

**STATEMENT OF THE HONORABLE JEFFREY RUSH, JR.**  
**INSPECTOR GENERAL**  
**DEPARTMENT OF THE TREASURY**  
**BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM**  
**SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,**  
**INTERGOVERNMENTAL RELATIONS AND THE CENSUS**  
**MARCH 10, 2004**

Mr. Chairman, Ranking Member Clay, Members of the Subcommittee, thank you for the opportunity to testify in this hearing on "Information Security in the Federal Government: One Year into the Federal Information Security Management Act." In your letter of February 26, 2004, you asked me to address three points in my statement: (1) a summary of the state of information security at Treasury, (2) the methodology used to audit Treasury and the resources available to my office, and (3) the circumstances that led to the delay in reporting our results under the Federal Information Security Management Act (FISMA).

First, although we have been reporting on serious information security weaknesses since 1998, I will limit my testimony to work done in the past 3 years. This is the third year we have assessed the information security programs and practices in Treasury. Our reporting for Fiscal Years (FY) 2001 and 2002 was under the Government Information Security Reform Act (GISRA). All three assessments, as well as management's own assessments, have identified serious deficiencies in information security throughout the Department. We issued our most recent evaluation report pursuant to FISMA on December 15, 2003, and a separate, classified FISMA report on Treasury's national security systems on December 24, 2003. These deficiencies include:

- Most systems have not been certified and accredited.
- Treasury has been unable to provide an accurate inventory year-to-year of systems to be certified and accredited.
- Treasury's plans of action and milestones for fixing serious security weaknesses were not always complete or consistently reported on.
- Treasury does not have a fully functioning computer security incident response capability. In addition, the requirements for reporting incidents were not being applied consistently among Treasury offices and bureaus.
- Treasury did not use the National Institute of Standards and Technology's (NIST) guidance for all of its program and systems reviews. Other methodologies that Treasury used were not sufficient to substitute for the NIST requirements.

- Interdependencies and interrelationships of mission critical operations and assets were not fully identified.
- Treasury has not provided sufficient information technology (IT) security training to the majority of its employees.

At least some aspect of these weaknesses has been reported in each of the last 3 years. While some progress has been made, these weaknesses have largely gone uncorrected. In fact, in the critical area of certification and accreditation, Treasury's performance has declined.

With respect to certification and accreditation, for FY 2001, 18 percent of Treasury systems were certified and accredited; for FY 2002, 32 percent of Treasury systems were certified and accredited; and for FY 2003, 23 percent of Treasury systems were certified and accredited, Department-wide. It should be noted that the FY 2003 decline was significantly impacted by the number systems operated by the Internal Revenue Service (IRS) that were not certified and accredited. Not including the IRS systems, 69 percent were certified and accredited. Nevertheless, this matter has been further complicated by the Department's inability to provide an accurate inventory of its systems to be certified and accredited on a year-to-year basis. For example, in FY 2002 Treasury identified 626 systems requiring certification and accreditation; in FY 2003, Treasury identified 708 systems requiring certification and accreditation.

To its credit, Treasury management declared the lack of substantial compliance with information security requirements as a material weakness under the Federal Manager's Financial Integrity Act based on our FY 2002 evaluation. It continued to report this deficiency as a material weakness for FY 2003.

Second, in conducting our FY 2003 evaluation of Treasury's information security program and practices, we followed the guidance issued by the Office of Management and Budget (OMB) on August 6, 2003. For your reference, I have attached a copy of the guidance to this statement. The guidance prescribed a set of questions to be answered by both agency management and by the Offices of Inspector General (OIG). In this regard, OIGs were to evaluate a representative sample of all types of agency systems. FISMA also supports the OIGs' use of results of other IT-related reviews performed during the reporting period. One area that was emphasized this year was the OIGs' assessment, against specific criteria, of whether the agency developed, implemented, and was managing an agency-wide plan of action and milestones process. The plans of action and milestones process is key to effective remediation of IT security weaknesses and instrumental for an agency to get to "green" under the Expanding E-Government Scorecard of the President's Management Agenda.

For FY 2003, we participated with the Department's Office of Chief Information Officer and the Treasury Inspector General for Tax Administration in a joint data call to Treasury offices and bureaus. We performed limited verification of the data received. We also considered the results of our work performed during the year that directly impacted information security. For example, we observed a disaster recovery test for the Treasury Communications System and audited the Department's implementation of its critical infrastructure protection program. We also considered IT security audit work that was performed in connection with the audits of the Department and bureau FY 2003 financial statements.

Finally, as background to the reason for our delayed FISMA reporting, during March 2003, we divested approximately 70 percent of our staff to the Department of Homeland Security Office of Inspector General pursuant to the Homeland Security Act of 2002. Our audit staff was reduced from 165 to 62 during the last six months of the fiscal year. Our annual audit plan had to be completely revised. This divestiture and subsequent attrition reduced our IT audit group from 14 to 5.

We had planned to complete our FISMA review by the OMB-prescribed deadline of September 22, 2003. However, with our much reduced staffing, we determined that we could not complete FISMA on schedule and sustain an accelerated audit of the Department's FY 2003 financial statements. In consultation with the Department and OMB, priority was given to our audit of the Department's FY 2003 financial statements, and we committed to issue our FISMA report 1 month later. Accordingly, the financial statement audit was completed on November 14, 2003, and we issued our FISMA report on December 15, 2003.

Considering our current staffing levels and looking forward, we have not been able, and do not anticipate being able to hire additional IT audit staff in the near future that would enable us to meet the anticipated FY 2004 FISMA reporting deadline. Thus, we plan to contract out the independent FY 2004 FISMA evaluation for non-national security systems. We will perform the FY 2004 FISMA evaluation for Treasury's national security systems with our staff. We also plan to perform audit work in certain key areas of vulnerability identified by our previous FISMA work. For example, we plan to audit Treasury's computer security incident response capability and conduct vulnerability scans of computer networks at selected bureaus. The results from these audit efforts, as well as any information security findings identified from our financial statement audits, will be integrated into our FISMA reporting for FY 2004.

This concludes my testimony. I would be pleased to answer any questions that the Committee may have. Thank you.