TESTIMONY OF
Margaret H. Graves
Acting Chief Information Officer
U.S. Department of Homeland Security
Before the
House Oversight and Government Reform
Subcommittee on Management, Organization, and Procurement

May 19, 2009

Chairwoman Watson, Ranking Member Bilbray, and Members of the committee, thank you and good morning. Today, I will discuss the current state of information security at the Department of Homeland Security (DHS) and our efforts to comply with the requirements established under the Federal Information Security Management Act of 2002 (P.L. 107-347).

The Federal Information Management Act of 2002 (FISMA) was originally enacted in the same year that the Department of Homeland Security was created. In a sense, both the Department and the statute have grown up together, and, for this reason, it is certainly appropriate for the Department to comment on the state of implementing FISMA requirements in the federal government. Thank you for that opportunity.

As the Acting Chief Information Officer (CIO) for DHS, I am regularly confronted with a wide range of issues associated with delivering robust and effective information technology (IT) services for one of the largest agencies in the Federal government. The requirements for IT services in the Department are just as diverse as are our missions; from protecting our borders, to securing air travel, to protecting key government officials, to providing immigration services, to managing Federal response after a disaster, and many other missions that are equally important.

The Department's complex IT infrastructure must support all of these diverse missions, each with their own unique IT requirements. To do this, DHS is leveraging the power of information technology to bring them together under a common, shared enterprise communications backbone. None of this would be possible without a strong information security program that not only fully implements the original Federal information security vision of Congress back in 2002, but also meets both the letter and the spirit of the FISMA statute as currently enacted.

In 2004, the Department of Homeland Security embarked on a multi-year strategy for bringing the Department into full FISMA compliance. In 2005, the Department conducted a comprehensive, Department-wide IT systems inventory. Today there are approximately 600 major systems in use in the Department. Approximately one-third of these systems reside in contractor facilities; however, all systems regardless of whether they reside in government or contractor facilities are required to undergo a full certification and accreditation prior to becoming operational. In 2006, all systems – both government and contractor operated - completed a full certification and accreditation to ensure that appropriate system-specific controls were in place. I should also point out that every system in the FISMA inventory is required to complete a risk assessment as part of the certification and accreditation process, and every risk assessment is reviewed by the Office of the CIO

We have also made great strides in improving our IT business processes, especially in the area of security compliance. The Department's Systems Engineering Life Cycle program requires security review at all appropriate key decision points. The Homeland Security Acquisition

Regulation includes specific contract language that expressly requires contractors to comply with applicable Department security policies. Additionally, the Office of the CIO reviews and approves all IT acquisitions over $2.5 million in the aggregate, and Component CIOs are required to review and approve IT acquisitions for any level of funding. This includes specific vetting to ensure that applicable security requirements are fully incorporated into each IT contract.

In 2007, the Department's Enterprise IT Security Operations Center (DHS SOC) was chartered to provide a 24X7 computer incident monitoring, handling, and response capability for the Department, and today this Center is the central coordinating and reporting authority for all computer security incidents throughout the Department. The primary focus of the DHS SOC has always been to mitigate the effects of the pervasive "Internet pollution" that permeates the Internet today. These threats include standard viruses, worms, and other forms of malicious payloads that do not directly target any specific agency or group. Mitigation activities for these threats include deploying commercially-provided antivirus protection; entry and egress proxy services and filtering, to include email filtering for SPAM; oversight and management for installing vendor provided software patches; aggressive scanning for evidence of infections; and a comprehensive Department-wide incident reporting and handling program.

By late 2007, it had also become apparent that in addition to these non-specific threats, there was a growing class of sophisticated actors who directly targeted the Department. For this reason, the Department created its own internal Focused Operations Team to improve situational awareness about these sophisticated actors, to better understand enterprise risk associated with

targeted attacks, and to develop and deploy response capabilities to deter them. This team is chartered under the DHS CIO and includes key representatives from the Office of Security, the Office of Intelligence and Analysis, and the DHS Security Operations Center. Appropriate CIOs and system owners from our components are also represented on a case-by-case basis. All DHS SOC personnel have been trained to look for and recognize incidents of special concern and that require more detailed analysis by the Focused Operations Team.

We have now learned first-hand about this growing category of threats that directly target the Federal government, our systems, and our information. We have also witnessed how these threats have become more persistent, more pervasive, and even more aggressive than we imagined. These actors appear to be highly-motivated and well-resourced, and it will take all of our collective efforts to keep them out of our networks. For this reason, the Department is fully committed to implementing all Federal IT security initiatives; including, deploying Trusted Internet Connections; complying with the Federal Desktop Core Configuration initiative; fully implementing Homeland Security Presidential Directive 12, to include logical access; and hardening our Domain Name Servers (DNS) with the use of the DNS Security protocol.

Over the last two years, the Department's Focused Operations Team has also provided some key recommendations for other internal enterprise security enhancements as part of an overall defense-in-depth strategy, and all of these initiatives have been specifically developed to better confront these sophisticated actors. Three enterprise consolidation initiatives are at the core of these efforts. All of these initiatives are fully supported in the President's fiscal year 2010 budget

that was recently submitted to Congress for approval, and I would ask for your support for them. Specific initiatives include:

1. "OneNet" is a major Department initiative for collapsing legacy wide-area networks (WAN) into one enterprise WAN. Each major component necessarily requires a unique set of IT security policies in support of their diverse missions, and these policies must be resolved separately in order to facilitate information sharing across a single, shared, enterprise wide-area network. Without the ability to effectively resolve these policy differences at the enterprise-level, either (1) information sharing will be severely limited, or, (2) the enterprise will naturally devolve to the least common denominator at the expense of protecting sensitive mission data.

For these reasons, the Department is transitioning all Components into mission-unique Trust Zones through the implementation of a series of Policy Enforcement Points (PEPs) beginning in 2010. PEPs are comprised of hardware and software packages positioned throughout the network, as well as appropriate management functions at the SOC. Specifically, each PEP will include an enterprise-managed firewall to resolve policy differences, and sophisticated monitoring capabilities that will provide the SOC with enhanced visibility across the entire enterprise. This enhancement will provide the ability to track and respond to sophisticated threat actors that now regularly target the Department.

2. Currently, phishing emails are the number one attack vector for adversaries who directly target DHS and our leadership. There are usually over 100 of these a week, and while we have

improved our ability to detect malicious emails at the perimeter, we must continue to engage at multiple levels in the phishing email battle. Security controls for email must be strengthened, and we are adding some email specific features to the Trusted Internet Connections that will allow us to further improve our ability to detect and respond to malicious emails.

3. The Department's Data Center Consolidation Program has now delivered two world-class enterprise data centers, each with a number of enhanced security controls to ensure high-confidentiality, high-integrity and high-availability for applications residing in the data centers. Additionally, each data center now houses one of the two Trusted Internet Connections that have been designed with sophisticated threats in mind. Further, the Department's new data centers deliver utility computing and Infrastructure as a Service, allowing DHS to realize the benefits of cloud computing while also providing the security so necessary for the threats we face today. We are in the process of migrating applications to the data centers and in this way we will improve protection and monitoring for those applications.

At this time I would like to acknowledge the great work that the United States Computer Emergency Readiness Team (USCERT) is doing on behalf of Federal agencies. A few years ago, US-CERT began deploying a new set of government-specific sensors that are specifically designed to alert on these sophisticated threats. This monitoring capability is called "Einstein" and of the 55 Einstein 1 sensors that were originally deployed government-wide, 17 have been deployed specifically to protect the DHS network perimeter. More recently, an enhanced version of Einstein has also been developed by US-CERT, and the first Einstein 2 sensor was deployed at the Department's Trusted Internet Connection at the DHS data center in Mississippi. A second

Einstein 2 sensor is also now deployed at our other Trusted Internet Connection at our second data center in southern Virginia. These sensors are a key component of our overall monitoring program and have greatly improved our ability to detect attacks in near real time, so that we can implement appropriate mitigation efforts before major damage occurs. The Department conducted a Privacy Impact Assessments for (PIA) the original Einstein system and the updated Einstein 2 system. These two PIAs are available on www.dhs.gov/privacy and serve both to explain how the system works and additional privacy protections DHS builds into its approach to information security.

As you can see, DHS has significant experience operating within the FISMA framework and it is clear to me that the original FISMA statute advanced the state of cybersecurity. It correctly places IT security accountability with three key individuals, the Agency Head, the Chief Information Officer, and a Senior Agency Official for Information Security, commonly referred in most federal agencies as the Chief Information Security Officer or CISO. The statute directed the National Institute of Standards and Technology (NIST) to develop both standards and guidance, and today the NIST IT security framework is considered to be the gold standard for security controls implementation. The statute also mandates annual, independent information security program reviews by the Inspector General, to ensure transparency and accountability. Finally, the statute acknowledges the fact that the real mission of the federal government is to provide a wide-range of diverse services to our citizens, by taking a risk-based approach to information security. Because of FISMA and the hard work of Federal employees to implement it, the federal government has made significant progress in strengthening our IT security posture.

Also as a direct result of the original FISMA statute, Federal agencies now have a comprehensive framework for implementing system-level controls, and these controls provide a strong foundation on which to build. Specifically within DHS, we have institutionalized all statutory requirements into our programmatics so that all system owners are building in security requirements as a matter of course. In addition, the DHS CISO ensures that security requirements are met at every stage of the system life cycle.

What is also apparent is that simply maintaining a controls framework alone is not enough. Sophisticated threat actors are persistent and aggressive, and despite our best efforts at maintaining effective controls, it is highly likely that these actors will from time-to-time be at least initially successful. We must count on this, plan for this, and be ready to act, so that a small problem doesn't become a big one. This means that in addition to implementing and maintaining strong system-level controls, and fully deploying government programs that are available, like those provided by USCERT, each and every agency must also develop in-house capabilities to improve overall situational awareness, especially with respect to enterprise network and systems transparency, and to be ready to respond quickly and effectively whenever there is any indication that an attack has begun. This means that CIOs and CISOs must have dedicated teams in place to monitor for, assess, and respond to these sophisticated actors. Team members must be cleared to appropriate levels to ensure they have the necessary situational awareness for dealing with these actors. Organizational processes must also be instituted so that the team can quickly engage with system owners, program managers, and agency leadership to ensure effective and timely responses that are consistent with overall mission objectives for the agency.

DHS has made significant and measurable progress in implementing all of the FISMA requirements, and, the enterprise security initiatives I have outlined represent major steps for improving the Department's overall security posture. But there is always more that can be done by both the Administration and the Congress in the area of Federal IT security management. The Department welcomes the opportunity to work with Congress in developing any future strategy that will not only build on past implementation successes, but also remain relevant and effective in today's ever changing IT security threat environment.