Prepared Testimony of
Tim Bennett
President
Cyber Security Industry Alliance

Before the Senate Homeland Security and Government Affairs Committee
Subcommittee on Financial Management, Government Information, Federal Services, and International Security

Wednesday, March 12, 2008
2:30 pm
Dirksen Senate Office Building Room 342

Chairman Carper, Ranking Member Coburn, and other Members of the Subcommittee on Financial Management, Government Information, Federal Services, and International Security, 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.

This hearing is most timely and further bolsters current Congressional consideration of the need for strengthening information security within the U.S. federal government. As we have painfully learned, federal systems are frequently vulnerable to the now relentless onslaught of cyber attacks, and oversight by the Congress is an important element in holding federal agencies accountable for improved information security as well as highlighting ongoing challenges and vulnerabilities. While today's hearing is not focused on a specific legislative proposal, **we believe the 110th Congress has an important opportunity to enhance FISMA to improve the information security posture of U.S. federal government agencies.** Even though the last few years have yielded some improvements in federal information security, there are unacceptable vulnerabilities in federal government information systems that urgently need to be addressed. The federal government should be the leader in adopting effective information systems practices based on understanding and addressing risks to sensitive information and not be the poster child for what can go wrong.

The time for strengthening FISMA is now given the escalating, large scale information security intrusions and data losses that have occurred at our federal agencies over the past couple of years. As the Subcommittee explores amending 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. Unsurprisingly to our members, the Information Technology Association of America's recent report[1] based on its annual survey of federal Chief Information Officers (CIOs) found, for the second year in a row, that "the broad area of IT security and cybersecurity remains the top challenge faced by Federal CIOs."

According to the Identity Theft Resource Center, the number of publicly reported data breaches rose over 40 percent in 2007 from the previous year while at the same time exposing over 127

[1] Transforming I.T. to Support the Mission: Information Technology Association of America's Eighteenth Annual Survey of Federal Chief Information Officers, February 2008

million records in 443 reported data breaches. Additionally, CSIA member company Symantec revealed in its most recent 2007 Internet Security Threat Report (ISTR) that the government sector (after home users and the education sector) is the third most targeted sector for global cyber attacks and 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. Several recent press reports tell 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 successful in raising awareness of information security in 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 a very small 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, in my view, 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.

There were encouraging signs of progress in the 2007 report, but we continue to be concerned that many mission critical agencies like the Defense Department and DHS are still lagging in their compliance. These and other agencies are lacking in implementing configuration plans, in performing annual tests of security controls, and are inconsistent in reporting incidents. The annual report card does, however, indicate that the federal government overall has made some improvements in the areas of 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. In fact, a senior DHS official testified[2] before the House Homeland Security Committee on February 28 that intrusion detection is inconsistent across the federal government. FISMA is a great baseline log, but clearly much more needs to be done in this area. We need to incentivize strong

[2] U.S. Department of Homeland Security, Under Secretary, National Protection & Programs Directorate, Robert D. Jamison before the House Homeland Security Committee, February 28, 2008

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. CSIA believes that optimal security policies would require agencies to conduct effective risk assessments, monitor networks more consistently, test penetration, complete forensic analyses, mitigate vulnerabilities, establish effective access controls to protect sensitive information, and use practices such as strong authentication controls which are widely recognized in the private and public sector as effective.

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, in a more organized and sophisticated manner, and often originating from state-sponsored sources, *there is precious little time to lose.*

The Office of Management and Budget (OMB) has been quite proactive in issuing guidance to federal agencies in an effort to improve the benefits of, and compliance with, FISMA implementation. For example, OMB issued guidance to heads of executive departments and agencies on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" on May 22, 2007. That guidance identified a number steps that federal agencies should take to "...reduce the risks related to a data breach of personally identifiable information" and included recommendations for "...a few simple and cost-effective steps" that included: 1) reducing the volume of collected and retained information to the minimum necessary; 2) limiting access to only those individuals who must have access; and 3) using encryption, strong authentication procedures, and other security controls to make information unusable by authorized individuals.

The OMB Guidance on May 22, 2007, also provided recommendations on how to develop a breach notification policy and processes for notification should a breach of sensitive information occur. It is CSIA's observation that some federal agencies have responded effectively to this guidance and that others are still challenged with it. In addition, the National Institute for Standards and Technology (NIST) has issued several standards, particularly Special Program 800-53: Recommended Security Controls for Federal Information Systems that was based on the internationally accepted standard, ISO 17799. Nonetheless, **CSIA believes that amending legislation is needed to give the weight and suasion of law to the improvements that we are recommending with this testimony.**

The protection of information resources needs to be institutionalized and behavior changed to ensure implementation is both efficient and cost effective. Information security, once viewed as primarily a technical issue, is now a senior management issue key to successful mission accomplishment and business enablement. There needs to be an acknowledgement that security is risk-based and, as such, nothing is absolutely secure. The effectiveness of information security is based on a number of factors including the agency's management, technical, and operations approach, how this fits the mission, the priority given and resources provided, and the incentives to maintain a long term commitment.

To assist in the Subcommittee's consideration of improvements to FISMA, CSIA offers the 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. Accountability at the individual level, not just agency level, is critical to obtaining improved security.

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, and by staffing and budget short-falls in some IG offices.

- 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 has yet to be achieved and 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 identify 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 of a more effective common curriculum for training.

6. **Codify the OMB guideline regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.**

- Given the growing number of incidents where sensitive personal information held by government agencies has been compromised, agencies should be required to notify individuals of data security breaches involving sensitive personal information that pose a risk of identity theft or other harm to the individual. The policies and processes outlined in OMB's May 22, 2007 Guidance titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" should serve as the basis for language in legislation.
- Data breaches of information systems maintained by contractors or other sources working on federal projects should be promptly notified to the Secretary and CIO of the contracting agency. OMB's Fiscal Year 2007 Report to Congress on Implementation of FISMA (released on March 1, 2008) found a decreasing number of federal agencies could confirm that their agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meets the requirements of FISMA, OMB policy, or NIST guidelines.

7. **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 and help direct it to where it is most needed. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding. Given the national security at stake, federal agencies should receive additional information security funds in FY2009 to manage the Administration's Trusted Internet Connections initiative and other priorities tied to the new Cyber Initiative. Federal agencies should not be expected to meet these requirements with current funding levels.

8. **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.

In closing, I commend the Subcommittee for examining whether enough is being done to protect federal IT and secure sensitive information security, and asking 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 information security safeguards that can more effectively secure complex federal computing enterprises. We need to get beyond focusing only on compliance processes; we need to encourage risk-based approaches to information security. We need to embrace the public-private partnership that information security requires; and we need to take steps immediately that improve both the policy and the practice of information security. The overriding objective should be to move federal agencies to act in a manner that equates strong information security practices with overall mission accomplishment. We all know what's at stake.

Thank you.