Prepared Testimony of
Tim Bennett
President
Cyber Security Industry Alliance

Before the House Oversight and Government Reform Committee
Subcommittee on Information Policy, Census, and National Archives

Thursday, February 14, 2008
11:30 am
Rayburn Building Room 2154

Chairman Clay, Ranking Member Turner, and other Members of the Subcommittee on Information Policy, Census, and National Archives, I thank you for the opportunity to share the views of the Cyber Security Industry Alliance (CSIA) on improvements to the Federal Information Security Management Act of 2002 (FISMA). CSIA is a group of leading security technology vendors that are dedicated to ensuring the privacy, reliability, and integrity of information systems through public policy, technology, education, and awareness. It is our belief that a comprehensive approach for enhancing the security and resilience of information systems is fundamental to economic security, national security, and sustained confidence in the Internet.

First please allow me to commend this Subcommittee and its parent Committee for the sustained attention that has been given in recent years to the critical objective of strengthening information security within the U.S. federal government. As we have painfully learned, federal systems are frequently vulnerable to cyber attacks, and the oversight by this Subcommittee and full Committee are an important element in holding federal agencies accountable for improved information security as well as highlighting ongoing challenges and vulnerabilities. The 110th Congress now has an important opportunity to amend FISMA to improve the information security climate at our federal government agencies. Even though the last few years have yielded a number of successes, there are certain weaknesses in our government's critical infrastructure which still urgently need to be addressed.

Today's hearing is especially timely given the escalating, large scale information security intrusions and data losses that have occurred at our federal agencies over the past year. As the Committee explores enhancing FISMA, I think that it is particularly important for us to first understand the current evolving threat landscape including the nature and scope of the threats to our government's IT security infrastructure.

According to the Identity Theft Resource Center, the number of publicly reported data breaches rose over 40% in 2007 from the previous year while at the same time exposing over 127 million records in 443 reported data breaches. Additionally, CSIA member company Symantec reveals in its most recent 2007 Internet Security Threat Report (ISTR) that the government sector is the third most targeted sector for global cyber attacks and yet at the same time is wholly responsible for 26 percent of all data breaches that may lead to identity theft.

It has become clear that the infiltration of federal government networks and the possible theft and/or exploitation of information are among the most critical issues confronting our federal government. We've recently become aware of a series of attacks perpetrated by hackers operating through Chinese Internet servers against our computer systems at several federal agencies. Hackers were able to penetrate Federal systems and use "rootkits" – a form of software that allows hackers to mask their presence – to send information back out of federal agency

systems. Last year, the Department of Homeland Security (DHS) reported that it had experienced 844 "cybersecurity incidents" in fiscal years 2005 and 2006. These incidents and statistics clearly underscore that we are all at risk and present clear warning signs that we must devote serious attention to our nation's information security. While progress has been made, much work remains to be done in order to truly secure our government's IT infrastructure.

FISMA has been fairly successful in getting agencies in general to pay closer attention to their information security obligations. Before FISMA, information security was not a top priority at federal agencies. FISMA has been very successful at raising awareness of information security in Congress and federal agencies (for both agency leaders and their IT departments). However, federal agencies scored an average grade of "C-" on 2007's information security report card. As you know, these scores were based on FISMA audits conducted throughout the past year. Last year's average grade was an improvement over 2006 when agencies scored an average of "D+".

Some argue that FISMA does not adequately measure information security: a high FISMA grade doesn't mean the agency is secure, and vice versa. That is because FISMA grades reflect compliance with mandated processes: they do not measure how much these processes have actually increased information security. In particular, the selection of information security controls is subjective and thus not consistent across federal agencies. Agencies determine on their own what level of risk is acceptable for a given system; they can then implement the corresponding controls, and certify and accredit them and thus be compliant and receive a high grade, regardless of the level of risk they have deemed acceptable.

While these grades show slow but steady improvement from past years, challenges obviously remain. There are encouraging signs of progress in the 2007 report, but we continue to be concerned that large agencies like the Defense Department and DHS are still lagging in their compliance. These and other agencies are still lacking in implementing configuration plans, in performing annual tests of security controls, and are inconsistent in reporting incidents. The annual report card does indicate that the federal government overall has made some improvements in developing configuration plans, employee security training, and certifying and accrediting systems.

FISMA does not tell the whole story when it comes to agencies' information security practices. Nowhere is an agency's ability to detect and respond to intrusions measured in FISMA. FISMA is a great baseline log, but clearly much more needs to be done in this area. We need to incentivize strong information protection policies and pursue a goal of security rather than compliance. The FISMA process is a good one, but we need to always ask ourselves if we can make it better as new threats evolve. We believe that optimal security policies would require agencies to monitor networks, test penetration, complete forensic analyses, and mitigate vulnerabilities.

Certainly, we want to avoid a 'check the box' mentality and don't want FISMA to be reduced to a largely paperwork drill among the departments and agencies, consuming an inordinate amount of resources for reporting progress while yielding few genuine security improvements. Unfortunately, in some cases that is what it has become. Some federal agency CISOs are measured on their compliance scores with FISMA, not on whether they have adequately assessed risk in their respective agency or prevented breaches of sensitive information.

Instead, we want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. With the benefit of five years' experience under FISMA and several insightful reports by the U.S. General Accountability Office, it is now possible to identify possible improvements that can address those weaknesses in FISMA implementation that

have now become apparent. With global attacks on data networks increasing at an alarming rate and in a more organized and sophisticated manner, *there is precious little time to lose*

Faced with this urgent need for action, CSIA applauds Chairman Clay for introducing H.R. 4791, the Federal Agency Data Protection Act of 2007. We strongly support this bill. It would undertake the important step of codifying many of the recommended steps that the Office of Management and Budget took in a series of memos to U.S. federal agencies after a series of significant data breaches during the past couple of years. The legislation provides much needed commonsense obligations to require agencies to develop policies and plans to identify and protect personal information, to develop requirements for reporting data breaches, and to report to Congress a summary of information security breaches reported by federal agencies.

We recommend that the proposed legislation also include language requiring that data breaches of information systems maintained by contractors or other sources working on federal projects be promptly notified to the Secretary and the CIO of the contracting agency. Contractor obligations for taking steps, such as notifying affected individuals or providing credit monitoring, may be unclear unless specified in the contract. Federal contractors were responsible for many of the data breaches that agencies reported. CSIA believes that it's important to reaffirm that the Federal Information Security Management Act applies to federal contractors.

We commend the Chairman for also having the insight to incorporate language into this legislation requiring that federal government agencies encrypt, or make unusable and unreadable, personal data and to establish minimum requirements for protection of information on mobile devices.

HR 4791 also prudently establishes security requirements for peer-to-peer networks. CSIA believes that agencies should be required to develop a plan to protect against the risks of peer-to-peer networks, and provide detailed technology and policy procedures they should take. Peer-to-peer file-sharing applications allow computers to exchange information directly without connecting to a central server. Peer-to-peer (P2P) file-sharing allows users to share files online through an informal network of computers running the same software. File-sharing can give users access to a wealth of information but it also has a number of security risks. You could download viruses or other malicious code without meaning to. Or you could mistakenly allow other people to copy files you don't mean to share which greatly increases the possibility of a security breach.

To assist in the Subcommittee's further consideration of H.R. 4791, CSIA offers the additional recommendations below.

1. **Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to *ensure* should become the power to *enforce* cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.**

- To effectively establish and maintain a comprehensive information security program for federal agencies, CIOs and CISOs need the enforcement authority, budget authority and personnel resources to carry out this essential mission. Funding needs to be allocated to those organizations and facilities that require the most support.

- The senior management of organizations that do not actively support the information security efforts must be held accountable for the failure of the organization to meet its FISMA responsibilities.

2. **Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.**

- Agencies need to implement strategies for security monitoring that assesses the health and resiliency of information systems on a regular, *continuous* basis.

- Although NIST issued base-line control updates in December 2006, additional emphasis on evaluation consistency for cyber security readiness among agencies is needed. This is complicated by differences in background and expertise at the Agency Inspector General level.

- Congress should codify CIO/CISO responsibility and authority for testing and continuous monitoring as needed, but more than once a year.

3. **Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.**

- The federal government is responsible for a massive amount of information technology assets that is expanded and maintained by a substantial IT budget. Those assets are located within the U.S. and abroad, within government owned buildings and leased buildings, in the homes of telecommuters and others, and can be stationary and mobile. It is a complicated task to complete a comprehensive inventory, but you can't protect what you don't know about even though an enemy might know about it. Control systems have been added to NIST guidance, but this needs to be incorporated into the law. Although this is presently a requirement, implementation of a complete inventory must be made a priority.

4. **Improve performance measurement and provide incentives to agencies that give information security a high priority.**

- OMB should establish metrics and leading indictors on an annual basis that address agency performance on a 12 to 24 month timeframe. This would provide Agencies with some lead time to identity resources and implement controls to achieve some measure of performance with the identified metrics. Using a security maturity model such as NIST's Program Review for Information Security Management Assistance (PRISMA) would also accomplish the same objectives.

- The large federal agencies and departments are viewed monolithically from the outside. Organizations such as the Departments of Energy, the Interior, or Treasury are viewed as a single organization predicated on the assumption the CIOs have management control over the policies, procedures, and implementation requirements of FISMA. In reality, the operating units must each tailor the requirements and institutionalize good security practices within their organizations. Performance must be measured and collected at both the operating unit and the Agency level.

- With the many competing priorities federal agencies face to deliver mission success in a cost-constrained environment, cyber security is seldom a high priority. Agencies need to be incentivized to provide information security high visibility and a high priority.

Incentives could address a broad range of rewards from public acknowledgement to additional funding or personnel bonuses.

5. **Institutionalize security within federal agency culture.**

- *Training at all levels and functional responsibilities is critical to the success of agencies' information security program.* OMB should establish a CISO Council to meet regularly and report to Congress on the effectiveness of sharing best practices, group purchases of automated tools and training courses, and development a more effective common curriculum for training.

6. **Increase Federal Agency IT Security Funding.**

- President Bush's proposed budget for fiscal 2009 includes $7.3 billion for cyber security efforts -- a 9.8 percent increase from last year. We urge Congress to meet and even exceed these proposed spending levels. According to documents issued by the Office of Management and Budget, five agencies currently rate unsatisfactory in cyber security efforts, based on reports from inspectors general. The Defense Department is still undergoing an audit. Federal agencies submitted planned IT security spending to OMB as part of their budget requests. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding.

7. **Reaffirm objective assessments of commercially available information technologies.**

- Given that new Internet technologies have the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies conduct an objective assessment of their security and not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.

8. **Narrow the scope of the privacy definition.**

- We recommend the Committee consider revising the bills current definition of "privacy" to a narrower scope as defined in the California data breach bill in which "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of California, when the data elements are neither encrypted nor redacted:
    a. Social Security number;
    b. Driver's license number or state identification card number issued in lieu of a driver's license; or
    c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.
    d. The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.

In closing, I commend all of you for highlighting the importance of information security and for examining how we can improve FISMA and federal agency information security practices going forward. FISMA can be strengthened if we develop processes and metrics that truly measure information security and help guide investments in personnel, capabilities, and technical controls that can more effectively secure complex federal computing enterprises. We need to get beyond counting solely on compliance; we need to encourage risk-based approaches to information