TESTIMONY OF PHILIP HENEGHAN,
CHIEF INFORMATION SECURITY OFFICER,
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID)
BEFORE THE SENATE HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS COMMITTEE'S SUBCOMMITTEE ON
FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL
SECURITY
March 12, 2008

Chairman Carper and Members of the Subcommittee, thank you for the opportunity to testify on USAID's information security program and our implementation of the Federal Information Security Management Act (FISMA). I would like to begin by describing USAID's mission and the unique information security challenges created by this mission. Then I would like to report how our risk-based information security program successfully implements FISMA. I will also discuss how we use innovative techniques and technologies to measure and manage the risk to our information and systems.

USAID's Unique Mission Drives Our Information Systems Security Program

USAID was created as an independent agency in 1961 by the Foreign Assistance Act. Since that time, USAID has been the principal U.S. agency responsible for promoting international development by supporting: economic growth; agriculture and trade; global health; democracy; conflict prevention; and humanitarian assistance.

USAID's mission requires us to work in developing countries and work in close partnership with many different Private Voluntary Organizations (PVOs), indigenous organizations, universities, American businesses, international agencies, other governments, and Non-Governmental Organizations (NGOs). The information technology and telecommunications infrastructure in most of the countries where USAID does its work are not as robust or dependable as the infrastructure here in the United States. Yet, work with our development partners compels us to work with and be part of this developing infrastructure. Some of the information technology infrastructure issues we face in these developing countries include: unreliable power grids, non-existent fiber optic connections, expensive bandwidth, and high latency. USAID's Office of Foreign Disaster Assistance (OFDA) also responds to complex emergencies and disasters, such as the recent events in Bangladesh, Ethiopia, Kenya, and Sudan. This requires USAID to support different risk models for network operations and creates many challenges for implementing a worldwide information security program.

Most of the USAID information technology activity occurs on AIDNET, which is a single worldwide network made up of 9,000 interconnected workstations and 8,000 other network infrastructure devices. Approximately 3,000 of the workstations are here in Washington with the remaining 6,000 workstations located in more than 70 countries around the world.

AIDNET is a very active and dynamic network. We receive approximately 23 million emails a month and block the 20 million of those emails that contain viruses or are spam. USAID's firewalls are located at

more than 50 sites around the world but are managed and controlled centrally in Washington, D.C. These firewalls handle more than 11 million access attempts each day and deny 4 million of those attempts. AIDNET is constantly changing. We recently established a new site in Banda Aceh, Indonesia, moved 11 other mission locations, will soon set up another site in Pakistan, and are regularly changing the communication channels for all sites back to Washington. We need to understand, manage, and monitor these changes to our network so that we can identify any change in the risk we have accepted. Our risk-based program requires us to be continually aware of the changing structure of our network and our focus on measurement ensures we can.

Risk-Based Program to Protect the Confidentiality, Integrity, and Availability of USAID Information Resources

Our information security program uses a risk-based management approach to effectively implement appropriate operational, technical, and managerial controls. To support this approach, we lean heavily on technologies that automate the collection and reporting of security information and metrics. For instance, through technology we have automated our security awareness training with a USAID-developed program we call Tip of the Day. The Tip of the Day program provides a brief security lesson and prompts the user to answer a question about that lesson before the user logs into one of our networks. We have partnered with our colleagues at the Department of State to make this and other security training available to others in the Federal Government and are

proud that this innovative program has been selected as a component of the Information System Security Line of Business (ISSLOB).

For the past four years, we have used a robust vulnerability management program that continually scans the 17,000 systems on our network to measure their security posture. This program ensures that each system is evaluated about 10 times a month. In 2006, we moved to the next level and implemented a risk modeling program that couples this vulnerability data with our network access rules (router configurations, firewall rules, and access control lists) to model our network and report any changes impacting the risk we've accepted. This virtual modeling occurs daily and provides a true picture of our exposure to identified threats; in addition, it provides a historical daily snapshot of our dynamic network to help us analyze alerts sent to us by US-CERT. We have also centralized the management of our entire security infrastructure in Washington to collect and analyze security events and network metrics from hundreds of remote security systems around the world.

We augment our situational awareness intelligence with DHS-provided technology. As one of the six Einstein pilot agencies since 2006, we have exchanged situational awareness information that has benefited our agency and the wider federal community. This was the beginning of a strong partnership with US-CERT, including the Government Forum for Incident Responders and Security Teams (GFIRST) program. GFIRST has provided a secure communications channel to the federal community for us, and we are an active participant, recently hosting the monthly GFIRST meeting in February.

Of course, these metrics and technologies would be useless if we did not engage the executives, managers, and systems administrators responsible for the individual systems and networks. This is an area where I believe we have implemented one of the foundational tenets of FISMA. For each system and network we have identified the executive who "owns" the system, and as a result has responsibility for and is in the best position to make risk-based decisions regarding the system's security controls. Our experience has shown that if provided the right metrics, system owners apply the necessary resources to ensure that their systems remain at an appropriately secure level. Our responsibility is to provide those system owners with the metrics they need to make information security decisions based on risk.

For example, when we started inventorying external websites we identified 160 USAID-branded sites. We evaluated these sites not only for compliance with OMB mandates but also scanned them for web-based vulnerabilities. As a result of these risk assessments, USAID executives decided to shut down more than 30 vulnerable sites.

Towards our goal of keeping executives informed of their security posture, we produce monthly security reports on our systems and networks and provide them to over 100 executives throughout the agency. We deliver these metrics in a report card format so that our leadership team can readily understand and act upon the information (we provide more detailed technical information to the managers and system administrators). We have found that because our reports are accurate, consistently produced, and actionable, they are extremely effective and as a result USAID maintains a high level of security on all our systems.

Conclusion

Our experience with FISMA has generally been very positive. We have adopted the risk management principles of the law, including the regulatory guidance, and have built a robust information security program. Protecting systems and information, though, is an ongoing effort. The threat is constantly changing, and attack methodologies are continually evolving. Therefore, we are always concerned about the threats we do not yet know about. However, by understanding our environment and our baseline through the use of technology and process, we are in a better position to identify deviations that may indicate a new threat. We can then reduce our risk exposure by implementing new operational, technical, or managerial controls.

I appreciate the opportunity to appear before you today, and I look forward to any questions that you may have.