

**GAO**

Report to the Subcommittee on  
Technology, Information Policy,  
Intergovernmental Relations and the  
Census, Committee on Government  
Reform, House of Representatives

---

November 2003

# INFORMATION SECURITY

## Improvements Needed in Treasury's Security Management Program





# INFORMATION SECURITY

## Improvements Needed in Treasury's Security Management Program

Highlights of [GAO-04-77](#), a report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

### Why GAO Did This Study

The Department of the Treasury relies heavily on information systems—and on the public’s trust in its work. Information security is therefore critical to Treasury operations. In support of its annual audit of the government’s financial statements, GAO assessed the effectiveness of (1) Treasury’s information security controls in protecting the confidentiality, integrity, and availability of the department’s systems and data and (2) Treasury’s implementation of its departmentwide information security program.

In assessing the adequacy of Treasury’s information security program, GAO focused on the effectiveness of its departmentwide policies and processes, rather than on bureau-specific directives and guidance.

### What GAO Recommends

GAO recommends that the Secretary of the Treasury direct the chief information officer to take specific actions to implement a more effective departmentwide information security program and improve management oversight of Treasury’s operating bureaus.

Treasury’s chief information officer, responding on behalf of the department, concurred with our assessment and recommendations.

[www.gao.gov/cgi-bin/getrpt?GAO-04-77](http://www.gao.gov/cgi-bin/getrpt?GAO-04-77).

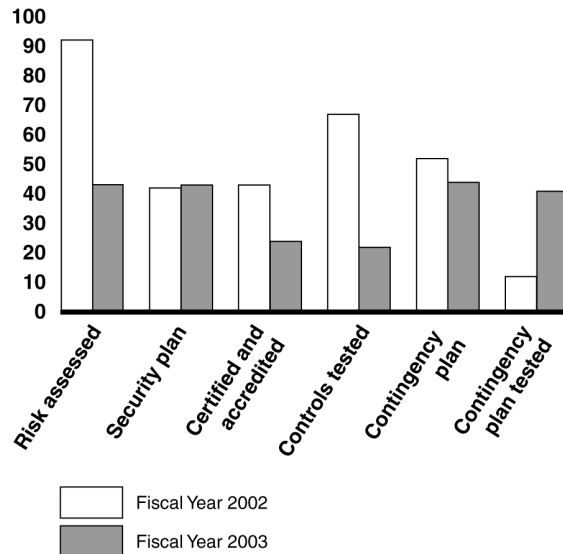
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or [daceyr@gao.gov](mailto:daceyr@gao.gov).

### What GAO Found

The Department of the Treasury and its key bureaus have not consistently implemented information security controls to protect the confidentiality, integrity, and availability of their information systems and data. Several bureaus have reported effective controls over their systems. However, long-standing information security weaknesses in access and software change controls, segregation of duties, and service continuity have been consistently identified at certain key Treasury bureaus, such as IRS and the Financial Management Service. Weaknesses at these bureaus place the sensitive information managed by the bureaus at increased risk of unauthorized access, use, disclosure, disruption, modification, or destruction. Moreover, bureaus have not consistently implemented key information security requirements. An analysis of performance data for the 11 Treasury bureaus that reported on these requirements for fiscal years 2002 and 2003 reveals that most Treasury systems did not meet certain key information security requirements in fiscal year 2003 and that the percentage of systems that meet certain requirements has decreased from fiscal year 2002 (see chart).

The information security weaknesses and inconsistent implementation of security controls at Treasury bureaus exist, in part, because Treasury’s departmentwide security program, while evolving, has not yet been fully institutionalized across the entire department. During fiscal year 2003, Treasury launched or expanded several initiatives to implement key elements of its program. However, additional actions are needed to effectively and consistently implement information security controls throughout the department.

**Percentage of Treasury Systems Meeting Certain Information Security Requirements**  
Percentage of total systems



Source: GAO analysis of Treasury data.

---

# Contents

---

<b>Letter</b>		1
	Results in Brief	1
	Background	2
	Objectives, Scope, and Methodology	6
	Implementation of Information Security Controls Has Been Inconsistent	7
	Treasury Has Begun to Implement Key Elements of a Departmentwide Information Security Program, but Challenges Remain	20
	Conclusions	26
	Recommendations for Executive Action	26
	Agency Comments	26
<b>Appendix I</b>	<b>Comments from the Department of the Treasury</b>	28
<b>Related GAO Products</b>		29
<b>Table</b>		
	Table 1: Analysis of BPD's Prior Year Weaknesses	9
<b>Figures</b>		
	Figure 1: Percentage of Systems with Risk Assessments during Fiscal Year 2003	15
	Figure 2: Percentage of Systems with Up-to-Date Security Plans during Fiscal Year 2003	16
	Figure 3: Percentage of Systems Certified and Accredited for Fiscal Year 2003	17
	Figure 4: Percentage of Systems with Security Controls Tested in Fiscal Year 2003	18
	Figure 5: Percentage of Systems with Tested Contingency Plans	19
	Figure 6: Percentage of Treasury Systems Meeting Certain Information Security Requirements	23

---

---

## Abbreviations

BPD	Bureau of the Public Debt
CIO	chief information officer
FISMA	Federal Information Security Management Act
FMS	Financial Management Service
GISRA	Government Information Security Reform Act
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	plan of action and milestones
TIGTA	Treasury Inspector General for Tax Administration

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.



G A O

Accountability \* Integrity \* Reliability

United States General Accounting Office  
Washington, DC 20548

---

November 14, 2003

The Honorable Adam H. Putnam  
Chairman  
The Honorable William Lacy Clay, Jr.  
Ranking Minority Member  
Subcommittee on Technology, Information Policy,  
Intergovernmental Relations and the Census  
Committee on Government Reform  
House of Representatives

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. Federal agencies face increasing security risks from viruses, hackers, and others who seek to disrupt federal operations or obtain sensitive information stored in federal computers.

The Department of the Treasury, which collects and maintains a significant amount of sensitive information, needs effective security controls to prevent the improper disclosure, manipulation, or destruction of this information. This report presents the results of our evaluation of the effectiveness of Treasury information security controls at key bureaus and its implementation of a departmentwide information security program. In response to your request, we are addressing this report to you.

---

## Results in Brief

Treasury and its key bureaus have been inconsistent in implementing information security controls to protect the confidentiality, integrity, and availability of their systems and data. Several Treasury bureaus have reported effective controls that help to secure and protect their information systems and data. However, long-standing weaknesses in information security controls (including logical access controls, physical security, software change controls, segregation of duties, and service continuity) at key bureaus have reduced these bureaus' effectiveness in preventing and detecting unauthorized access to sensitive systems and data, protecting and controlling physical access to assets, mitigating the risk of unauthorized or inappropriate software programs, minimizing the risk of errors or fraud, and ensuring the continuity of data processing operations when unexpected interruptions occur. In addition, Treasury bureaus have not consistently performed required information security

---

activities. These weaknesses expose Treasury to increased risks of unauthorized disclosure and modification of data and disruption of service that threaten the confidentiality, integrity, and availability of its sensitive systems and data.

The information security weaknesses and inconsistent security practices identified at the bureaus exist, in part, because Treasury's departmentwide security program, while evolving, is not yet fully institutionalized across the entire department. Prior to fiscal year 2003, Treasury had not provided adequate direction and oversight to ensure that the bureaus fully or consistently implemented effective information security controls. During fiscal year 2003, Treasury launched or expanded several initiatives that were designed to promote the implementation of key elements of its departmental information security program. Although Treasury has made progress implementing these initiatives, it remains challenged to effectively and consistently implement security controls across the department. The effects of a major reorganization on departmental information technology security staffing, the lack of a designated senior agency information security official, and issues relating to the reliability and completeness of performance management data contribute to the challenges confronting Treasury as it endeavors to improve the security of its information systems and data. Until Treasury can fully implement its departmentwide program and adequately mitigate known weaknesses, increased risk exists that individuals could gain unauthorized access to critical hardware and software, and intentionally or inadvertently use, disclose, disrupt, modify, or destroy sensitive data or computer programs.

We are making recommendations to the Secretary of the Treasury that address these issues. In providing written comments on a draft of this report, the Treasury chief information officer responded on behalf of the department and concurred with our assessment and recommendations, and provided technical comments that were incorporated into the report as appropriate.

---

## Background

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, these factors 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 concerns about attacks from individuals and groups with such malicious intent, including terrorists. These concerns are well founded for a number of reasons, including the dramatic increase in reported computer 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 cyber attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent computer security weaknesses that place a variety of critical federal operations, including those at Treasury, at risk of disruption, fraud, and inappropriate disclosure.<sup>1</sup> This body of audit evidence led us, in 1997, to designate computer security as a governmentwide high-risk area in reports to the Congress.<sup>2</sup> It remains so today.<sup>3</sup>

How well federal agencies are addressing these risks is a topic of increasing interest in both the Congress and the executive branch. This is evidenced by recent hearings on information security<sup>4</sup> and recent legislation intended to strengthen it—the Federal Information Security Management Act (FISMA) and the Government Information Security Reform (GISRA) provisions of the Fiscal Year 2001 National Defense Authorization Act.<sup>5</sup> In addition, the administration has taken important

---

<sup>1</sup>U.S. General Accounting Office, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, [GAO/AIMD-00-295](#) (Washington, D.C.: Sept. 6, 2000).

<sup>2</sup>U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: February 1997).

<sup>3</sup>U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, [GAO-03-121](#) (Washington, D.C.: January 2003).

<sup>4</sup>U.S. General Accounting Office, *Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*, [GAO-03-852T](#) (Washington, D.C.: June 24, 2003); *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, [GAO-03-564T](#) (Washington, D.C.: Apr. 8, 2003); *Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk*, [GAO-03-303T](#) (Washington, D.C.: Nov. 19, 2002).

<sup>5</sup>Federal Information Security Management Act (FISMA), Title III, Public Law 107-347, Dec. 17, 2002, and the Government Information Security Reform provisions (commonly referred to as GISRA) of the Fiscal Year 2001 National Defense Authorization Act, Division A, Title X, Subtitle G, Public Law 106-398, Oct. 30, 2000.

---

actions to improve information security, such as integrating information security into the President's Management Agenda Scorecard. Moreover, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued security guidance to agencies.

---

## Treasury Helps Promote the Nation's Economy and Manages Federal Finances

The Department of the Treasury is responsible for promoting prosperous and stable domestic and international economies, managing the government's finances, and safeguarding federal financial systems. Treasury is organized into two major components—departmental offices and operating bureaus. The departmental offices are primarily responsible for formulating policy and managing the department as a whole, while the operating bureaus carry out the specific functions of the department. The basic functions of the department include

- managing federal finances;
- collecting taxes and monies due to the U.S. and making most of the payments of the U.S. government;
- producing all postage stamps, currency, and coinage;
- managing government accounts and the public debt;
- supervising national banks and thrift institutions;
- advising on domestic and international financial, monetary, economic, trade, and tax policy;
- enforcing federal finance and tax laws; and
- investigating and prosecuting tax evaders.

In fiscal year 2003, Treasury experienced significant organizational changes. The Homeland Security Act of 2002<sup>6</sup> (signed by the President on November 25, 2002) called for several Treasury bureaus or elements to be transferred to the newly formed Department of Homeland Security and to the Department of Justice. On January 24, 2003, the Bureau of Alcohol,

---

<sup>6</sup>Public Law 107-296.



---

Tobacco, and Firearms' law enforcement function moved to Justice. The tax and trade functions of the bureau remained with Treasury under the newly formed Alcohol and Tobacco Tax and Trade Bureau. On March 1, 2003, three Treasury bureaus moved to Homeland Security: the Federal Law Enforcement Training Center, the U.S. Customs Service, and the U.S. Secret Service. The reorganized department had a fiscal year 2003 budget of \$10.7 billion and a staff of about 115,000. Staff located at the bureaus makes up about 97 percent of the Treasury work force.

To support the department's overall mission, Treasury and its key bureaus, including the Internal Revenue Service (IRS)—by far the largest; Financial Management Service (FMS); U.S. Mint; and the Bureau of the Public Debt (BPD), have diverse functions. For example, IRS is responsible for determining, assessing, and collecting internal revenue in the United States. It collects taxes, processes tax returns, and enforces the nation's tax laws. In fiscal year 2003, IRS processed about 130 million<sup>7</sup> individual tax returns, accounted for almost \$2 trillion in collections, and paid about \$300 billion in refunds to taxpayers. FMS receives and disburses public monies, maintains government accounts, and prepares reports on the status of government finances. As the government's financial manager, FMS disbursed more than \$1.6 trillion in fiscal year 2003. BPD borrows the money needed to finance the federal government and administers the public debt through Treasury financial instruments. It is responsible for ensuring that reliable systems and processes are in place for purchasing and servicing Treasury securities. In fiscal year 2003, BPD conducted about 200 auctions and issued about \$4 trillion in marketable securities.

Treasury and its bureaus rely heavily on information management systems to fulfill their many financial management stewardship roles and responsibilities for the nation. The bureaus have distinct, numerous, and complex information systems to process, store, and secure highly sensitive data. Treasury and its bureaus report in fiscal year 2003 that they have 708 distinct information systems supporting their operations. A centralized data communications network and management system interconnects networks and systems at the bureaus and departmental offices.

FISMA provides that the Secretary of the Treasury is responsible for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from

---

<sup>7</sup>As of August 31, 2003.

---

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. Treasury's CIO is responsible for developing and maintaining a departmentwide information security program; developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements; and assisting senior agency officials concerning their responsibilities under the act. In addition, the CIO provides oversight, strategic management, and policy direction on all information security programs within Treasury. The Office of Security Compliance within the Office of the CIO is responsible for developing departmentwide information security policies and ensuring bureau implementation. Each bureau is responsible for implementing Treasury-mandated security policies within its domain. In order to implement departmentwide security policies, the bureaus are required to develop their own information security programs, including their own security compliance functions.

---

## Objectives, Scope, and Methodology

Our objectives were to (1) determine whether Treasury and its key bureaus have effectively implemented information security controls to protect the confidentiality, integrity, and availability of their systems and data and (2) determine whether Treasury has effectively implemented its departmentwide information security program.

To determine the effectiveness of the information security controls implemented at Treasury and its bureaus, we considered the results of prior information security reviews that we performed at IRS, BPD, and FMS. We also examined and analyzed the contents of audit reports and associated work papers for information security and internal control<sup>8</sup> reviews performed by the Treasury Office of the Inspector General (OIG) or independent auditors in connection with their audits of the bureaus' financial statements. In addition, we reviewed the department's

---

<sup>8</sup>A review of an entity's internal controls includes a review of the information security controls—general controls and application controls—that protect an organization's computer environment.

---

performance and accountability reports to document Treasury's information security-related weaknesses.

To assess Treasury's departmentwide information security program, we

- reviewed and evaluated the department's information security policies in effect at the time of our review;
- analyzed data presented in Treasury's GISRA report for fiscal year 2002 and FISMA report for fiscal year 2003;<sup>9</sup>
- examined and assessed reports and other documents related to the department's information security program, and
- interviewed Treasury officials regarding their processes and procedures for overseeing, monitoring, evaluating, and reporting on the implementation of information security across the department.

Our review was performed at Treasury headquarters and our headquarters in Washington, D.C., from March through October 2003, in accordance with generally accepted government auditing standards.

---

## Implementation of Information Security Controls Has Been Inconsistent

The effective implementation of appropriate, properly designed security controls is an essential element for ensuring the confidentiality, integrity, and availability of information systems and information. Weak security controls can expose information systems and information to an increased risk of unauthorized access, use, disclosure, disruption, modification, and destruction.

Treasury's bureaus have not consistently implemented effective information security programs and resolved known information security control weaknesses. Some bureaus have consistently reported implementing effective controls over their information systems and/or limiting the negative effect control weaknesses could have on the preparation of financial statements and internal controls. Other key Treasury bureaus, including IRS and FMS, have reported long-standing weaknesses in information security controls and continued to report

---

<sup>9</sup>GISRA expired Nov. 29, 2002. Effective Dec. 17, 2002, FISMA replaced GISRA with similar, but strengthened, provisions.

---

significant weaknesses in fiscal year 2002. As a result of the weaknesses and inconsistencies in the overall implementation of the bureaus' information security programs, the Treasury OIG designated information security as a departmentwide material weakness<sup>10</sup> in its fiscal year 2002 financial audit report.

---

### Several Bureaus Have Effectively Implemented Controls

Several Treasury bureaus have consistently implemented effective information security controls over their computing environments and/or implemented compensating controls to correct or mitigate the weaknesses identified during previous audits. For example, the external auditors for the Office of Thrift Supervision, the Office of the Comptroller of the Currency, and the Bureau of Engraving and Printing have not reported significant information security control weaknesses. BPD has also consistently implemented internal control over its financial systems. Since 1997 we have reviewed the general and application controls over key BPD systems as part of our audit of the Schedule of Federal Debt managed by BPD. We found that, although security over its computer systems and service continuity controls needed strengthening, BPD maintained, in all material respects, effective internal control, including general and application computer controls, related to reporting reliable financial information on the Schedule of Federal Debt.

In instances in which information security improvements were needed, BPD management has been responsive in taking corrective action or in implementing compensating controls to mitigate the weaknesses identified during our reviews. As the following table indicates, our subsequent audits have found that, as of May 2003, BPD had taken action to correct or mitigate a substantial percentage of the security weaknesses reported during the prior year's audit.

---

<sup>10</sup>A material weakness is a condition that precludes the agency's internal controls from providing reasonable assurance that material misstatements in the financial statements would be prevented or detected on a timely basis.

**Table 1: Analysis of BPD's Prior Year Weaknesses**

Fiscal year audited	Weaknesses from prior year	Weaknesses resolved	
		Number	Percentage
2002	17	12	71
2001	13	8	62
2000	17	16	94
<b>Total/Average</b>	<b>47</b>	<b>36</b>	<b>77</b>

Source: GAO.

## Key Bureaus Have Ineffective Security Controls

Strengthening information systems controls at other bureaus is one of the management challenges currently facing the Department of the Treasury. In fiscal year 2002, significant information security weaknesses existed in the computer systems used at key Treasury bureaus to process sensitive information and data needed to accomplish Treasury's mission. Weaknesses span all six general control audit areas addressed in our information security audit methodology.<sup>11</sup> These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. We identified information systems security as a major challenge for Treasury in our 2003 performance and accountability report on the department.<sup>12</sup> The following examples highlight the serious information security weaknesses that existed at Treasury's key bureaus.

<sup>11</sup>U.S. General Accounting Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999).

<sup>12</sup>U. S General Accounting Office, *Major Management Challenges and Program Risks: Department of the Treasury*, GAO-03-109 (Washington, D.C.: January 2003).

Since 1992,<sup>13</sup> we have reviewed the effectiveness of IRS information security in connection with our annual audit of IRS's financial statements and conducted information security reviews over IRS's computing facilities and electronic filing systems at the request of the Congress. The results of these reviews have led us each year to designate information security as a material weakness. During the 3-year period ending July 31, 2002, we conducted 14 information security reviews at 11 IRS tax processing facilities nationwide. These reviews identified 765 specific general control weaknesses and demonstrate the departmentwide challenge IRS and Treasury face in addressing information security. In addition, we conducted 5 application control reviews and reported 112 application control weaknesses during this same period. While the majority of general control weaknesses identified fell in the area of logical access controls, weaknesses in physical security, software change controls, segregation of duties, and service continuity also posed significant risk to IRS systems and taxpayer information, as the following illustrates:

- Inadequate logical access controls diminished the reliability of IRS's computerized data and increased the risk of unauthorized disclosure, modification, and use of sensitive systems and taxpayer data. Logical access controls at IRS facilities did not effectively prevent, limit, or detect access to computing resources. IRS did not adequately control user accounts and passwords to ensure that only authorized individuals were allowed access to computer systems. Inactive and unused user system accounts were found at all 11 IRS computing facilities reviewed. In addition, IRS inappropriately granted powerful operating system privileges to users who did not need them and granted users access to certain system files for which they had no business need. Further, inadequate controls over network services and devices were found that could allow intruders to gain unauthorized access to valuable information about IRS systems without logging on to the systems.
- Physical security control weaknesses, such as inadequate physical barriers and ineffective screening of visitors, contributed to weakening the perimeter security at several IRS facilities. As a result, increased risk exists that individuals could gain unauthorized access to facility grounds, buildings, sensitive computing resources, and taxpayer data, without detection.

---

<sup>13</sup>U.S. General Accounting Office, *Financial Audit: Examination of IRS's Fiscal Year 1992 Financial Statements*, GAO/AIMD-93-2 (Washington, D.C.: June 30, 1993).

- 
- Software change control procedures at two facilities did not provide sufficient control mechanisms to ensure that the facilities received all authorized program updates. In addition, software developer accounts and/or development tools were allowed on production servers at five facilities, which increases the risk that individuals could make unauthorized modifications to production software on these servers.
  - Inadequate segregation of duties was also an issue, as IRS did not consistently separate incompatible computer-related activities among individuals performing system administration and security administration duties at its computing facilities. In addition, IRS assigned incompatible operating system privileges to users, such as granting auditing privileges to system administrators at 10 facilities. As a result, increased risk exists that erroneous or unauthorized activity could occur and go undetected.
  - Service continuity control weaknesses limited IRS's ability to restore and continue critical data processing services in the event of unexpected service interruptions. IRS had not developed disaster recovery plans for certain key systems and/or had not adequately tested service continuity plans at several facilities. As a result, increased risk exists that IRS will not be able to protect or recover essential information and critical business processes in the event of an unexpected interruption of service.

IRS has made progress in correcting the general and application control weaknesses identified in our information security reviews during this 3-year period. In May 2003 we reported that IRS had corrected about one-third of the 765 general control weaknesses and 55 percent of the application control weaknesses identified in our reviews.<sup>14</sup> Although IRS has corrected a significant number of weaknesses, many significant weaknesses in information security controls remain.

## Financial Management Service

FMS has experienced long-standing weaknesses in its computer controls. It has reported its overall information systems security environment as a material weakness every year since fiscal year 1998. Treasury has recognized the seriousness of this problem and reported FMS's computer controls as a material weakness in its annual accountability reports for each of those fiscal years. In January 2002, we reported that FMS's overall information security control environment was ineffective in identifying,

---

<sup>14</sup>U.S. General Accounting Office, *Information Security: Progress Made, but Weaknesses at the Internal Revenue Service Continue to Pose Risks*, GAO-03-44 (Washington, D.C.: May 30, 2003).

---

deterring, and responding promptly to computer control weaknesses.<sup>15</sup> In November 2002, the independent external auditor responsible for auditing FMS's fiscal year 2001 and 2002 financial statements reported a material weakness in the general controls over the Hyattsville (Md.) Regional Operations Center. The external auditor reported that general controls did not effectively prevent (1) unauthorized access to the disclosure of sensitive information, (2) unauthorized changes to systems and application software, (3) unauthorized access to programs and files that control computer hardware and secure applications, or (4) disruption of critical operations. Specifically, the external auditor found weaknesses in the following areas:

- *Access controls.* The majority of information security weaknesses were identified in this area. Weaknesses were found in the administration of access controls, access to computer programs and files, and access to sensitive data.
- *Systems software.* The development and enforcement of systems software policies and procedures over usage and modifications to operating system upgrades and utilities were inadequate.
- *Change controls.* Configuration change management control procedures were not consistently enforced across all major FMS applications reviewed.
- *Service continuity.* Although FMS has completed its business impact assessment,<sup>16</sup> the results of this assessment had not been incorporated into detailed disaster recovery plans.

Although the independent external auditor reported that FMS had made improvements in its information security control environment during fiscal year 2002, the external auditor was critical of the overall effectiveness of FMS's information security management program. FMS management was still in the process of implementing its new entitywide security plan—authorized in September 2002—for most of the year under audit. While FMS has corrected vulnerabilities in some areas, subsequent

---

<sup>15</sup>U.S. General Accounting Office, *Financial Management Service: Significant Weaknesses in Computer Controls Continue*, [GAO-02-317](#) (Washington, D.C.: Jan. 31, 2002).

<sup>16</sup>FMS's business continuity planning activities have been split into two phases: conducting a business impact assessment and preparing detailed recovery plans.



---

reviews have found that previously identified weaknesses continue to exist on other systems.

U.S. Mint

Significant information security weaknesses also existed at the U.S. Mint. The independent external auditor responsible for auditing the Mint's fiscal year 2001 financial statements identified numerous general and application control weaknesses. Due to the magnitude of these weaknesses, the external auditor reported two separate material weaknesses—one for general controls and one for application controls. In its audit report on the Mint's fiscal year 2002 financial statements, the external auditor aggregated the two previously reported material weaknesses into one material weakness on information systems controls. The auditor noted that the Mint had made improvements in its computer control environment and systems security control activities, which included the development of a comprehensive corrective action plan, and hired a new chief information officer. However, the external auditor noted weaknesses in the Mint's information systems general controls relating to its network infrastructure, systems documentation, software change control, and related security policies and procedures.

---

**Bureaus Have Not Consistently Performed Required Information Security Activities**

Assessing and managing the risks associated with information systems are key elements of an information security program. FISMA<sup>17</sup> and other federal guidance<sup>18</sup> require federal agencies to develop comprehensive information security programs based on assessing and managing risks. OMB requires agencies to report performance measure data related to required aspects of their information security programs. These data include the number and percentage of systems that have

- been assessed for risk and assigned a level of risk,
- up-to-date security plans,
- been certified and accredited,

---

<sup>17</sup>Public Law 107-347, section 301(2002); 44 USC 3544(b).

<sup>18</sup>The February 1996 revision to OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, directs agencies to use a risk-based approach to determine adequate security, including a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

- 
- security controls that have been tested/evaluated within the last year,
  - contingency plans, and
  - tested contingency plans.

Treasury also requires that its bureaus use these same performance measures when reporting to it on the status of bureau information security programs. Performance data reported by the bureaus indicate that the bureaus have not consistently performed these required information security activities and that certain bureaus performed them better than others. For example, bureaus reported that the percentage of systems that they performed these required activities ranged from 0 to 100 percent of their systems.

#### Many Systems Do Not Have Risk Assessments

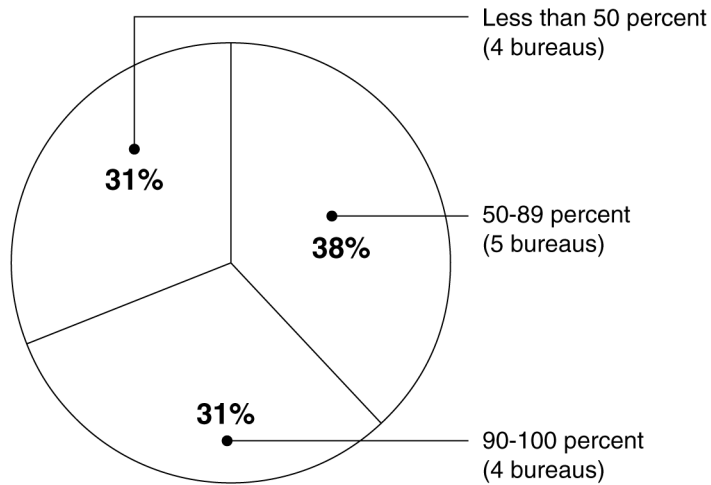
Risk management is a process that allows information technology managers to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information technology systems and data that support organizational missions. Agencies, including Treasury, are required to perform periodic threat-based risk assessments for systems and data. Risk assessments are an essential element of risk management and overall security program management and, as our best practice work has shown, are an integral part of the management processes of leading organizations.<sup>19</sup> Risk assessments help ensure that the greatest risks have been identified and addressed, increase the understanding of risk, and provide support for needed controls.

Treasury bureaus have not consistently assessed their systems for risk. According to Treasury's FISMA report for 2003 and as illustrated in figure 1, four bureaus reported that they had assessed risk for 90 to 100 percent of their systems. However, figure 1 also shows that the other nine bureaus, including the four that reported that less than half of their systems had been assessed for risk, did not consistently assess risks for their systems.

---

<sup>19</sup>[GAO/AIMD-98-68](#).

**Figure 1: Percentage of Systems with Risk Assessments during Fiscal Year 2003**



Source: GAO analysis of Treasury data.

The bureaus also experienced mixed results in fiscal year 2003 with increasing the percentage of their systems that have been assessed for risk. Of the 11 bureaus that reported this security metric in both fiscal years, 4 reported an increase in the percentage of systems assessed for risk in fiscal year 2003 compared with fiscal year 2002, while 4 reported a decrease. The remaining 3 bureaus did not report a change in the percentage of systems assessed for risk.

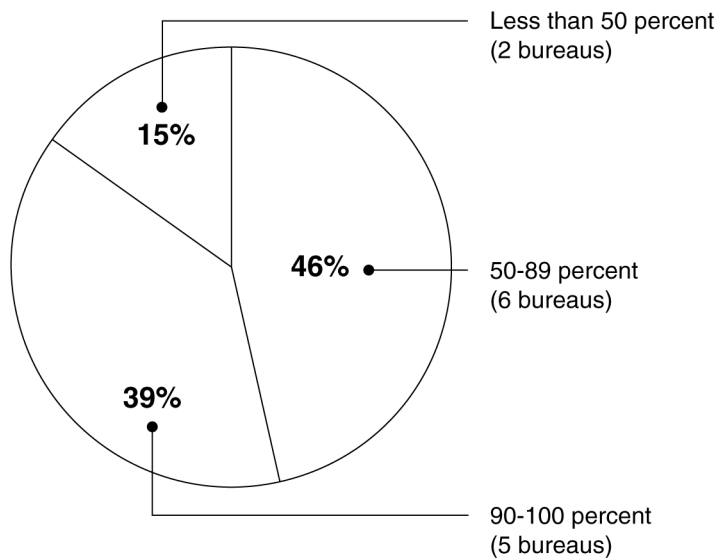
### Systems Often Lack Up-to-Date Security Plans

OMB Circular A-130 requires that security plans be prepared for all federal systems that contain sensitive information. The purpose of these plans is to (1) provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements, (2) delineate the responsibilities and expected behavior of all individuals who access the system, and (3) serve as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Treasury bureaus did not consistently maintain up-to-date security plans for their systems. According to Treasury's FISMA report for 2003, only 304 (43 percent) of the department's 708 systems had up-to-date security plans. Although IRS had by far the largest number of systems without a security plan, 8 of the 13 bureaus reported that they had up-to-date

security plans for less than 90 percent of their systems for fiscal year 2003, as shown in figure 2.

**Figure 2: Percentage of Systems with Up-to-Date Security Plans during Fiscal Year 2003**



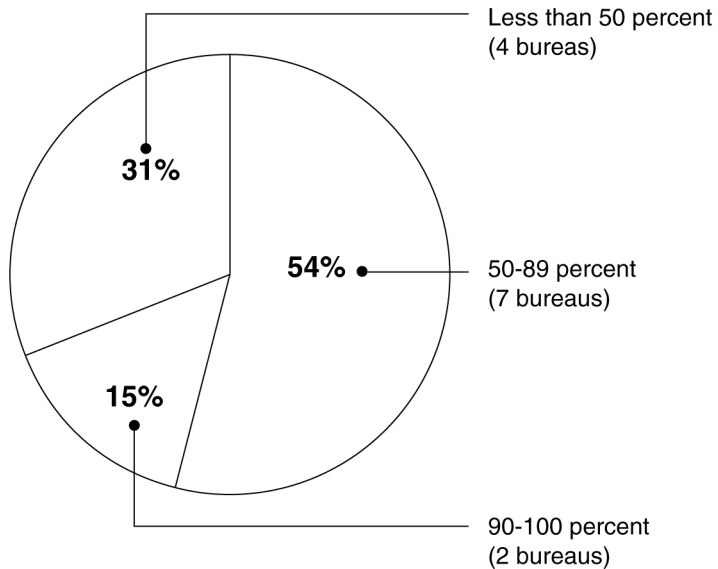
Source: GAO analysis of Treasury data.

### Bureaus Have Not Certified and Accredited Many Systems

OMB and Treasury require management officials to formally authorize the use of each general support system and major application through a certification and accreditation process before it becomes operational, when a significant change occurs, and at least every 3 years thereafter. System certification is based on a technical evaluation of an information system to see how well it meets its security requirements, including all applicable federal laws, policies, regulations, and standards. System accreditation is the written management authorization for a system to operate and/or process information.

Treasury bureaus did not certify and accredit many of their systems. According to Treasury's FISMA report for fiscal year 2003 and as shown in figure 3, 11 of 13 bureaus reported that less than 90 percent of their systems had been certified and accredited for fiscal year 2003. Moreover, 2 bureaus reported that none of their systems had been authorized for processing following system certification and accreditation.

**Figure 3: Percentage of Systems Certified and Accredited for Fiscal Year 2003**



Source: GAO analysis of Treasury data.

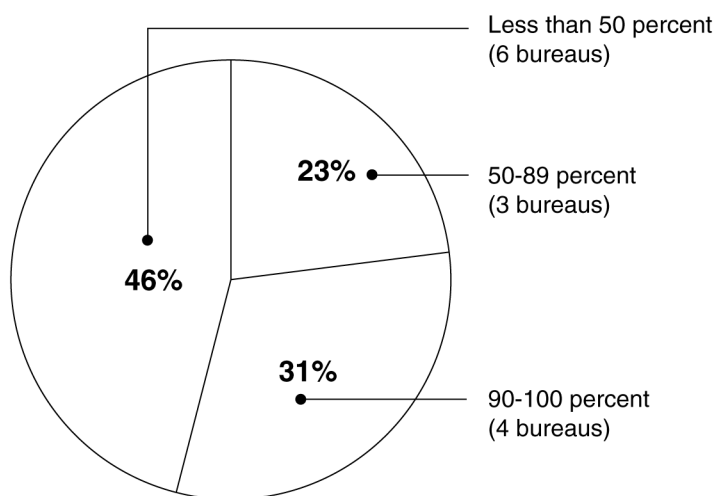
Our analysis of data submitted by the 11 bureaus that reported on this performance measure for both fiscal years 2002 and 2003 showed mixed progress. For example, 5 of the 11 bureaus reported a decrease in the percentage of systems authorized for processing following certification and accreditation, while 5 of the remaining 6 bureaus showed improvement in this area.

### Bureaus Are Not Routinely Testing and Evaluating Security Controls

An agency head is responsible for ensuring that the appropriate agency officials evaluate the effectiveness of the information security program, including testing controls. Further, the agencywide information security program is to include periodic management testing and evaluation of the effectiveness of information security policies and procedures. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost-effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of the program reviews can supplement control testing and evaluation in IG and our audits to help provide a more complete picture of the agency's security posture. FISMA requires that agencies test the management, operational, and technical controls of every information system identified in their inventories of major information systems no less than annually.

Most Treasury bureaus did not test the security controls on each of their inventoried systems during fiscal year 2003. As illustrated below, 9 of the 13 Treasury bureaus reported in Treasury's FISMA report that they had tested the controls on less than 90 percent of their systems for fiscal year 2003, including 6 that tested controls on less than half of their systems.

**Figure 4: Percentage of Systems with Security Controls Tested in Fiscal Year 2003**



Source: GAO analysis of Treasury data.

### Bureaus Have Not Consistently Prepared or Tested Contingency Plans

Contingency plans provide specific instructions for restoring critical systems, including such items as arrangements for alternative processing facilities, in case the usual facilities are significantly damaged or cannot be accessed.

These plans and procedures help to ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, an accidental loss of files, or a major disaster. Contingency plans should also identify which operations and supporting resources are critical and need to be restored first and should be tested to identify their weaknesses. Without such tested plans, agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

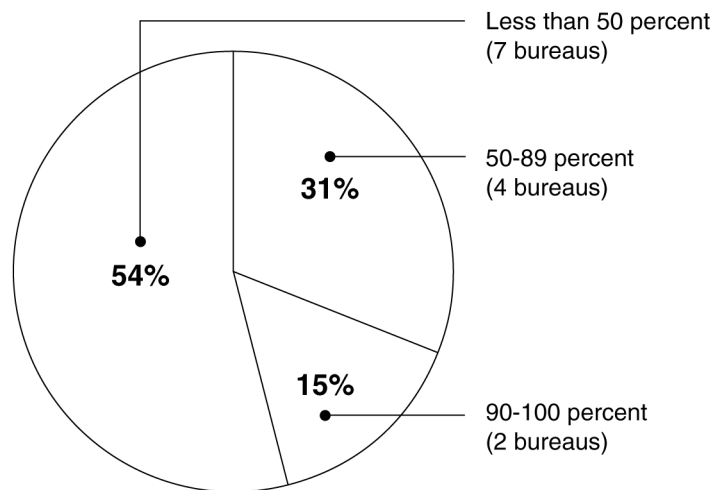
Treasury bureaus have not consistently prepared or tested contingency plans for their information systems. According to Treasury's FISMA report for fiscal year 2003, only 44 percent of its systems had a contingency plan.

---

Bureaus also reported that 41 percent of their systems had tested contingency plans. As shown in figure 5, only 2 of 13 bureaus reported that they had tested contingency plans for at least 90 percent of their systems. Moreover, 4 bureaus reported that none of their contingency plans had been tested.

---

**Figure 5: Percentage of Systems with Tested Contingency Plans**



Source: GAO analysis of Treasury data.

The bureaus' inconsistent track record for performing these essential information security activities can lead to the implementation of insecure systems and/or the implementation of inadequate or inappropriate security controls that do not sufficiently address threats to these systems and could result in costly efforts to subsequently implement effective controls.

---

## Treasury Has Begun to Implement Key Elements of a Departmentwide Information Security Program, but Challenges Remain

The information security weaknesses and inconsistent security practices identified at the bureaus exist, in part, because Treasury's departmentwide security program, while evolving, is not yet fully institutionalized across the entire department. At Treasury, the vast majority of the department's information system assets and computing operations are located at the operating bureaus. Each bureau has been assigned responsibility for developing and maintaining an effective information security program for managing its information security risks, in accordance with departmental policies. Although responsibility for developing and maintaining an effective bureau-specific information security program has been delegated to each operating bureau, broad program responsibility for information security throughout the department is assigned to the Treasury CIO. However, prior to fiscal year 2003, Treasury had not provided adequate direction to or oversight of the bureaus to ensure that key elements of a strong information security program were fully and consistently implemented at each bureau, as the following examples illustrate.

- *Treasury's information security policies and procedures were outdated and incomplete.* The principal policy document governing Treasury's information security program was Treasury Directive 71-10, *Department of Treasury Security Manual*. The primary purpose of this document was to establish comprehensive, uniform security policies, procedures, and guidelines that were to be followed by each bureau in developing its own specific policies and operating directives. However, the security manual contained policies that had not been revised since 1992 and did not reflect current federal guidance. For example, the manual was silent in many areas where security policy was needed, such as voice mail, e-mail, and security-incident reporting. In addition, Treasury's security manual did not provide to the bureaus policies or guidance in the areas of virus protection, audit trails, and warning banners. Although most bureaus have developed their own information security policies, five relied exclusively on these outdated and incomplete policies to implement their information security programs.
- *Treasury had not established effective processes and procedures for monitoring and overseeing the implementation of security at the bureaus.* The Office of Security Compliance within the Office of Treasury CIO is responsible for monitoring Treasury bureaus and ensuring compliance with federal and Treasury security policies. However, prior to fiscal year 2002, the office did not conduct security reviews of bureau information security programs. In fiscal year 2002, the office conducted 35 security reviews of the bureaus' information systems and programs. According to Treasury officials, these reviews were limited in scope, were conducted only at selected bureaus, and did not represent a complete



---

---

## Treasury Is Implementing Elements of an Information Security Program

security program review. For example, some security reviews consisted primarily of reviewing a system's security plan and did not include testing security controls for the system.

To address these issues and improve oversight of information security at the bureaus, Treasury launched or expanded several initiatives during fiscal year 2003 that were designed to promote the implementation of key elements of a departmentwide information security program.

- *Appointment of chief information officer.* In March 2003, Treasury appointed a new departmental CIO. FISMA provides that the authority to ensure compliance with the requirements imposed on the agency under the act be delegated to the agency CIO. The CIO's responsibilities include developing and maintaining a departmentwide information security program and security policies and providing oversight, strategic management, and policy direction on all information security programs within Treasury.
- *Development of information security governance model.* The Treasury CIO proposed a governance model for information security during fiscal year 2003. Elements of the model include integrating security programs both functionally with capital planning and organizationally across bureaus; increasing CIO oversight; increasing bureau self-assessments; creating and distributing comprehensive security policies, standards, and procedures; establishing a security policy forum; and linking the information technology governance process to the enterprise architecture and capital investment and planning process.
- *Updated departmental information security policies and procedures.* During fiscal year 2003, Treasury undertook a major revision of its outdated and incomplete information security policies. In August 2003, Treasury published a comprehensive, up-to-date body of information security policies and procedures—the *Treasury Information Systems Security Program*—consisting of the *Treasury Information Technology Security Program Policy* (Volume 1) and the *Treasury Information Technology Security Program Handbook* (Volume 2). The documents replaced Treasury Directive 71-10 and formally establish a uniform baseline for the department's information security requirements. They are based on requirements levied by the FISMA, NIST, and OMB and are to serve as a framework for the bureaus as they develop their specific policies and operating directives.
- *Expanded program and system review.* Treasury expanded its review of the bureaus' information security programs and systems during fiscal year

---

2003. According to Treasury's fiscal year 2003 FISMA report, one departmental initiative to create and maintain a system inventory revealed an additional 270 systems in fiscal year 2003. The department also conducted reviews of each bureau's information security program and performed 21 system certification and accreditation package reviews. In addition, Treasury conducted vulnerability scans on networks and performed system penetration tests as part of its program and system reviews.

- *Analysis of bureaus' plans of action and milestones.* Treasury continued tracking and analyzing the plan of action and milestones (POA&M) reported by the bureaus on a quarterly basis. This plan is a tool that details the tasks that need to be accomplished and the resources required, milestones, and scheduled completion dates for accomplishing the tasks. The purpose of a POA&M is to help agencies identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems. OMB requires agencies to (1) develop a separate POA&M for every program and system for which weaknesses were identified and (2) report quarterly on progress implementing the plans. Accordingly, Treasury requires its bureaus to maintain POA&Ms on all information security weaknesses and provide quarterly updates to the Treasury CIO's office. Treasury monitors bureau progress in correcting weaknesses by using the plans as a performance tracking mechanism. According to the Treasury CIO, Treasury analyzes the updated plans for quality and completeness and evaluates progress and other significant trends that may influence the resolution of security-related weaknesses.
- *Educational outreach programs.* According to Treasury's FISMA report for fiscal year 2003, Treasury's oversight and compliance program also developed and maintained a series of outreach programs that are designed to educate Treasury employees about elements of information security compliance and to stimulate dialogue among security practitioners and stakeholders across the department.
- *Increased funding for information technology security.* According to Treasury's FISMA report for fiscal year 2003, the department more than doubled its total information security spending, from \$85 million in fiscal year 2002 to \$174 million in fiscal year 2003.

## Despite Initiatives, Information Security Challenges Remain

Although Treasury has significantly increased funding for information security and has begun to make progress implementing key elements of its information security program, it remains challenged to effectively and consistently implement security controls and procedures across the department. As illustrated in figure 6, an analysis of security metric data in

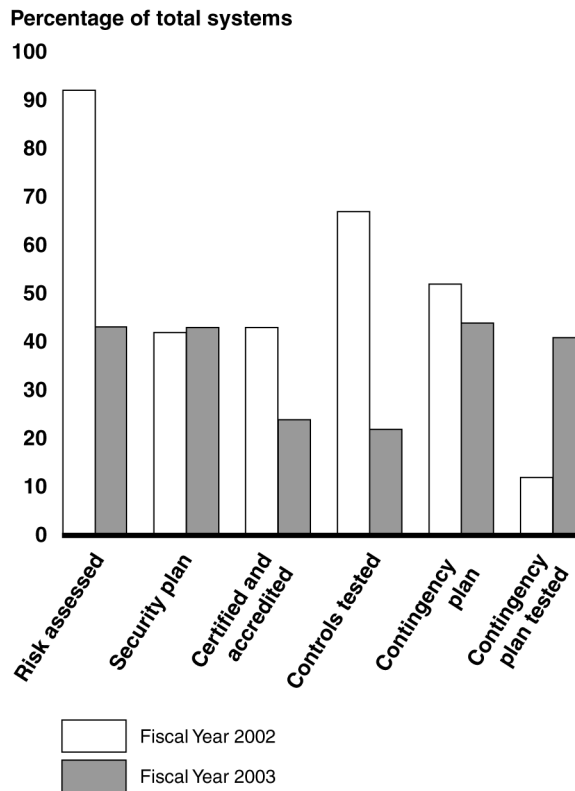
---

Treasury's fiscal year 2002 GISRA report and its fiscal year 2003 FISMA report<sup>20</sup> shows that

- the majority of Treasury systems do not meet key information security requirements, and
- Treasury's reported performance in meeting certain of these requirements has decreased.

---

**Figure 6: Percentage of Treasury Systems Meeting Certain Information Security Requirements**



Source: GAO.

Note: This chart reflects data for the 11 Treasury bureaus that reported on these security requirements for both years.

---

<sup>20</sup>IRS management indicated that controls in additional systems were tested subsequent to the effective date of Treasury's FISMA report.

---

Treasury reported that it did not implement any of these six required information security activities on a majority of its systems for fiscal year 2003. For example, Treasury established a specific goal that 80 percent of all information systems be certified and accredited by the end of fiscal year 2003. However, as of August 15, 2003—the date of data contained in its FISMA report for fiscal year 2003—Treasury had certified and accredited only about 24 percent of its 708 systems. According to Treasury’s CIO, this was due to (1) the discovery of 276 additional systems at the IRS as a result of an effort to compile an accurate inventory and (2) a new reporting requirement that stipulated that systems with an interim authority to operate not be counted in fiscal year 2003 as an accredited system. In fiscal year 2002, such systems were counted as accredited for reporting purposes.

In addition, implementation of certain information security requirements has decreased from fiscal year 2002. For the 11 bureaus that reported performance measures for both years, the percentage of Treasury systems implementing five of the six requirements decreased in fiscal year 2003, while it increased for one. For example, Treasury-reported data for fiscal year 2002 shows that 93 percent of the systems at those bureaus were assessed for risk and assigned a level of risk, while for fiscal year 2003 only 42 percent were.

Treasury’s overall performance demonstrates that it continues to face challenges implementing and monitoring information security throughout the department. The following factors contribute to the challenges confronting Treasury as it endeavors to improve the security of its information systems and data:

- *Treasury reorganization.* Throughout fiscal year 2003, Treasury underwent a major reorganization. The reorganization resulted in the reassignment of three bureaus to the Department of Homeland Security, the creation of a new entity within Treasury, and the transfer of about 50 percent of Treasury’s information technology security staff to the Department of Homeland Security. The reduction in staff resulting from the reorganization, combined with the reported increase in the total number of departmental systems, could hinder the department’s ability to provide effective oversight and direction over the bureaus’ information security programs.
- *Senior information security officer has not been designated.* FISMA requires that a senior agency information security officer be designated to carry out the information security duties and responsibilities of the CIO

---

under the act. This senior level official is to (1) have information security as his or her primary duty; (2) head an office with the mission and resources necessary to assist in ensuring compliance with the act; and (3) possess the professional qualifications, including training and experience, required to administer the functions described in the act. The official would oversee the development and implementation of departmental information policies, procedures, and control techniques and coordinate departmentwide security-related activities to ensure that weaknesses identified in one bureau's systems do not place the entire department's information assets at undue risk. However, Treasury has not designated a senior agency information security officer to develop, maintain, and oversee the department's security program. The lack of a senior information security officer with the stature and experience as well as the responsibility and authority for directing and overseeing the implementation of the departmentwide program could impair departmental control or influence in information security program decisions made by the bureaus.

- *Reliability and completeness of performance information.* Although FISMA reporting provided performance information on key security areas, it is important for agencies to ensure that they have the appropriate management structures and processes in place to strategically manage information security, as well as to ensure the reliability of performance information. For example, disciplined processes can routinely provide the agency with timely, accurate, and useful information for day-to-day management of information security. Treasury has established a process for receiving quarterly updates on the bureaus' plans of actions and milestones and issuing an annual data call to the bureaus for performance information on key information security requirements used in FISMA reports. However, the Treasury reports reveal issues with the reliability and completeness of bureau-reported information. For example, in Treasury's fiscal year 2002 FISMA report, there were significant differences between what Treasury and the OIG reported for the percentage of systems that met certain information security requirements.

In addition, the Treasury Inspector General for Tax Administration (TIGTA) states in the fiscal year 2003 FISMA report that IRS's POA&Ms do not report on the status of system-specific vulnerabilities and are not specific enough to ensure accountability and timely remediation of the vulnerabilities. TIGTA also states that since IRS's POA&Ms are not reported by system, justifications for information security funding found in its business cases cannot be tied to or linked with weaknesses reported in the POA&M. With the need for effective oversight to ensure compliance with the departmentwide information security program and the need to

---

comply with a new requirement by OMB for quarterly reporting of agency progress against certain information security performance measures, disciplined processes that can routinely provide Treasury with timely, accurate, and useful information for day-to-day management of information security will become more important for the department.

---

## Conclusions

Weaknesses in information security controls at Treasury bureaus have placed its financial and information management systems at risk and could hinder its ability to effectively and efficiently accomplish its mission. Although Treasury has taken the initial steps necessary to implement a departmentwide information security program, key elements of such a program—those needed to help mitigate Treasury’s long-standing information security weaknesses—have not been fully implemented. Implementing an effective information security program could help ensure that known weaknesses affecting Treasury’s computing resources are promptly mitigated and that general controls effectively protect its computing environments. Until Treasury oversees the implementation of a departmentwide security program, limited assurance exists that it and its bureaus will be able to resolve known information security weaknesses and adequately safeguard their information resources.

---

## Recommendations for Executive Action

To improve oversight and compliance with Treasury’s information security program, we recommend that the Secretary of the Treasury direct the chief information officer to do the following:

- Assess the staffing and resource requirements for performing the department’s oversight and compliance efforts to ensure that departmental information security policies are effectively and consistently implemented throughout the organization.
- Designate a senior agency information security officer.
- Examine existing reporting processes and implement procedures to enhance the reliability and completeness of the bureau-provided information required for day-to-day management of information security.

---

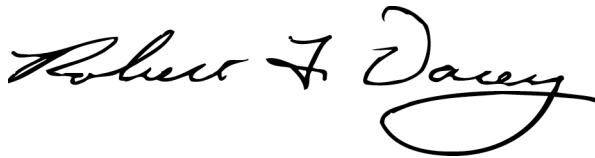
## Agency Comments

In providing written comments on a draft of this report (which are reprinted as appendix 1), the Treasury CIO responded on behalf of the department and concurred with our assessment and recommendations. In addition, the CIO underscored his commitment to implementing a new

---

security governance model that not only aligns with Treasury's information technology governance model but also aligns with security policies and security operations. The Treasury CIO also provided technical comments that have been incorporated into the report as appropriate.

If you have any questions or need further information, please contact Gregory C. Wilshusen, Assistant Director, at (202) 512-6244, or me at (202) 512-3317. We can also be reached by e-mail at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) and [dacey@gao.gov](mailto:dacey@gao.gov), respectively. Kenneth A. Johnson and Ronald E. Parker made key contributions to this report.

A handwritten signature in black ink that reads "Robert F. Dacey". The signature is written in a cursive style with a large, looping flourish at the end of the name.

Robert F. Dacey  
Director, Information Security Issues

# Appendix I: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

November 7, 2003

Mr. Robert F. Dacey  
Director  
Information Security Issues  
General Accounting Office  
441 G Street, NW, Rm 5T37  
Washington, DC 20548

Dear Bob:

Thank you for the opportunity to review and to comment on your draft report entitled "Information Security: Improvements Needed in Treasury's Security Management Program" (Report #GAO-04-77). I concur with the GAO's assessment and its recommendation; attached please find comments that may provide additional clarification.

Please note the following on C&A: the Department has stressed to the bureaus they need to identify and to report an accurate inventory of systems. In FY 2003, the Department obtained from each bureau a complete register of general support systems and major applications. Through diligent work conducted by each bureau and the Department IT Security Program, Treasury now has a truer – but higher – number of systems based on FISMA requirements. While we endorse moving the "bar" to its correct position means Treasury's percentage of systems C&A'd decreases, the benefits to our security objectives should be emphasized.

Finally, I want to underscore my commitment to implementing a new security governance model that not only aligns with our overall IT governance model (affecting how we allocate IT funds across Treasury) but also aligns security policies and security operations – a critical issue that, once properly addressed, will accelerate progress. Ensuring that the Department is not only promulgating policies but also enforcing policies across the bureaus with sufficient resources is essential to securing the Treasury Department.

If you have any questions regarding our comments, please contact me at 202 622-1200 or via email at [drew.ladner@do.treas.gov](mailto:drew.ladner@do.treas.gov).

Thank you for your assistance.

Sincerely,

A handwritten signature in cursive script that reads "Drew Ladner".

Drew Ladner  
Chief Information Officer

Attachment



---

# Related GAO Products

---

*Information Security: Computer Controls Over Key Treasury Internet Payment System.* [GAO-03-837](#). Washington, D.C.: July 30, 2003.

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

*Bureau of the Public Debt: Areas for Improvement in Computer Controls.* [GAO-03-524R](#). Washington, D.C.: May 1, 2003.

*Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures.* [GAO-03-564T](#). Washington, D.C.: Apr. 8, 2003.

*High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures.* [GAO-03-121](#). Washington, D.C.: January 2003.

*Major Management Challenges and Program Risks: Department of the Treasury.* [GAO-03-109](#). Washington, D.C.: January 2003.

*Computer Security: Progress Made, But Critical Federal Operations and Assets Remain at Risk.* Washington, D.C.: [GAO-03-303T](#). Nov. 19, 2002.

*Financial Audit: IRS's Fiscal Years 2002 and 2001 Financial Statements.* [GAO-03-243](#). Washington, D.C.: Nov. 15, 2002.

*Financial Audit: Bureau of the Public Debt's Fiscal Years 2002 and 2001 Schedules of Federal Debt.* [GAO-03-199](#). Washington, D.C.: Nov. 1, 2002.

*Bureau of the Public Debt: Areas for Improvement in Computer Controls.* [GAO-02-1082R](#). Washington, D.C.: Sept. 18, 2002.

*Information Security: Comments on the Proposed Federal Information Security Management Act of 2002.* [GAO-02-677T](#). Washington, D.C.: May 2, 2002.

*Information Security: Additional Actions Needed to Implement Reform Legislation.* [GAO-02-470T](#). Washington, D.C.: Mar. 6, 2002.

*Financial Audit: IRS's Fiscal Years 2001 and 2000 Financial Statements.* [GAO-02-414](#). Washington, D.C.: Feb. 27, 2002.

*Financial Audit: Bureau of the Public Debt's Fiscal Years 2001 and 2000 Schedules of Federal Debt.* [GAO-02-354](#). Washington, D.C.: Feb. 15, 2002.

*Financial Management Service: Significant Weaknesses in Computer Controls Continue.* [GAO-02-317](#). Washington, D.C.: Jan. 31, 2002.

*Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets.* [GAO-02-231T](#). Washington, D.C.: Nov. 9, 2001.

*Bureau of the Public Debt: Areas for Improvement in Computer Controls.* [GAO-01-1131R](#). Washington, D.C.: Sept. 13, 2001.

*Management Letter: Improvements Needed in IRS's Accounting Procedures and Internal Controls.* [GAO-01-880R](#). Washington, D.C.: July 30, 2001.

*Computer Security: Weaknesses Continue to Place Critical Federal Operations and Assets at Risk.* [GAO-01-600T](#). Washington, D.C.: Apr. 5, 2001.

*Internal Revenue Service: Progress Continues But Serious Management Challenges Remain.* [GAO-01-562T](#). Washington, D.C.: Apr. 2, 2001.

*Financial Audit: Bureau of the Public Debt's Fiscal Years 2000 and 1999 Schedule of Federal Debt.* [GAO-01-389](#). Washington, D.C.: Mar. 1, 2001.

*Financial Audit: IRS' Fiscal Year 2000 Financial Statements.* [GAO-01-394](#). Washington, D.C.: Mar. 1, 2001.

*Information Security: IRS Electronic Filing System.* [GAO-01-306](#). Washington, D.C.: Feb. 16, 2001.

*Computer Security: Critical Federal Operations and Assets Remain at Risk.* [GAO/AIMD-00-314](#). Washington, D.C.: Sept. 11, 2000.

*Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies.* [GAO/AIMD-00-295](#). Washington, D.C.: Sept. 6, 2000.

*Information Security: Software Change Controls at the Department of Treasury.* [GAO/AIMD-00-200R](#). Washington, D.C.: June 30, 2000.

*Management Letter: Suggested Improvements in IRS's Accounting Procedures and Internal Controls.* [AIMD-00-162R](#). Washington, D.C.: June 14, 2000.

*Financial Audit: IRS's Fiscal Year 1999 Financial Statements.* [AIMD-00-76](#). Washington, D.C.: Feb. 29, 2000.

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

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

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

*Financial Audit: Examination of IRS's Fiscal Year 1992 Financial Statements.* [GAO/AIMD-93-2](#). Washington, D.C.: June 30, 1993.

---

## GAO's Mission

The General Accounting 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 the Internet. GAO's Web site ([www.gao.gov](http://www.gao.gov)) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

---

## 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. General Accounting 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](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

---

## Public Affairs

Jeff Nelligan, Managing Director, [NelliganJ@gao.gov](mailto:NelliganJ@gao.gov) (202) 512-4800  
U.S. General Accounting Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548