Office of Inspector General

Testimony of Bruce N. Crandlemire, Assistant Inspector General for Audit
U.S. Agency for International Development

Submitted to the Committee on Government Reform
U.S. House of Representatives

No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade

April 7, 2005

Mr. Chairman and other Committee members:

Thank you for the opportunity to provide testimony on the U.S. Agency for International Development's (USAID) compliance with the Federal Information Security Management Act of 2002 (FISMA). As you have requested, my testimony will focus on the state of information security at USAID and the methodology we used to perform our fiscal year 2004 FISMA audit. In addition, I will discuss the need for a standardized FISMA auditing framework and what additional guidance is needed for agencies to fully comply with FISMA.

STATE OF INFORMATION SECURITY AT USAID

USAID has made many positive strides over the last few years in addressing information security weaknesses. In particular, USAID has made several improvements in response to audits performed by my office and, in turn, substantially improved its computer security program. Although there have been improvements in information security, USAID still faces several important challenges to refine its information security environment.

In 1997, the Office of Inspector General (OIG) identified information security as a material weakness at USAID. USAID information technology officials agreed with our conclusion and included it in USAID's annual report as required by the Federal Managers' Financial Integrity Act. At that time, USAID did not have (1) an organizational structure that clearly delegated information security responsibilities, (2) policies that provided for an effective information security program, and (3) key management processes to ensure that security requirements were met. This material weakness remained outstanding for seven years until fiscal year 2004 when USAID concluded, and we agreed, that information security was no longer a material weakness for the agency. As a result, information security at USAID today is a different story than it was in 1997.

In recent years two of the most significant changes are the appointment of an Information Systems Security Officer and the implementation of a centralized information security framework. Under this framework, USAID (1) centrally manages its Windows 2000 domain servers, firewall, and virus scan software for most of USAID's networks; (2) instituted a process to assess information systems security for the purchase of capital assets; and (3) is continually updating its information security policies and procedures.

The Agency has also initiated several significant technological changes to improve its computer security. For example, USAID has done the following:

- Deployed Windows 2000, which has allowed the Agency to lock down configured security settings and incorporated many security improvements in comparison to Windows 98.
- Installed operating network sensors to help detect unauthorized attempts to access USAID's network.
- Run daily scans of its worldwide network to proactively identify potential vulnerabilities in its network. Based on the results of the scans, the Agency's Information Systems Security Officer has been issuing monthly grades, similar to the grades listed in FISMA's annual report card, to its overseas missions.
- Implemented "Tips of the Day", which is an automated information security awareness program that provides security reminders to all system network users each day as a prerequisite to network login.

Through these system-wide information technology policy and network changes, information security and information security awareness at USAID's locations around the world have been significantly increased.

Although USAID has made substantial progress in improving information security, weaknesses still remain. As reported in our fiscal year 2004 FISMA audit report, the Agency had not developed disaster recovery plans for three major systems and had not tested disaster recovery plans for two other major systems. This represents a significant vulnerability because USAID is not fully prepared for an emergency event. To a lesser degree USAID also needs to:

- Improve its information resource management processes, such as the full implementation of information technology program management and oversight practices.
- Improve several management controls, such as outdated virus definitions, the installation of unauthorized software on employee computers, and the inconsistent updating of security software patches to individual computers.
- Test the effectiveness of USAID's security awareness program.

METHODOLOGY AND RESOURCES USED FOR THE FISMA AUDIT

The OIG approach to assessing USAID information security under FISMA was to conduct an audit as opposed to an evaluation. Our audit addressed all the reporting requirements of the Office of Management and Budget's (OMB) reporting template and the FISMA requirements.

In fiscal year 2004, the audit fieldwork was conducted from August 19 through October 6, 2004, and involved 610 staff hours. In addition, we relied on other audits (e.g., general control and Phoenix financial system audits) to support and compliment our FISMA fieldwork. For example, the fiscal year 2004 general control audit, which involved reviewing security controls of USAID's financial systems (in most cases, the same systems reviewed for FISMA), involved 2,843 staff hours. This audit included reviewing USAID's systems in Washington and at 12 overseas missions.

Our goal was to not only validate USAID's responses to OMB's questionnaire, but to also verify actions that USAID had taken to comply with FISMA. By verifying USAID's answers to OMB's reporting template, we could conclude where the Agency stood in terms of its compliance with FISMA.

Systems covered by the audit included the Washington financial system, the Missions financial system, the contract and procurement system, USAID's network system, and the Office of Foreign Disaster Assistance's network system. In addition to covering systems operated by USAID, we also determined whether the Agency had obtained security assurances for three systems operated by third parties: the payroll system operated by the National Finance Center, the letter of credit system operated by the Department of Health and Human Services, and the loan management system operated by Riggs Bank.

To perform the audit, we interviewed USAID officials to discuss their answers to OMB's questionnaire and then requested support for their answers. Types of source documents that we reviewed included: certification and accreditations for Agency and third party-operated systems, reviews of contractor facilities, reports to the United States Computer Emergency Team (USCERT) and internally generated security incident reports.

For each of USAID's 49 answers to the questionnaire, we determined whether the Agency's answer was supported by the source document provided and testimonial evidence. If an Agency answer was not supported, we brought that issue to management's attention. In the end, we agreed with 48 of the Agency's 49 answers. The one answer that we did not agree with involved whether the OIG had been included in the development and verification of the Agency's IT systems inventory.

NEED FOR AN INSPECTOR GENERAL AUDITING FRAMEWORK FOR INFORMATION SECURITY

In my opinion, since OIG input into the FISMA process is used to grade security among civilian agencies, there is an implicit assumption that there must be a defined common set of attributes to facilitate meaningful comparisons of independent evaluations/audits performed by each IG. Further, the establishment of these attributes or a common IG security auditing framework should be developed on a collaborative basis among the IG community (such as through the President's Council on Integrity and Efficiency forum), OMB and Government Accountability Office. Additionally, the framework should address the resources needed to carry-out the development and implementation of the framework along with Congressional support for such an initiative.

ADDITIONAL GUIDANCE, PROCEDURES, OR RESOURCES NEEDED TO IMPROVE COMPLIANCE WITH FISMA

In regards to OMB's FISMA questionnaire, there are two suggestions that we would like to make:

2. Agencies and IGs need more time to respond to the annual OMB FISMA questionnaire. Since 2002, time to respond to the questionnaire has decreased each year as follows:
   - In 2002, under GISR, OMB issued its guidance (M-02-09) on July 2 and expected responses by September 16—76 days.
   - In 2003, OMB issued its FISMA guidance (M-03-19) on August 6 and expected responses by September 22—47 days.
   - In 2004, OMB issued its FISMA guidance (M-04-25) on August 23 and expected responses by October 6—44 days.

3. The Office of Inspector General is responsible for conducting the FISMA audits at three micro-agencies: the Millennium Challenge Corporation, the African Development Foundation, and the Inter-American Foundation. OMB has established an abridged FISMA reporting format for micro-agencies (agencies with less than 100 Federal employees). While helpful, small agencies with more than 100 Federal employees struggle with responding to full FISMA requirements. This was noted by OMB in early 2005 and we understand that OMB is considering standardizing cyber security business processes of agencies to save money, increase security, and help those agencies with small IT budgets. In the future, OMB might want to consider not just employee numbers, but also IT budgets in its definition of micro-agencies (e.g. agencies with less than 250 employees and IT budgets less than a certain dollar threshold).

SUMMARY

In summary, USAID has made positive strides in addressing information security weaknesses, and our audits have confirmed the improvements. Although there is still work to be done, USAID is on the right path.

Again, thank you for the opportunity to testify today. I will be happy to respond to any questions you may have.