STATEMENT OF FRANK DEFFER

ASSISTANT INSPECTOR GENERAL, INFORMATION TECHOLOGY AUDITS

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

APRIL 7, 2005

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to be here today to discuss the status of the implementation of the Federal Information Security Management Act of 2002 (FISMA) within DHS. My testimony will address: the state of information security at DHS; the methodology and the resources used to evaluate the information security program at DHS; whether there is a need for a standard IG auditing framework for information security; and, whether additional or modified guidance is needed to improve compliance with FISMA. This testimony does not include the status of FISMA as it relates to intelligence systems. I would be happy to brief you on that issue at a later date.

DHS' Information Security Program

DHS developed an Information Security Program Strategic Plan, dated April 4, 2004 to provide the foundation for an agencywide, consolidated information security program. Under this plan, DHS' Chief Information Officer (CIO) and Chief Information Security Officer (CISO) identified eight security program areas:

- Management and Integration
- Security Policy
- Security Operations
- Security Architecture
- Continuity Planning
- Compliance and Oversight
- Training, Education, and Awareness
- National Security Systems and COMSEC

These distinct security program areas comprise the framework of the department's security program. The strategic plan describes the goals and objectives for establishing a dynamic information security organization over the next five years, too. We believe the program areas established in this plan represent key segments necessary for an effective information security program.

DHS' CIO, who has oversight responsibilities for the information security program, delegated the CISO, as required under FISMA, the authority to establish information security policies and procedures throughout the department. In June 2004, the CISO developed the Information Security Program Management Plan, which is the blueprint for managing DHS' information security program. At the same time, the CISO developed an Information Security Risk Management Plan, which documents DHS' plan to develop, implement, and institutionalize a risk management process in support of its information security program. Based on our review of these plans, DHS has established an adequate structure, blueprint, and process to implement and manage its information security program.

Additionally, the CISO developed and issued baseline IT security policies and procedures in a management directive; and a Sensitive Systems Policy Publication and its companion, the Sensitive Systems Handbook as well as a National Security Systems Policy Publication and its companion, the National Security Systems Handbook. While the guidance issued adequately documents key information security policies and procedures, there is additional guidance that needs to be either strengthened or developed to help DHS and its organizational components implement and maintain an effective information security program. Areas where additional guidance is needed include:

1) wireless technologies according to NIST SP 800-48;
2) protecting critical infrastructures from cyber vulnerabilities and threats;
3) remote access to DHS' systems;
4) vulnerability scanning;
5) penetration testing;
6) incident detection, analysis, and reporting;
7) security configuration policies and procedures;
8) specialized security training; and,
9) IT security training costs.

The department has developed an adequate process to report and capture known security weaknesses in its Plan of Action and Milestones (POA&M) and has adopted an enterprise management tool, *Trusted Agent FISMA*, to collect and track data related to all POA&M activities. *Trusted Agent FISMA* is used to collect data on other FISMA metrics, too. Last, the department purchased a certification and accreditation tool that will be used by all components to certify and accredit all systems.

Each organizational component has appointed an Information Systems Security Manager (ISSM) to ensure that the component's information security requirements are properly implemented, managed, and enforced; and, that its information security program is aligned with the DHS Information Security Program. DHS' CISO issued guidance, in the *ISSM Guide to the DHS Information Security Program* (dated July 19, 2004), to the organizational component's ISSMs which outline specific responsibilities. Together, the policies and procedures developed by the DHS CIO and CISO - when fully implemented by the components - should provide DHS with an effective information security program that complies with FISMA.

While DHS has made significant progress over the last two years to develop, manage, and implement its information security program, its organizational components have not yet fully aligned their respective security programs with DHS' overall policies, procedures, or practices.

Factors which kept the department from having an effective information security program include lack of a system inventory, lack of a formal reporting structure between the CIO and the organizational components, and lack of a verification process for FISMA performance metrics including security weaknesses.

- One of the impediments to implementing DHS' agencywide information security program is that the CIO is not a member of the department's senior management team. Therefore, the CIO does not have the authority to strategically manage agencywide IT programs, systems, or investments. Furthermore, there is no formal reporting relationship between the DHS CIO and the component CIOs or between the DHS CISO and the organizational components' ISSMs. While DHS' CISO meets with the ISSMs on a regular basis and has issued departmental security policies and procedures, he does not have the authority to oversee or ensure that the organizational components' management of their information security program complies with DHS' agencywide security program policies and procedures.

- DHS does not have an accurate and complete system inventory. An initial attempt at developing a system inventory in FY 2003 did not lead to an accurate picture of DHS' information systems. The lack of understanding by those responsible for identifying required system information has hindered DHS' ability to compile a comprehensive system inventory. In September 2004, DHS began a second effort using an outside contractor to establish an agencywide system inventory. A standard methodology for identifying the inventory at each organizational component was developed and the department hopes to complete this task by the end of the summer. Once the inventory is complete, the department should be positioned to better manage its critical systems.

- While DHS has developed an adequate process to report and capture known security weaknesses in its Plan of Action and Milestones (POA&Ms), DHS' organizational components have not established verification processes to ensure that all known IT security weaknesses are included in POA&Ms. With no assurance that all security weaknesses have been identified, DHS cannot verify that all security weaknesses are mitigated or corrected.

- Finally, due to the lack of resources in the DHS CISO office, there has been a limited effort devoted to verifying FISMA metrics as reported by the organizational components. Until the CISO can determine with confidence the FISMA metrics for its components, DHS cannot effectively manage its information security program.

Overall, DHS is on the right track to create and maintain an effective information security program. However, the department and its components still have much work to do to get to the point where DHS has a mature FISMA compliant information security program.

Methodology and Resources Used to Audit DHS

The Information Security Audit Division, within the Information Technology Audit group is responsible for assessing the security of information systems and for conducting the annual FISMA evaluation. We performed the 2004 FISMA evaluation utilizing the requirements outlined in OMB Memorandum M-04-25, *FY 2004*

Reporting Instructions for the Federal Information Security Management Act. We conducted our fieldwork at the program level (DHS CISO) and at DHS' major organizational components. We assessed DHS' compliance with the security requirements mandated by FISMA and other federal information systems security policies, procedures, standards, and guidelines; including NIST SP 800-26 (*Security Self-Assessment Guide for Information Technology Systems*) and NIST SP 800-37 (*Guide for the Security Certification and Accreditation of Federal Information Systems*).

Specifically, we used the previous year's FISMA independent evaluation as a baseline for our evaluation and assessed the progress that DHS and its organizational components have made in resolving weaknesses previously identified. We reviewed DHS' Plan of Action and Milestones (POA&M) process to determine whether all security weaknesses were identified, tracked, and addressed. We identified the policies, procedures, and practices that DHS has at the program level as well as at the organizational component level. We evaluated the processes, such as certification and accreditation, security training, and incident response, that DHS has implemented as part of its agencywide information security program.

We utilized contractors to test DHS' compliance with NIST security guidance for a sample of eight systems at seven organizational components to ensure that weaknesses, if any, were identified, captured, and tracked in the POA&Ms. Contractors were used to evaluate DHS' major organizational components progress in developing, aligning, and managing their information security program and practices in compliance with the agencywide information security program. Areas that were reviewed included information security awareness training; security incident detection, handling, response and reporting; certification and accreditation; security configuration management; and, POA&Ms.

Additionally, we included in our FISMA responses the results of audits which were performed during the reporting period - including the financial statement audits, and information security audits of wireless networks, remote access systems, and national security systems. Our ongoing audit work will allow us to determine how the department and its components are managing and securing its information systems. For example, we are currently performing audits of network security, database security, and the major DHS application - US-VISIT.

Need for a Standard Information Security Audit Framework

There is a need for a standard audit framework for information security similar to that used in financial audits. This framework would help ensure that all IGs review and report on the same information across all agencies. At this time, each IG performs its FISMA evaluation based on its interpretation of FISMA and OMB guidance. The extent and depth of the FISMA evaluation also is based on the resources that are available to perform the review. A standard audit framework should allow OMB and Congress to more effectively and objectively determine the status of information security across the entire federal government. A standard audit framework would help the agencies, OMB and Congress to determine the progress each agency is making in improving or maintaining its information security program.

Additional Guidance and Procedures Needed to Comply with FISMA

OMB issues annual guidance to agencies and IGs to promote consistent reporting across government and to ensure that agencies comply with FISMA. However, clearer guidance would assist agencies and IGs in helping to ensure that all federal agencies comply with and report on FISMA.

One suggestion is to establish a standard “cut-off” or “as-of” date to perform the annual agency assessment and IG independent evaluation, similar to the fiscal year-end used for financial statement audits. The cut-off date should be one-two months prior to the report’s due date to OMB. By establishing a fixed date, agencies and IGs would have adequate time to review the information security programs and respond to OMB. Any security program improvements made after the cut-off date would be addressed in the next year’s FISMA report. A cut-off date would allow for consistency among agency reports since all reports would cover the same period of time. Further, if OMB requests that IGs evaluate the agency’s FISMA responses, the IGs reports should be due at least one month after the agency’s FISMA report is due. This would allow the IG to evaluate the agency’s responses to the FISMA metrics and questions and obtain responses to any recommendations.

The timing of the OMB issuance of the guidance needs to occur sooner in the year. Each year the final guidance is issued closer to the date the FISMA report is due to OMB. Last year, for example, OMB did not issue its final guidance until August 23, 2004 - when the final report was due to OMB October 6, 2004. In the previous year, the final guidance was issued on August 6, 2003 and in 2002 the guidance was issued on July 2, 2002. Such late issuance of the reporting instructions does not allow the CIOs or IGs to effectively collect all program measures required by OMB throughout the year. Since there is little time to address the additional and changed performance measures from the previous years’ reporting requirements, the IG may need to reallocate resources to determine the status of these performance measures very quickly in order to complete the FISMA report timely. Additional performance measures that were requested last year included determining if the agencies had begun assessing systems for E-authentication risk; determining the policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training; determining if agency wide policies that require specific security configurations have been implemented and the degree by which the configurations have been implemented; and determining the overall quality of the certification and accreditation process.

Also, DHS’ organizational components have struggled with the definition of a “system” for FISMA reporting. Since the DHS CISO has been unable to rely on the number of systems reported by the components, the CISO cannot properly manage the information security of all critical systems. Other areas where the department has struggled with definitions in the FISMA guidance include contractor services and the role that the agency has in overseeing the security of the contractor as well as the difference between significant deficiencies, material weaknesses, and reportable conditions as they relate to FISMA reporting.

Another area of concern is how security of systems is measured by the FISMA metrics. OMB asks the agencies and IGs for the number of systems that have been reviewed, certified, and accredited but treats all systems the same. That is, systems are not differentiated between routine or mission-critical systems. For example, an agency may have certified and accredited 80% of its systems, but it could still be seriously at risk if its mission-critical systems are those systems that have not been certified and accredited.

An area where modification to the OMB guidance would be helpful to the IGs and does not appear to be a benefit in reporting is the requirement for the IGs to fill out numbers in some of the tables (i.e., system inventory, incident reporting and analysis, training) that are already reported by the agency. Since the guidance only requires that the IGs report on systems that they have reviewed or information that they have verified, there does not appear to be any benefit in reporting these numbers for larger agencies.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the Committee.

Related DHS OIG Information Security Audit Reports

- DHS Information Security Program Evaluation, FY 2003 (OIG-IT-03-02, September 2003)
- Evaluation of DHS' Information Security Program for Fiscal Year 2004 (OIG-04-41, September 2004)
- Inadequate Security Controls Increase Risks to DHS Wireless Networks (OIG-04-027, June 2004)
- Progress and Challenges in Securing the Nation's Cyberspace (OIG-04-029, July 2004)
- DHS Need to Strengthen Controls for Remote Access to Its Systems and Data (OIG-05-03, November 2004)
- DHS Requires Additional Processes and Controls Over Its National Security Systems (OIG-05-09, January 2005)