Treasury direct the IRS Commissioner to take several actions to fully implement an effective agencywide information security program and to assess whether taxpayer data have been disclosed to unauthorized individuals. GAO also recommends that the Secretary of the Treasury direct the FinCEN Director to assess whether Bank Secrecy Act data have been disclosed to unauthorized individuals. The Acting Deputy Secretary of the Treasury generally agreed with the recommendations and identified specific completed and planned corrective actions.

www.gao.gov/cgi-bin/getrpt?GAO-05-482.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Greg Wilshusen at 202-512-3317 or wilshuseng@gao.gov.

INFORMATION SECURITY

Internal Revenue Service Needs to Remedy Serious Weaknesses over Taxpayer and Bank Secrecy Act Data

What GAO Found

IRS has made progress in correcting or mitigating previously reported information security weaknesses and in implementing controls over key financial and tax processing systems that are located at one of its critical data processing facilities. It has corrected or mitigated 32 of the 53 weaknesses that GAO reported as unresolved at the time of our prior review in 2002.

However, in addition to the remaining 21 previously reported weaknesses for which IRS has not completed actions, 39 newly identified information security control weaknesses impair IRS's ability to ensure the confidentiality, integrity, and availability of its sensitive financial and taxpayer data and FinCEN's Bank Secrecy Act data. For example, IRS has not implemented effective electronic access controls over its mainframe computing environment to logically separate its taxpayer data from FinCEN's Bank Secrecy Act data—two types of data with different security requirements. In addition, IRS has not effectively implemented certain other information security controls relating to physical security, segregation of duties, and service continuity at the facility. Collectively, these weaknesses increase the risk that sensitive taxpayer and Bank Secrecy Act data will be inadequately protected from unauthorized disclosure, modification, use, or destruction. Moreover, weaknesses in service continuity and business resumption plans heighten the risk that assets will be inadequately protected and controlled to ensure the continuity of operations when unexpected interruptions occur.

An underlying cause of these information security control weaknesses is that IRS has not fully implemented certain elements of its agencywide information security program. Until IRS fully implements a comprehensive agencywide information security program, its facilities and computing resources and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

Contents

Letter

	1
Results in Brief	2
Background	3
Objectives, Scope, and Methodology	7
IRS Has Made Progress in Correcting Previously Reported Weaknesses	8
Serious Weaknesses Place Taxpayer and Bank Secrecy Act Data at Risk	9
Information Security Program Is Not Fully Implemented at IRS	15
Conclusions	19
Recommendations for Executive Action	19
Agency Comments	20

Appendixes

Appendix I: Comments from the Secretary of the Treasury	23
Appendix II: GAO Contact and Staff Acknowledgments	26
GAO Contact	26
Staff Acknowledgments	26

Abbreviations

BSA	Bank Secrecy Act
CIO	chief information officer
FinCEN	Financial Crimes Enforcement Network
FISMA	Federal Information Security Management Act of 2002
IRS	Internal Revenue Service
MASS	Mission Assurance and Security Services
RACF	Resource Access Control Facility

This is a work of the U.S. government and is not subject to copyright protection in the United States. It 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, D.C. 20548

April 15, 2005

The Honorable F. James Sensenbrenner Jr.
Chairman
The Honorable John Conyers Jr.
Ranking Minority Member
Committee on the Judiciary
House of Representatives

As part of our audit of the Internal Revenue Service's (IRS) fiscal year 2004 financial statements,¹ we assessed the effectiveness of IRS's information security controls² over key financial systems, data, and interconnected networks at one of IRS's critical data processing facilities that support the processing, storage, and transmission of sensitive financial and taxpayer data. In addition, the facility maintains Bank Secrecy Act data on behalf of the Financial Crimes Enforcement Network (FinCEN). These data are used by federal law enforcement and regulatory agencies, as well as IRS, to support their investigations of financial crimes, including terrorist financing and money laundering.

This report describes (1) the status of IRS's actions to correct or mitigate previously reported weaknesses at the facility and (2) whether controls over key financial and tax processing systems have been effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer data. In response to your request, we are addressing this report to you.

Separately, we issued a Limited Official Use Only report to you detailing the results of our review. This version of the report, for public release, provides a general summary of the vulnerabilities identified and our recommendations to help strengthen and improve IRS's information security controls.

¹GAO, *Financial Audit: IRS's Fiscal Years 2004 and 2003 Financial Statements*, GAO-05-103 (Washington, D.C.: Nov. 10, 2004).

²Information security controls include electronic access controls, software change control, physical security, segregation of duties, and service continuity. These controls are designed to ensure that access to data is appropriately restricted, that only authorized changes to computer programs are made, that physical access to sensitive computing resources and facilities is protected, that computer security duties are segregated, and that back-up and recovery plans are adequate to ensure the continuity of essential operations.

Results in Brief

IRS has made progress in correcting or mitigating previously reported information security weaknesses and implementing controls over key financial and tax processing systems that are located at a critical data processing facility. The agency has corrected or mitigated 32 of the 53 weaknesses that we reported as unresolved at the time of our prior review in 2002. For example, IRS improved perimeter security by installing barriers at the facility's entrance and implemented procedures to ensure that up-to-date copies of disaster recovery plans would be maintained at an off-site storage facility.

However, IRS has not effectively implemented controls over key financial and tax processing systems located at the facility. In addition to the remaining 21 previously reported weaknesses, for which IRS has not completed actions, 39 newly identified information security control weaknesses impair IRS's ability to ensure the confidentiality, integrity, and availability of its sensitive financial and taxpayer data and FinCEN's Bank Secrecy Act data. IRS has not implemented effective electronic access controls to prevent, limit, or detect unauthorized access to computing resources from the internal IRS computer network. For example, access controls over the mainframe computing environment did not logically separate IRS's taxpayer data from FinCEN's Bank Secrecy Act data—two types of data with different security requirements. As a result, all mainframe users could read or copy Bank Secrecy Act data, and law enforcement users could read or copy taxpayer data. In addition, IRS had not effectively implemented certain other information security controls relating to physical security, segregation of duties, and service continuity at the facility. Collectively, these weaknesses increase the risk that sensitive taxpayer and Bank Secrecy Act data will not be adequately protected from unauthorized disclosure, modification, use, or loss. Moreover, weaknesses in service continuity and business resumption plans heighten the risk that assets will not be adequately protected and controlled to ensure the continuity of operations when unexpected interruptions occur.

These information security control weaknesses exist primarily because IRS has not fully implemented an agencywide information security program to effectively protect the information and information systems that support the operations and assets of the agency. Although IRS has taken some action, including establishing the office of Mission Assurance and Security Services, appointing a senior information security officer to manage the program, and establishing a task force for conducting risk assessments and security test and evaluations, as part of activities required for certification

and accreditation, it has not fully implemented key elements of an effective information program. For example, it has not (1) fully implemented established security policies and procedures, (2) provided specialized training to employees with significant security responsibilities, and (3) effectively instituted a process for performing periodic test and evaluation of its systems. Until IRS fully implements a comprehensive agencywide information security program, its facilities, computing resources, and the information that is processed, stored, and transmitted on its systems will remain vulnerable.

We are making recommendations to the Secretary of the Treasury to direct the IRS Commissioner to take several actions to fully implement a comprehensive agencywide information security program and to determine whether taxpayer information has been disclosed to unauthorized individuals. We further recommend that the Secretary of the Treasury direct the FinCEN Director to perform an assessment to determine whether Bank Secrecy Act data have been disclosed to unauthorized users. The IRS Chief of Mission Assurance and Security Services informed us that certain corrective actions have been completed subsequent to the completion of our fieldwork.

In providing written comments on a draft of this report, the Acting Deputy Secretary of the Treasury generally agreed with our recommendations, identified specific corrective actions that IRS has taken or plans to take to address the recommendations, and provided other comments.

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.

Protecting the computer systems that support critical operations and infrastructures has never been more important because of the concern

about attacks from individuals and groups, including terrorists. These concerns are 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.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of critical federal operations, including those at IRS, at risk of disruption, fraud, and inappropriate disclosure. We have designated information security as a governmentwide high-risk area since 1997³—a designation that remains today.⁴

In December 2002, Congress enacted the Federal Information Security Management Act of 2002 (FISMA) to strengthen security of information and systems within federal agencies.⁵ FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. In addition, FISMA requires that the Secretary of the Treasury be responsible for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information systems and information; (2) ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and (3) delegating to the agency chief information officer (CIO) the authority to ensure compliance with the requirements imposed on the agency under the act.

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

⁴GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005).

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

Treasury's CIO 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 the IRS, is responsible for implementing Treasury-mandated security policies within its domain. In order to implement departmentwide security policies, IRS is required to develop its own information security program, including its own security compliance functions.

IRS Is a Key Steward of Personal Taxpayer Information

As the nation's tax collector, IRS has the demanding responsibility of collecting taxes, processing tax returns, and enforcing the nation's tax laws. In fiscal years 2004 and 2003, IRS collected about \$2 trillion in tax payments, processed hundreds of millions of tax and information returns, and paid about \$278 billion and \$300 billion, respectively, in refunds to taxpayers. IRS employs tens of thousands of people in its 10 service campuses,⁶ three computing centers, and numerous field offices throughout the United States. To efficiently fulfill its tax processing responsibilities, IRS relies extensively on interconnected networks of computer systems to perform various functions, such as collecting and storing taxpayer data, processing tax returns, calculating interest and penalties, generating refunds, and providing customer service.

Because of the nature of its mission, IRS also collects and maintains a significant amount of personal and financial data on each American taxpayer. The confidentiality of this sensitive information must be protected; otherwise, taxpayers could be exposed to loss of privacy and to financial loss and damages resulting from identity theft or other financial crimes.

To help provide information security for its operations and assets (including computing resources and taxpayer information), IRS has developed and is implementing an agencywide information security program. The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, availability, and integrity of information and information systems supporting the agency and its operations. The Chief of MASS is responsible for developing policies and procedures

⁶IRS campuses perform functions such as customer service, account management, and tax examination services, whereas computing centers focus primarily on data processing and software development activities.

regarding information technology security; providing assurance services to improve physical, data, and personnel security; conducting independent testing; and ensuring security is integrated into its modernization activities. To help accomplish these goals, IRS has developed and published information security policies, guidelines, standards, and procedures in the *Internal Revenue Manual*, *Law Enforcement Manual*, and other documents.

IRS Also Provides Processing Support for FinCEN

In addition to processing its own financial and tax information, IRS provides information processing support to FinCEN, another Treasury bureau. FinCEN administers and enforces the Bank Secrecy Act (BSA)⁷ and its implementing provisions. Congress enacted the BSA to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, criminal activity. Since its passage, Congress has amended the BSA to enhance law enforcement effectiveness. Today, more than 170 crimes are listed in federal money-laundering statutes. They cover a broad range, including drug trafficking, gunrunning, murder for hire, fraud, acts of terrorism, and the illegal use of wetlands. The list also includes certain foreign crimes. The reporting and record keeping requirements of the BSA regulations create a paper trail for law enforcement to investigate money laundering schemes and other illegal activities. This paper trail operates to deter illegal activity and provides a means to trace the movements of money through the financial system.

FinCEN relies on IRS to operate and maintain computer systems that process and store a significant amount of FinCEN's sensitive information. This information includes reports and filings from banks and other financial institutions that are required under BSA, such as currency transactions, foreign bank and financial accounts, international transportation of currency or monetary instruments, and criminal referrals of suspicious activities reports. This information is determined by FinCEN to have a high degree of usefulness in criminal, tax, regulatory, intelligence, and counterterrorism investigations, and in implementing counter money laundering programs and compliance procedures. This network supports

⁷Titles I and II of Public Law 91-508 and 31 U.S.C. sections 5311-5330, as amended by the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004, are known as the Bank Secrecy Act. Regulations implementing the Bank Secrecy Act appear at 31 C.F.R. Part 103.

federal, state, and local law enforcement, and intelligence and investigative agencies as part of the federal government's effort to combat terrorism and to investigate and prosecute crime.

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of IRS's actions to correct or mitigate previously reported weaknesses and (2) whether controls over key financial and tax processing systems located at the facility have been effective in ensuring the confidentiality, integrity, and availability of sensitive financial and taxpayer data. We concentrated our evaluation primarily on threats emanating from internal sources on IRS's computer networks. To guide our work, we used the audit methodology described in our *Federal Information System Controls Audit Manual*,⁸ which discusses the scope of such reviews and the type of testing required for evaluating general controls. We also used FISMA to guide our review of IRS's implementation of its information security program. Specifically, we evaluated information system controls intended to

- limit, detect, and monitor logical and physical access to sensitive computing resources and facilities, thereby safeguarding them from misuse and protecting them from unauthorized disclosure and modification;
- maintain operating system integrity through effective administration and control of powerful computer programs and utilities that execute privileged instructions;
- prevent the introduction of unauthorized changes to application software in the existing software environment;
- ensure that work responsibilities are segregated, so that one individual does not perform or control all key aspects of computer-related operations and thereby have the ability to conduct unauthorized actions or gain unauthorized access to assets or records;
- minimize the risk of unplanned interruptions and recover critical computer processing operations in the case of disaster or other unexpected interruptions; and

⁸GAO, *Federal Information System Controls Audit Manual*, [GAO/AIMD-12.19.6](#) (Washington, D.C.: January 1999).

-
- implement an agencywide information security program that includes a continuing cycle of assessing risk, implementing and promoting policies and procedures to reduce such risk, and monitoring the effectiveness of those activities.

To evaluate these controls, we identified and reviewed pertinent IRS information security policies and procedures, guidance, security plans, relevant reports, and other documents, and we tested the effectiveness of these controls. We also discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

We performed our review at the IRS facility, at IRS's National Office in New Carrollton, Maryland, and at our headquarters in Washington, D.C., in accordance with generally accepted government auditing standards from August through December 2004. We discussed the results of our review with IRS, Treasury, and FinCEN officials.

IRS Has Made Progress in Correcting Previously Reported Weaknesses

IRS has made progress in correcting previously reported information security weaknesses. The agency has corrected or mitigated 32 of the 53 weaknesses that we reported as unresolved at the time of our last review in 2002. For example, IRS has

- improved perimeter security by installing barriers at the facility's entrance to prevent unauthorized vehicles from entering the premises,
- implemented policies and procedures to ensure that system software products are tested and evaluated prior to installation,
- discontinued the practice of using shared accounts and passwords to administer its network authentication server and firewall, and
- implemented procedures to ensure that disaster recovery plans are up-to-date and maintained at the off-site storage facility.

While IRS has taken steps to strengthen its information security controls, it had not completed actions to correct or mitigate the remaining 21 previously reported weaknesses. These weaknesses include granting and authorizing inappropriate access permissions over Unix system files, permitting remote access capabilities that expose passwords and user identifications, allowing users to implement easily guessed passwords, and

permitting unrestricted physical access to sensitive computing areas. Failure to resolve these issues will leave IRS facilities and sensitive data vulnerable to unauthorized access, manipulation, and destruction.

Serious Weaknesses Place Taxpayer and Bank Secrecy Act Data at Risk

IRS has not effectively implemented information security controls to properly protect the confidentiality, integrity, and availability of data processed by the facility's computers and networks. In addition to the 21 previously reported weaknesses that remain uncorrected, we identified 39 new information security weaknesses during this review. Serious weaknesses related to electronic access to computing resources from sources located on IRS's internal computer network place sensitive taxpayer and Bank Secrecy Act data—including information related to financial crimes, terrorist financing, money laundering, and other illicit activities—at significant risk of unauthorized disclosure, modification, or destruction. In addition, information security weaknesses that exist in other control areas, such as physical security, segregation of duties, and service continuity, further increase risk to the computing environment.

Collectively, these weaknesses threaten IRS's ability to perform its operational missions, such as processing tax returns and law enforcement information, both of which rely on IRS's computer systems and networks to process, store, and transmit data.

Electronic Access Controls Were Inadequate

A basic management objective for any organization is to protect the data supporting its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing electronic controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and data. Electronic access controls include user accounts and passwords, access rights and permissions, network services and security, and audit and monitoring of security-related events. Inadequate electronic access controls diminish the reliability of computerized data and increase the risk of unauthorized disclosure, modification, and destruction of these data.

Electronic access controls were not effectively implemented to prevent, limit, and detect unauthorized access to the facility's computer systems and data. Numerous vulnerabilities existed in IRS's computing environment because of the cumulative effects of control weaknesses in the areas of

user accounts and passwords, access rights and permissions, network services and security, and audit and monitoring of security-related events.

User Accounts and Passwords

A computer system must be able to identify and differentiate among users so that activities on the system can be linked to specific individuals. Unique user accounts assigned to specific users allow systems to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity through some means of authentication, such as a password, known only to its owner. The combination of identification and authentication, such as user account/password combinations, provides the basis for establishing individual accountability and controlling access to the system. Accordingly, agencies should (1) implement procedures to control the creation, use, and removal of user accounts and (2) establish password parameters, such as length, life, and composition, to strengthen the effectiveness of account/password combinations for authenticating the identity of users.

IRS did not adequately control user accounts and passwords to ensure that only authorized individuals were granted access to its systems and data. For example, it did not adequately protect mainframe systems files that contain embedded user accounts and passwords. Access to these files was not adequately restricted, and user account and password combinations could have been read by any authorized user—IRS, law enforcement, and contractors—of the system. In addition, IRS did not adequately control user accounts and passwords to ensure that only authorized individuals were allowed access to its servers and networks. As a result, increased risk exists that unauthorized users could gain authorized user ID and password combinations to claim a user identity and then use that identity to gain access to sensitive taxpayer or Bank Secrecy Act data.

Access Rights and Permissions

A basic underlying principle for securing computer systems and data is the concept of least privilege. This means that users are granted only those access rights and permissions they need to perform their official duties. Organizations establish access rights and permissions to restrict the access of legitimate users to only the specific programs and files that they need to do their work. User rights are allowable actions that can be assigned to users or groups. File and directory permissions are rules associated with a file or directory; they regulate which users can access them and in what manner. Assignment of rights and permissions must be carefully considered to avoid giving users unnecessary access to sensitive files and directories.

IRS routinely permitted excessive access to the facility's computer systems—mainframes, Unix, and Windows—that support sensitive taxpayer and Bank Secrecy Act data and to critical datasets and files. Access controls over the mainframe computing environment did not logically separate IRS's data from FinCEN's data. For example, IRS granted all 7,460 mainframe users—IRS employees, non-IRS employees, contractors—regardless of their official duties, the ability to read and modify sensitive taxpayer and Bank Secrecy Act data, including information about citizens, law enforcement personnel, and individuals subject to investigation. In addition, IRS also did not adequately restrict access rights and permissions on its Windows servers. For example, it did not adequately restrict access to Windows accounts with powerful rights over the operating system. Inappropriate access to accounts with powerful rights can compromise the integrity of the operating system and the privacy of the data that reside on the servers.

Network Services and Security

Networks are series of interconnected devices and software that allow individuals to share data and computer programs. Because sensitive programs and data are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests and deny unauthorized requests and by limiting the services that are available on the network. Network devices include (1) firewalls designed to prevent unauthorized access into the network, (2) routers that filter and forward data along the network, (3) switches that forward information among parts of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between computers. Insecurely configured network services and devices can make a system vulnerable to internal or external threats, such as denial-of-service attacks. Since networks often provide the entry point for access to electronic information assets, failure to secure those networks increases the risk of unauthorized use of sensitive data and systems.

IRS did not securely control network services to prevent unauthorized access to and ensure the integrity of IRS's computer networks and systems at the facility. For example, IRS did not adequately secure its network against known vulnerabilities or misconfigured network services on several of its infrastructure devices. As a result, an unauthorized user could gain access to these network devices and gain control of the facility's

network, placing IRS and FinCEN data at risk. Further, this unauthorized control could seriously disrupt computer operations.

Audit and Monitoring of Security-Related Events

Determining what, when, and by whom specific actions were taken on a system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. Organizations accomplish this by implementing system or security software that provides an audit trail for determining the source of a transaction or attempted transaction and for monitoring users' activities. How organizations configure the system or security software determines the nature and extent of audit trail information that is provided. To be effective, organizations should (1) configure the software to collect and maintain sufficient audit trails for security-related events; (2) generate reports that selectively identify unauthorized, unusual, and sensitive access activity; and (3) regularly monitor and take action on these reports. Without sufficient auditing and monitoring, organizations increase the risk that they may not detect unauthorized activities or policy violations.

The risks created by the serious electronic access control weaknesses discussed above were heightened because IRS did not effectively audit and monitor system activity on its servers. For example, not all Windows servers at the facility were configured to ensure sufficient retention of security logs. As a result, there was a higher risk of unauthorized system activity going undetected.

IRS and FinCEN Data Are at Significant Risk

The cumulative effect of inadequate electronic access controls specific to user accounts and passwords, access rights and permissions, network services and security, and audit and monitoring places sensitive taxpayer and Bank Secrecy Act data at risk of unauthorized disclosure, use, modification, or destruction, possibly without detection. More specifically, electronic access controls over authorized users—IRS employees, contractors, and law enforcement officials—were not effectively implemented to restrict these users to the data they needed in order to perform their official duties and to protect sensitive programs and data from unauthorized access, manipulation, and use.

As a result, we were able to view and print Bank Secrecy Act data from datasets containing *Suspicious Activity Reports* that have been filed under the Bank Secrecy Act. The information we were able to capture included, among other things, dates of the investigation, the name, Social Security number, and driver's license number of the individual under investigation,

the number and total dollar amount of financial transactions, and suspected terrorist activity, if any. Moreover, the weaknesses in electronic access controls also allowed FinCEN users, who include federal, state, and local law enforcement officials, the capability to access sensitive IRS systems and view taxpayer information. The Internal Revenue Code⁹ prohibits disclosure of taxpayer data generally, and the Taxpayer Browsing Protection Act¹⁰ prohibits unauthorized browsing of taxpayer returns or information by federal, state, and local employees. We have previously reported violations of IRS employees browsing taxpayer information and on IRS's efforts to monitor employee browsing.¹¹ Given the weaknesses with its audit and monitoring controls, it is unlikely that IRS would be able to detect any illegal browsing of taxpayer information with the systems currently in use.

Unless these weaknesses are corrected, sensitive taxpayer and Bank Secrecy Act data will remain at risk of unauthorized disclosure, use, modification, or destruction, possibly without detection.

Other Information Security Weaknesses Exist

In addition to the electronic access security controls, other information security controls should be in place to ensure the confidentiality, integrity, and availability of an organization's systems and data. These controls include policies, procedures, and control techniques that physically secure an organization's computer resources and systems, provide proper segregation of incompatible duties and computer functions among computer users, and ensure continuity of computer processing operations in the event of a disaster or unexpected interruption.

Physical Security

Physical security controls are important for protecting computer facilities and resources from vandalism and sabotage, theft, accidental or deliberate alteration or destruction of information or property, attacks on personnel, and unauthorized access to computing resources. Physical security

⁹26 U.S.C. § 6103.

¹⁰26 U.S.C. § 7213A.

¹¹GAO, *IRS Systems Security and Funding: Additional Information on Employee Browsing and Tax Systems Modernization*, [GAO/AIMD/GGD-97-140R](#) (Washington, D.C.: June 23, 1997); *IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified*, [GAO/T-AIMD-97-82](#) (Washington, D.C.: Apr. 15, 1997).

controls should prevent, limit, and detect access to facility grounds, buildings, and sensitive work areas and the agency should periodically review the access granted to computer facilities and resources to ensure that this access continues to be appropriate. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. Inadequate physical security could lead to the loss of life and property, the disruption of functions and services, and the unauthorized disclosure of documents and information.

Although IRS has implemented physical security controls, certain weaknesses reduce the effectiveness of these controls in protecting and controlling physical access to assets at the facility. For example, guards did not always verify employees' identities as they entered the facility. Failure to check IRS photo identifications increases the risk that unauthorized individuals could gain access to the facility. In addition, IRS did not always maintain effective control over the issuance of master keys. The lack of accountability over master keys increases the likelihood that an unauthorized person could gain possession of a master key and use it to access sensitive areas.

Segregation of Duties

Controls that segregate duties are the policies, procedures, and organizational structure that prevent one individual from controlling key aspects of computer-related operations and thereby having the capability to conduct unauthorized actions or gain unauthorized access to assets or records without being promptly detected. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed.

We identified instances in which duties were not adequately segregated to ensure that no individual had complete authority or system access, which could result in fraudulent activity. For example, developers were routinely granted production level access on the facility's mainframe processing environment by individuals other than those responsible for the security administration of the mainframe. A review of one month of audit logs showed that 24 users (including 5 contractors) who were only granted access to the development mainframe environment had their access privileges elevated to production—several of them on a daily basis. Although user access was being logged, MASS employees neither controlled the action that elevated the developers' access permissions nor routinely monitored audit logs. As a result, MASS employees did not detect that users' access had been elevated. Granting developers access to

production systems creates the potential for those individuals to perform incompatible functions.

Service Continuity

Service continuity 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.

IRS has in place environmental controls designed to protect computing resources and personnel; it also has a program for periodic testing of disaster recovery plans. However, IRS's disaster recovery and business resumption plans for resuming operations following a disruption did not include procedures for Unix and Windows systems. In the event of a disaster, the facility may not be able to coordinate appropriate measures to restore critical Unix and Windows systems.

Information Security Program Is Not Fully Implemented at IRS

The weaknesses described in this report are symptomatic of an agencywide information security program that is not fully implemented across IRS. Implementing an information security program is essential to ensuring that controls over information and information systems work effectively on a continuing basis, as described in our May 1998 study of security management best practices.¹²

We previously recommended to the IRS Commissioner that IRS complete its implementation of an effective agencywide information security program.¹³ Since our last review, IRS has made important progress toward improving information security management. For example, as part of

¹²GAO, *Executive Guide: Information Security Management—Learning from Leading Organization*, [GAO/AIMD-98-68](#) (Washington, D.C.: May 1998).

¹³GAO, *Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks*, [GAO-03-44](#) (Washington, D.C.: May 30, 2003).

activities required for certification and accreditation of all IRS general support systems,¹⁴ it established MASS, appointed a senior information security officer to manage the program, and established a task force for conducting risk assessments and security test and evaluations. However, the recurring and newly identified weaknesses discussed in this report, as well as the similarity of these weaknesses to those we have previously identified at other IRS facilities, are indicative of an information security program that is not fully implemented across the agency.

FISMA, consistent with our security management best practices guide, requires key elements of an agency's information security program to strengthen information security and to adequately protect the information and systems that support its operations. These elements include

- policies and procedures that (1) are based on risk assessments, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- security awareness training to inform personnel, including contractors and other users of information systems, of information security risks and their responsibilities in complying with agency policies and procedures; and
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to the management, operational, and technical controls of every major information system that is identified in the agencies' inventories.

Establishing and Implementing Policies

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. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local and wide area networks and interconnections to contractor and other federal agencies that support critical mission operations. In addition, technical security

¹⁴General support systems are sets of resources that provide necessary information technology infrastructure support to applications and business functionality such that compromise would have a severe adverse effect on the IRS mission, tax administration functions, or employee welfare.

standards are needed to provide consistent implementing guidance for each computing environment. 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 and controls. Otherwise, agency systems and information will not receive the protection that should be provided by the security policies and controls.

Although IRS has established and documented policies and procedures for specific security areas, including password standards and disaster recovery planning, it frequently has not implemented them. We continue to report that the facility has not implemented policies and procedures contained in IRS's *Law Enforcement Manual* and *Internal Revenue Manual* pertaining to user accounts and passwords, access rights and permissions, network services and security, audit and monitoring, and other information system controls. Of the new weaknesses identified, 33 of 39 resulted from IRS not implementing its established security policies and procedures. As a result, IRS is at increased risk that sensitive financial, taxpayer, and Bank Secrecy Act data could be exposed to unauthorized access without detection.

Promoting Security Awareness and Training

Another key element of an information security program involves promoting awareness and providing required training so that users understand the risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA mandates that all federal employees and contractors involved in the use of agency information systems be provided periodic training in information security awareness and accepted information security practice. Further, FISMA requires agency heads to ensure employees with significant information security responsibilities are provided sufficient training.

IRS has established information security awareness programs for its employees and contractors. These programs include distributing security awareness bulletins and brochures and creating information security poster boards. As reported by Treasury's OIG in its 2004 FISMA report, 100

percent of IRS employees received security awareness training; however, only 28 percent of IRS government and contractor employees with significant security responsibilities received specialized training. Security administration staff at the facility stated that they were largely self-taught in security software and that only one staff member in the past 2 years had received technical mainframe security training. Consequently, the staff was not knowledgeable about some of the more recent technical advances relating to the mainframe operating system and security software.

Subsequent to the completion of our fieldwork, the Chief of MASS informed us that he formally assigned information system security officers for each of the IRS campuses and computing centers, and the IRS network and held specialized training for these officers.

Testing and Evaluating the Effectiveness of Controls

The final key element of an information security program is ongoing testing and evaluation to ensure that systems are in compliance with policies, and that policies and controls 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.

IRS performs periodic testing and evaluation of its Unix, Windows, and Mainframe systems. Specifically, IRS uses software tools and monitoring reports to determine if its systems are in compliance with agency information security policies, procedures, and practices. However, output from these tools was not always reliable and accurate. Further, IRS did not effectively audit and monitor the facility's information security systems. Specifically, user activity on critical Unix systems were not being logged, full auditing of system user rights was not always occurring, audit logs on Windows servers were not always retained, and monitoring reports detailing security-related events on mainframe computers were not always complete.

Until IRS fully implements an effective program, it will not be able to ensure the security of its highly interconnected computer environment, facilities, and resources. Moreover, IRS will not be able to ensure the confidentiality, integrity, or availability of the sensitive financial, taxpayer, and Bank Secrecy Act data that it processes, stores, and transmits. As a result, IRS's operations and assets remain vulnerable to unauthorized disclosure, manipulation, use, or destruction.

Conclusions

Significant information security weaknesses exist at IRS that place sensitive financial, taxpayer, and Bank Secrecy Act data at risk of disclosure, modification, or loss, possibly without detection, and place IRS's operations at risk of disruption. Specifically, IRS has not consistently implemented effective electronic access controls, including user accounts and passwords, access rights and permissions, and network security, or fully implemented a program to audit and monitor access activity. In addition, weaknesses in physical security, segregation of duties, and service continuity increase the level of risk. Although IRS continues to make progress in mitigating previously reported information security weaknesses and implementing general controls over key financial and tax processing systems at the facility, it has not taken all the necessary steps to mitigate known information security control weaknesses and to ensure the confidentiality, integrity, and availability of taxpayer and Bank Secrecy Act data. Consequently, taxpayer and Bank Secrecy Act data may have been disclosed to unauthorized individuals. Ensuring that known weaknesses affecting IRS's computing resources are promptly mitigated and that general controls are effective to protect the facility's computing environment require top management support and leadership, disciplined processes, and consistent oversight. Until IRS takes steps to mitigate these weaknesses and fully implements its agencywide information security program, limited assurance exists that taxpayers' personal information and IRS-processed law enforcement information will be adequately safeguarded against unauthorized disclosure, modification, or destruction.

Recommendations for Executive Action

To help fully implement IRS's information security program, we recommend that Secretary of the Treasury direct the IRS Commissioner to take the following three actions:

- Ensure that established security policies and procedures are consistently followed and implemented.

-
- Ensure that employees with significant information security responsibilities are provided the sufficient training and understand their role in implementing security related policies and controls.
 - Implement an ongoing process of testing and evaluating IRS's information systems to ensure compliance with established policies and procedures.

In addition, we recommend that the Secretary of the Treasury direct the IRS Commissioner to perform an assessment to determine whether taxpayer data has been disclosed to unauthorized individuals.

Further, we recommend that the Secretary of the Treasury direct the FinCEN Director to perform an assessment to determine whether Bank Secrecy Act data have been disclosed to unauthorized individuals.

We are also making recommendations in a separate report designated for "Limited Official Use Only." These recommendations address actions needed to correct the specific information security weaknesses related to electronic access controls and other information system controls at the facility.

Agency Comments

In providing written comments on a draft of this report (reprinted in app. I), the Acting Deputy Secretary of the Treasury generally concurred with our recommendations in both the public and Limited Official Use Only reports and identified specific corrective actions that IRS has taken or plans to take to address the recommendations.

The Acting Deputy Secretary of the Treasury concurred with our recommendation to take several actions to fully implement an effective agencywide information security program. The Acting Deputy stated that IRS continues to make progress in addressing the computer security deficiencies throughout the agency, as noted in our public and Limited Official Use Only reports. The Acting Deputy stated that in mid-2004, IRS began an agencywide initiative to complete required security activities, such as the development of security plans and security testing by fiscal year 2005.

The Acting Deputy's comments also addressed several completed corrective actions, including properly configuring access rights to the mainframe computing environment, auditing the activity of high-level user

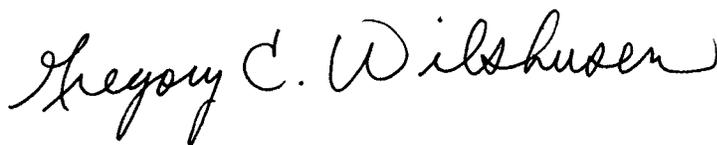
access on the mainframe environment, capturing and pursuing all security violations, designating Information Systems Security Officers at all IRS locations, and establishing the position of Director, Information Technology Security to ensure that the overall design of new applications and the operation of current systems adhere to security requirements.

The Acting Deputy Secretary also concurred with our recommendation to direct the IRS Commissioner to perform an assessment to determine whether taxpayer data have been disclosed to unauthorized individuals.

Regarding our recommendation to direct the FinCEN Director to perform an assessment to determine whether Bank Secrecy Act data have been disclosed to unauthorized individuals, the Acting Deputy stated that it is more appropriate to have IRS conduct this review because FinCEN does not have the legal authority to conduct such an assessment of IRS tax information. This alternative approach meets the intent of our recommendation as long as IRS reports the results of its assessment to the Director of FinCEN.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the House Committee on Government Reform; House and Senate Committees on Appropriations; House and Senate Committees on Budget; Secretary of the Treasury; Commissioner of Internal Revenue; and Treasury's Director, Financial Crimes Enforcement Network. We also will make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your office have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-3317 or Keith A. Rhodes at (202) 512-6412; we can also be reached by e-mail at wilshuseng@gao.gov or rhodesk@gao.gov. Other contacts and key contributors to this report are listed in appendix II.



Gregory C. Wilshusen
Director, Information Security Issues



Keith A. Rhodes
Chief Technologist

Comments from the Secretary of the Treasury



THE DEPUTY SECRETARY OF THE TREASURY
WASHINGTON

April 14, 2005

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

Dear Mr. Wilshusen:

I am writing to provide the Treasury Department's comments on the Government Accountability Office's draft report, entitled *Information Security: Internal Revenue Service Needs to Remedy Serious Weaknesses Over Taxpayer and Law Enforcement Data*, and its related limited-official use report. The draft report contains three recommendations. The first two recommend that the IRS fully implement an effective agency-wide information security program and assess whether taxpayer data have been disclosed to unauthorized individuals. The third recommends that the Financial Crimes Enforcement Network (FinCEN) assess whether law enforcement data have been disclosed to unauthorized individuals.

With regard to the first recommendation and other findings related to the IRS that you presented in the report, the IRS continues to make progress in addressing computer security deficiencies throughout the agency. Many weaknesses have been corrected and additional controls have been implemented; however, more challenges remain and are being addressed. The IRS began an extremely aggressive initiative in mid-2004 to complete the full suite of required security activities at each of its computing centers and campuses and to support security certification and accreditation. This is being accomplished using the latest processes and guidance specified by the National Institute for Standards and Technology and in accordance with the requirements of the Federal Information Security Management Act (FISMA). The security activities include the development of security plans, security documentation, and security testing. These activities are scheduled to be completed in FY 2005 at all of the computing centers and campuses. In addition, access rights to the mainframe computing environment at the facility have now been properly configured, and the mainframe computing environment makes use of additional auditing tools. The output logs generated by these tools are reviewed regularly by the computing center IT staff and the security staff. The activities of any user with higher level system privileges are specifically audited by the tools in place, and all security violations are captured and aggressively pursued.

Appendix I
Comments from the Secretary of the
Treasury

To facilitate the accomplishment of the required security activities, the IRS implemented several organizational changes. For example, the IRS's Mission Assurance and Support Services organization designated Information Systems Security Officers for each computing center and campus. These security professionals are responsible for day-to-day security operations. Moreover, the IRS's Chief Information Officer established the position of Director of Information Technology Security, to ensure that the overall design of new applications and the operation of current systems adhere to security requirements.

Further, as mandated by FISMA, all IRS senior officials are engaged in fulfilling their security responsibilities for the business systems and applications in operation at the computing centers and campuses. To strengthen the security program, the IRS recognizes that compliance with established policies and procedures is mandatory. Accordingly, specialized security technical training is currently underway to support the secure operations of IRS's complex computing environments. Enhanced security processes are being defined for all new systems developments and systems upgrades. The IRS anticipates significantly improved performance in this summer's FISMA annual systems security review. This review should also demonstrate noteworthy progress in the establishment of a more robust agency-wide information security program. Due to proactive initiatives, the IRS anticipates achieving noteworthy progress by the end of this fiscal year in resolving or mitigating GAO and the Treasury Department Inspector General for Tax Administration (TIGTA) audit findings and weaknesses. Finally, the IRS has developed mandatory testing activities for all systems.

With regard to the second recommendation, ensuring taxpayer data integrity is a responsibility that the IRS does not take for granted. The mainframe system at the facility is audited yearly by either GAO or TIGTA. The facility has operated the systems containing Bank Secrecy Act information since the early 1980s, and there has never been a separate system to administer the requirements of the Act. This audit is the first to identify the issue of how the data at the facility are segmented, and now that it has been identified as an issue, the IRS is working to address the finding. Therefore, the IRS will assess the extent to which taxpayer data may have potentially been disclosed to unauthorized individuals.

With regard to the third recommendation, related to FinCEN, we concur that it is appropriate to assess whether Bank Secrecy Act data have been disclosed to unauthorized individuals as a result of the GAO findings. However, the IRS is the more appropriate entity to conduct this review of its audit and monitoring capabilities. Moreover, FinCEN does not have the legal authority under Title 26 to assess systems housing IRS tax information. Such an assessment would be very difficult for FinCEN to accomplish.

I would like to request that throughout your report, all references to FinCEN's data as "law enforcement data" be changed to "Bank Secrecy Act data" (including in the report's title). Also, please note that on page 7, second paragraph, second sentence, the words "criminal referrals of" need to be deleted.

Appendix I
Comments from the Secretary of the
Treasury

To ensure the Treasury Department takes all necessary steps to address the issues identified in the audit, I have asked the Chief Information Officer to review the status of these efforts on a quarterly basis and keep me informed of our progress.

Thank you for the opportunity to respond to this draft GAO report. If you have any questions or wish to discuss these comments further, please contact Barry K. Hudson (Acting Chief Financial Officer) at (202) 622-0750.

Sincerely,



Arnold I. Havens
Acting Deputy Secretary

cc: Mark W. Everson, Commissioner, IRS
William J. Fox, Director, FinCEN
Ira L. Hobbs, Chief Information Officer

GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer Wilson, (202) 512-9192

**Staff
Acknowledgments**

In addition to the individual named above, Gerald Barnes, Bruce Cain, Joseph Cruz, Joanne Fiorino, Denise Fitzpatrick, Ed Glagola, David Hayes, Myong Suk Kim, Harold Lewis, Mary Marshall, Duc Ngo, Ron Parker, Charles Roney, Eugene Stevens, and Henry Sutanto 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