Written Testimony of

John M. Gilligan

To the

Subcommittee on Government Management, Organization and Procurement

Committee on Oversight and Government Reform

March 24, 2010 Hearing on

"Federal Information Security: Current Challenges and Future Policy Considerations"

I would like to thank the Subcommittee for this opportunity to testify before you today, and I would like to congratulate you on the Federal Information Security Amendments Act of 2010. I believe that this bill is an important step in the nation's efforts to provide the secure and reliable information technology enterprise necessary to ensure our economic and national security.

The perspective that I bring to the Subcommittee is from a career in the Federal government and having had the privilege of serving as a Chief Information Officer as well as a procurement official for complex information technology systems. I also have background in doing secure systems research, systems design and development, as well as consulting in cyber security prior to my government career.

Like many of you, I have a personal sense of urgency for making dramatic improvements in cyber security within the Federal government. This sense of urgency is informed by the growing threat to our way of life resulting from the fundamental weaknesses in the computers and networks that have become the foundation for our nation's prosperity. I have watched over the past decades as the cyber threat has steadily grown and the pace of our ability to protect against these threats has continued to be slowed by lack of attention and in many cases poorly focused efforts. I believe that the Subcommittee's proposed legislation contains the key focus areas needed to make rapid progress against the growing threat. Before I describe these elements, I would like to characterize some aspects of the current cyber security problem as background for my comments on the proposed bill.

Perhaps it is useful to start with the question of: "Why is it so difficult to provide security for our government computer-based systems?" To understand the answer to this question, it is important to examine the enormous complexity of the problem. Cyber attacks focus on vulnerabilities that can and do exist in every hardware and software component. For example, such components include desktop computers, network routers, servers, operating systems, data base systems, web sites, commercial applications, government developed applications, and so forth. Each Federal department has hundreds of thousands or in some cases millions of these hardware and software components. The actual vulnerabilities that become the avenues for cyber attack are contained in the logic statements that comprise each and every one of the hundreds of thousands or in some cases millions of hardware and software components used by each government organization. Also, each of these components has an enormous number of logic statements. For example, there are well over a million of logic statements in even a simple operating system. To achieve a fully secure system, one must ensure that all of these hardware and software logic statements are both perfectly correct and that they cannot be manipulated to compromise security. This requires correctness of many trillions of logic statements. It is important to know that a single logic error can become the entry point and the pathway to successfully attack against an entire enterprise.

The problem of ensuring logic correctness for our computer and network components is one that has been addressed by the world's top scientists for a long time. Suffice it to say that we are not close to having solutions to ensure absolute correctness of the trillions of logic statements. Even if and when solutions become available, it will take a generation to replace the current systems with more secure ones. As a result, we must recognize and deal with the situation that there are many thousands of vulnerabilities that exist in our fielded hardware and software systems that can be exploited by a range of adversaries ranging from malicious individuals and criminals with modest skill levels, to organized crime and nation state actors who in many cases have greater skill levels. Moreover, the threats against our cyber infrastructure are growing in number from both highly trained sophisticated attackers as well as so called unsophisticated attackers.

The Federal information Security Management Act of 2003 was a positive step in improving security within the government. The law established the imperative for Federal managers to put strong emphasis on cyber security. The bill highlighted the need to use a risk-based approach to identify and implement the minimum controls and to establish an independent review process. I was the CIO of the United States Air Force when FISMA was enacted. At that time, I was optimistic about the benefits of the new law.

While FISMA has many positive elements, the implementation of FISMA has been less than fully effective. For example, rather than focusing on minimum controls as required in FISMA, OMB policy guidance to Federal agencies has been to implement the entire catalog of controls (over 300 separate controls) published by the National Institutes of Standards and Technology (NIST). This is not possible for any government agency of any size and has resulted in a "scatter shot" approach to improving security. Moreover, the strong desire to measure and grade Federal agencies has resulted in placing emphasis on characteristics that could be easily measured rather than on controls and activities that best reflect effective security. In general, the required FISMA metrics were manually generated, had little correlation to actual security, and were costly to produce. In addition, the areas emphasized in the metrics did not encourage investments or improvements that would have long lasting improvement in security. In my view, the implementation of FISMA has been like getting on a treadmill as a means to go to a destination, such as to go to the store, or school or church. A treadmill is great if all you want is exercise, but it is not the way to reach a destination. To continue the metaphor, in the implementation of FISMA, the Federal government has certainly burned a lot of calories, but we are still a long way from reaching our destination of dramatically improved security for Federal systems.

While total security is beyond our current reach for the foreseeable future, there are many things that we can and should do to dramatically reduce our vulnerability to attacks, especially from those attackers who are relatively unsophisticated. Studies have shown that the relatively unsophisticated attackers group constitutes the majority of current attacks--about 80%[1] of all attacks as assessed by the National Security Agency. Unfortunately, our current cyber defense mechanisms are currently so fragmented and weak that a malicious individual with virtually no computer skill can download a "canned" attack program from the World Wide Web and can cause significant harm to cyber systems in government and industry.

Despite spending literally billions of dollars spent each year to improve security of cyber systems in the Federal government, we have not been able to implement the basic safeguards that can address what has been assessed as the majority of the threat, the relatively unsophisticated attacker. The root causes for this failure in my view are the following. First, we have not provided sufficient focus for our government security investments preferring instead to let individual organizations determine where to make investments. Given the complexity of the cyber problem just described and the enormous difficulty of assessing cyber attack risks, it is not surprising that this approach has resulted in well intended but poorly focused efforts in most government agencies. Second, the government has been slow to take advantage of available automation in a coordinated manner. Sure the government has bought lots of tools, but their usage is poorly aligned and not integrated. This has resulted in major gaps in security that have become the avenue for attacks. And third, we have relied far too heavily on manual methods to monitor and evaluate technical aspects of cyber security when the complexity of the government cyber environment makes these manual methods ineffective.

While we don't have the ability to produce totally secure systems, we do have the ability to implement the basic safeguards needed to protect our cyber systems from the relatively unsophisticated attacker—the 80% portion of the threat. Recent collaborative efforts among government and the private sector have resulted in guidance for organizations to help focus on the top priority security control areas and to make effective use of automation. In particular, a little over a year ago a group of security experts from the National Security Agency and other Defense organizations, the Department of Homeland Security, the Department of Justice, and the National Laboratories along with private sector security organizations collaborated on the identification of the most common attack patterns against cyber systems. They subsequently identified the corresponding security controls along with the automated means to implement these controls. This collaborative consensus effort among these experts produced a guideline entitled "20 Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines"[2]. This

[1] Testimony of Richard Schaeffer, Jr., Director Information Assurance Directorate, National Security Agency, Senate Judiciary Committee's Terrorism and Homeland Security Subcommittee, November 17, 2010

[2] Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, http://www.sans.org/critical-security-controls/

document describes the 20 most frequent cyber attack patterns and the controls that are needed to protect against these attacks. In effect, these so called ‘20 Critical Controls’ reflect the highest priority security controls necessary to ensure the core foundation of security for our information technology infrastructure. During the past eighteen months, the United States Department of State has implemented the 20 Critical Controls guideline and has achieved significant progress in improving the effectiveness of cyber security department-wide. Other government agencies are beginning to follow the example set by the State Department.

As just noted, the 20 Critical Controls focus on a foundational of controls for our computer and communications systems. While these so-called “good hygiene” control areas will not ensure that the trillions of logic statements are absolutely correct, they provide a solid foundation level of security needed to thwart relatively unsophisticated attackers--the 80% of the problem. These controls include such things as maintaining an accurate and automated inventory of hardware, software, and external connections. Without such an inventory, malicious devices or software can be introduced into government systems disrupting operations or compromising security. Another control is ensuring that the configurations for hardware and software products are set to enable security features and disable potential vulnerabilities. This control area expands on the very successful Federal Desktop Core Configuration (FDCC) initiative. The FDCC was initiated by the United States Air Force to take the “out of the box” operating systems from Microsoft and ensure that the many hundreds of optional settings were securely enabled. Over 600 settings comprise the FDCC. These settings ensure that attackers do not have easy access to break into the system. And while the FDCC is a good start, we need to duplicate this effort for every other software and hardware component as advocated in the 20 Critical Controls. Other controls in the 20 Critical Controls guideline address system administrator privileges, performing vulnerability assessments, implementing boundary and connection defenses, and controls over wireless devices.

While the 20 Critical Controls are not intended to provide absolute security, implementation of them has proven to dramatically improve the ability of complex systems to withstand the majority of attacks. As a result, implementing this foundation or “good hygiene” not only dramatically reduces the impact of cyber attacks, but also permits our cyber defenders to focus their energy on countering the smaller number of attacks from sophisticated adversaries. To me this is a prudent approach to make rapid progress in improving our cyber defenses.

Implementing good hygiene security controls such as those identified in the 20 Critical Controls has additional benefits. Let me illustrate some of these benefits. When an organization implements an automated capability to register and enforce tracking of software and hardware components, also called ‘asset management’, agencies are better able to manage expensive license agreements and to accurately manage their inventory of cyber devices. As another example, when organizations use so called “locked down” configurations such as FDCC and automated tools to ensure continuous enforcement of these configurations, help desk calls are dramatically reduced and system availability is increased. Related automated methods used to distribute software patches for these locked down configurations dramatically reduces the demand on network and system administrators, permitting personnel reductions and significantly reduced system down time. The bottom line is that a cyber system that implements good hygiene through a solid foundation of controls is a lot cheaper to operate. In fact, my experience in the Air Force convinced me that implementing good hygiene such as the controls reflected in the 20 Critical Controls has such a positive impact on cost of operations that the security benefits are achieved with cost savings—not additional costs. This raises the question of why any CIO or government manager would not immediately rush to implement these controls. After all, implementing the controls gives you better security, better system availability, and lower cost. For me, this is an example of the "ultimate no brainer" for a CIO.

If this is such a "no brainer", then why have government and industry organizations not been more aggressive to implement these controls? The answer I assert is twofold. First, all organizations, but in particular in government organizations, are unwilling to deviate from policy mandates. As an example, if OMB mandates paper reports from departments and agencies and is publishing 'grades' based on the paper reports, a CIO better ensure that he or she has the required paper reports. The solution in this case is to ensure that the policy mandates focus on the right things.

A second reason for the failure to implement these controls is a bit more subtle. Implementing a disciplined cyber environment such as suggested by the 20 Critical Controls will result in the lessening or elimination of autonomy of individual users as well as local system and network administrators. No longer can users download software which may or not include malicious code when they desire. Also, local administrators can no longer tinker with the configurations to "optimize" the system. These and other common practices degrade overall security across the enterprise by introducing vulnerabilities that are exploitable often by even the most unsophisticated attackers. However, removing this autonomy from users and local administrators goes to the heart of the culture surrounding computer technology. Most users think that they should be able to control their computer. After all, wasn't the first desktop appropriately called the 'personal computer'? Likewise, local administrators believe that they know best how to operate and secure local systems to meet their local mission needs. This is not the case of individuals being malicious, nor is this cultural phenomenon unique to government. Very strong leadership is required to counter this cultural resistance in order to implement an organization wide cyber environment that provides the disciplined foundation controls that are called for in guidelines such as the 20 Critical Controls. The most senior officials in government organizations must unequivocally endorse these changes to overcome the cultural resistance.

The proposed legislation does an excellent job in responding to the needs for improving the security of our Federal government systems. Putting the focus for coordinating our Nation's cyber security in the White House, in the National Office for Cyberspace (NOC), ensures that we have the focused attention on cyber security and leadership from the most senor levels in government to help overcome organizational and cultural resistance. Moreover, the proposed Federal Cybersecurity Practice Board provides the necessary expertise and authority to help the Director of the NOC develop effective policy guidance and standards. I acknowledge that NIST has done an excellent job of developing guidelines. What is needed at this point is policy to focus government organizations on how to apply the NIST guidelines. The emphasis in the bill on minimum controls and the use of automation to continuously monitor the controls is both properly aligned and much needed. Finally, the bill addresses an often overlooked area, the need to leverage the power of the government acquisition buying power to require dramatic improvements in the security and reliability of software and hardware products. As we found with the FDCC, this type of action not only results in improved products for the Federal government but more secure products that can be purchased by the private sector as well.

In summary, I would again emphasize that while total security is beyond the state of the art, there are a number of practical and cost-effective approaches that can be taken to mitigate the majority of attacks against our government cyber systems. The State Department and other organizations have provided positive examples of both enforcing a baseline of technical controls as well as the leadership approach necessary to overcome cultural resistance. The proposed bill adds key responsibilities and structure that are necessary to complement existing government authorities. It also provides the appropriate and necessary focus to make rapid progress to get ahead of the rapidly growing cyber threat. We will be well served if Congress passes this bill.