OIG

Report Synopsis

The Department of the Treasury
Office of Inspector General

Report Title

INFORMATION TECHNOLOGY: Evaluation of Treasury's FISMA Implementation For Fiscal Year 2003 (OIG-CA-04-001; issued December 15, 2003) (Limited Official Use)

This report is not available on the Department of the Treasury Office of Inspector General (OIG) website. For further information, please contact the OIG Office of Counsel at (202) 927-0650 or send an email to webmaster@oig.treas.gov.

Synopsis

As required by the Federal Information Security Management Act of 2002 (FISMA), we performed an independent evaluation of the information security program and practices of the Department of the Treasury (Treasury) for Fiscal Year (FY) 2003 as they relate to the following 12 Treasury bureaus and offices: Alcohol and Tobacco Tax and Trade Bureau, Bureau of Engraving and Printing, Bureau of the Public Debt, Community Development Financial Institutions Fund, Departmental Offices, Financial Crimes Enforcement Network, Financial Management Service, Office of the Comptroller of the Currency, Office of Inspector General; Office of Thrift Supervision, U.S. Mint, and Treasury Inspector General for Tax Administration (TIGTA). TIGTA performed the FISMA evaluation for the Internal Revenue Service (IRS). We performed our work in Washington, DC, from May to December 2003. Our evaluation was conducted in accordance with the Office of Management and Budget's (OMB) guidance, issued August 6, 2003, and with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*, issued March 1993.

Treasury's information security program and practices, as they relate to non-national security systems, need to be improved. Our evaluation determined that, despite some progress, many of the weaknesses observed in our FY 2002 Government Information Security Reform Act evaluation continued to exist. For example, (1) the percentage of systems, including those of the IRS, that were certified and accredited for secure operation is 23 percent, which is significantly lower than Treasury's goal of 70 percent and less than the percentage reported in FY 2002; (2) bureau Plans of Action and Milestones to address security weaknesses were not always complete; (3) Treasury's computer security incident response capability was not fully functional; and (4) IT security training was insufficient--only 31 percent of Treasury employees received IT security training in FY 2003.

We believe that the weaknesses in the information security program and practices constitute, in the aggregate, a material weakness in Treasury's management controls as defined in OMB Circular A-123, *Management Accountability and Control*. We noted that management reported lack of substantial compliance with FISMA as a material weakness under the Treasury's Federal Manager's Financial Integrity Act process. We recommended

that the Treasury Chief Information Officer provide effective oversight to ensure that Treasury implements the corrective actions necessary to achieve compliance with FISMA.