



# 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).

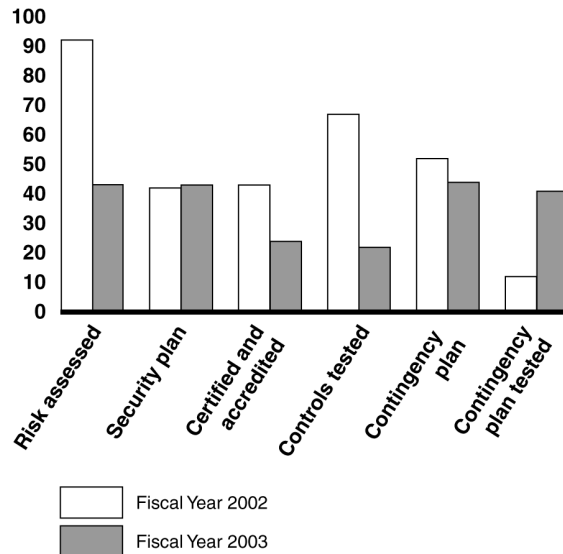
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or [dacey@gao.gov](mailto:dacey@gao.gov).

### 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.