



**Testimony before the
House Committee on Oversight and Government
Reform
Subcommittee on Government Management,
Organization, and Procurement
and the
Subcommittee on Information Policy, Census, and
National Archives**

**“FEDERAL IT SECURITY: THE
FUTURE FOR FISMA”**

June 7, 2007

A Statement by

James A. Lewis
Senior Fellow and Director,
Technology and Public Policy Program

Thank you for this opportunity to testify on this important subject. Improving information security in the Federal Government is a crucial task for the United States. Recent events in Washington and in Estonia highlight the importance of this task. In my testimony, I will briefly discuss the threats we face; the status of federal information security; thoughts about FISMA; and additional ideas for improvement.

I am sure that the Committee members are well aware of the damage done to national security by successful penetrations of Federal networks. Much valuable information has been lost to our opponents. This damage is different from the sort of risks one often hears from the IT community – the risk that a cyber attack will produce physical damage in the U.S. The electronic Pearl Harbor scenarios of the 1990s are entertaining, but not a useful guide for policy or legislation. That kind of risk is small. Our concerns should be with the loss of sensitive information and in the disruption of key services and data as a result of hostile intrusions into our information systems.

Our adversaries have exploited vulnerabilities in Federal networks to obtain information of military and economic value. This has been going on since at least the late 1980s. The most recent episode involved penetration of networks at various agencies, including Commerce and State, and the downloading of masses of information. We should note that an agency's FISMA score was largely irrelevant to how well it was able to withstand these penetrations.

We do not want to overstate the risks. At the same time, we do not want to ignore the damage to national security from intelligence gathering, economic espionage, and the theft of technological or military information. In addition to the theft of government information that damages U.S. security and economic leadership, there is also a real risk that opponents will seek to disrupt government activities by scrambling data and by creating confusion and uncertainty. It is these kinds of informational attacks that pose the risk of even greater harm to the U.S. in the future.

The rapid increase in the sophistication of software tools available for cyber crime and espionage increases the risk of these attacks. A flourishing network of professional criminals has assembled an arsenal of tools. Criminals create and use "bot" networks, where programs automatically search the internet for vulnerable computers and then implant programs that make the infected computer a "robot" available for attacks or spamming. Their ranks now include skilled programmers and cryptographers who carefully monitor and test their own weapons. They also constantly probe networks and software products for new vulnerabilities to exploit. Intelligence agencies, of course, can draw upon the skills and tools offered by cyber criminals (botnets, for example, can be rented by the hour), recruit hackers to carry out missions, and supplement criminal talents and tools with their own specialized skills.

The events in Estonia show how foreign governments, criminal organizations, or cyber protestors can use the tools of cybercrime to disrupt key services. Hackers, probably Russian and probably encouraged by the Russian government, used "botnets" to flood Estonian government and business networks. Botnets are a collection of computers on which a cybercriminal has been able to illicitly load software that makes the computer a "zombie," carrying out the criminal's instructions without the computer's owner even being aware that his or her machine is being used. Millions of computers around the world are infected. The effect of these botnet attacks, which peaked at perhaps a thousand a second, meant that the targeted Estonian networks were unable to respond to legitimate queries from employees, citizens, and customers, and in some cases had to shut down.

There are several lessons we should draw from the Estonian experience. The first is that while the attack was disruptive, it did not turn Estonia into a quivering mass of jelly. There was neither terror nor destruction. The Estonians responded calmly and rapidly to the attacks. Many sites had restored service, at least to minimal levels, within a day or two of the attacks. In part, this was because the kind of attack used against Estonia – called “denial of service” is not the most damaging form of attack. A more determined attacker would have penetrated Estonian computers and scrambled the information located on them. This is a much more damaging tactic for information warfare, and it is the kind of attack about which we should worry.

Estonia is a small nation that has much attention to e-government. The U.S. is much larger, and operates many more networks. This makes it a more difficult target, but at the same time, I am not sure that we would be as efficient in our response as the Estonians. In the last few years, the Department of Homeland Security has undertaken several exercises to test private sector and Federal responses to cyber attack. These exercises point to improvement in our defenses but are not conclusive.

The question of efficiency goes to the heart of the FISMA problem. The U.S. government operates thousands of computer networks to which hundreds of thousands of computers and other devices are attached. We talk about an “Enterprise architecture,” a term from business that entails restructuring a corporation under a powerful CEO to unify the efforts of its business units, but this sort of restructuring and control is not possible for the federal enterprise. No single agency has the ability to control this multifaceted complex of networks.

The tools for managing this complex federal information system are limited. The Office of Management and Budget (OMB), the Defense Department, and the Director of National intelligence each have primary responsibilities for cyber security. Of these lead agencies, OMB faces the most difficult task. Unlike DOD or the DNI, where the component agencies have relatively similar missions and are innately concerned with security, OMB faces agencies with disparate tasks and structures. It is to these “civilian” agencies that FISMA is most useful as a guide, because in the absence of FISMA, cybersecurity would likely receive even less attention than it receives now.

Congress passed the Federal Information Security Management Act of 2002 (FISMA) to bolster computer and network security within the Federal Government. FISMA provides a framework for security and mandates yearly audits, where Agencies report to OMB on their efforts at information security and their compliance with a collection of standards, laws, rules, and processes produced over the years by Congress, the Executive Branch, and the National Institute for Standards and Technology (NIST). The reports include an independent evaluation, either by an Agency's Inspector General or by an outside auditor hired to write the various required reports.

The intent of FISMA was good. There are benefits from FISMA. Unfortunately, an agency can get good marks in FISMA and still be vulnerable. This is despite much good work in the Federal government in recent years to improve the security environment. In assessing why this is so, we need to ask whether FISMA has become irrelevant.

One approach to answering this question is to look at the FISMA process. FISMA involves the production of reports and other documentation. The report certifies whether certain standards are being met. These standards, if followed, may produce security, or they may not.

FISMA is a direct measurement of compliance with processes and an indirect measure of performance. In effect, FISMA does not directly measure security, and if we asked agencies whether or not their networks were secure, as measured by penetrations and data loss, rather than if they were following certain processes or standards, their answers would produce different and better results than FISMA. As many have said, focusing FISMA on performance and outcomes would be an improvement over the current process.

Another way to answer the question of whether FISMA is still relevant or useful is to consider the ways in which technology has changed in the last five years. The most important lies in how the internet is used. FISMA came at a time when the Government was moving from a mainframe environment to what are called client- server networks. This focus on agency networks was appropriate at the time FISMA was written, but it is increasingly less valuable for security as more of the activity happens outside of the agency's network. Some of this change in focus involves what some people call "Web 2.0." Web 2.0 sounds like a marketing term, and to some extent, it is, but it also describes new web applications that are seeing growing use. Federal agencies use some of these applications, such as wikis, blogs, and podcasts. Other applications, such as a reliance on web-based services (those accessible over the Internet) rather than on services hosted at an agency's own computer networks, are not yet widely used in government.

This is the direction technology is taking. In the future, when Federal employees do their work, they will need to access many different networks outside of their own agency. Agency networks will need to be more open to enable information sharing. FISMA is not well suited to this emerging Internet environment. While there are many impediments to getting the Federal government to adopt the most productive and efficient processes found in the private sector, including workforce rules, the budget and acquisitions process, and a preference for low-risk solutions, FISMA is probably an impediment as well. Any re-examination of FISMA should update the Act to allow for the evolution of technology and to move away from a focus on securing the agency network as the way to produce information security to a focus on securing the information itself.

FISMA is the tool we have now for encouraging agency action and until it is replaced, it is the tool we must use. Since FISMA measures the wrong things and does not accurately reflect the real state of information security at an agency, the answer to the question as to whether it is still useful is: FISMA needs a thorough overhaul.

One way to carry out this overhaul would be to replace FISMA's emphasis on certification that an agency had complied to various standards with performance-based measures that focused on vulnerability to attack. These methods could include creating a Federal "Red Team" that periodically tested each agency's defenses to find vulnerabilities. The results of a Red Team exercise might do better at identifying vulnerabilities that could be fixed than a process that assumes that compliance with a standard produces security. Revising FISMA to focus on actual performance measures, such as how many times a Federal information system was probed or penetrated, what vulnerabilities allowed for a successful attack, and what steps the agency had taken to rectify these vulnerabilities, might be the single most important change that the Congress could make.

One way to make improve FISMA or any successor act would be to link it to mandatory consequences. FISMA is not action forcing. A low FISMA score is painful now for Chief Information Officers, but this is not enough. If gangs of hostile foreigners broke into Federal buildings, trashed offices, and carted off dozens of file cabinets, it would be a scandal. When

the same thing happens in cyberspace, we tend to either downplay it or simply throw up our hands. Responsibility for a low score or a successful attack should lie with the head of an Agency, not just the Chief Information Officer. A successful attack or, if we continue to use FISMA, a low score, should trigger a requirement for agencies to reprioritize and reallocate funding to counter information security risks, consistent with appropriations laws.

By itself, FISMA will be insufficient to secure Federal information systems even if it is revised. A revised FISMA should be part of a larger strategy for Federal information security. The elements of this strategy should include increased accountability and responsiveness by agency leadership, adequate funding for security, use of the federal IT acquisitions process, and increased emphasis on protecting information rather than networks.

Using the Federal Acquisitions process to encourage suppliers to produce more secure IT products should also be part of a Federal information security strategy. In this regard, FISMA is just one of several standards and processes already used to evaluate products or processes for security. Other leading standards include the Common Criteria, the Carnegie Mellon Software Institute's Capability Maturity Model (CMM), the ISO 9000 series, ISO 19779, SAS 70, and NSTISSP 11. In addition, the Department of Homeland Security is developing a new evaluation process for software products. All of these standards have their strengths, but the common industry view is that they are inadequate for increasing security. As with FISMA, a Federal information system can use products or networks that have passed these various standards and still be vulnerable.

The Common Criteria process is the most important of the existing processes for certifying software for sensitive Federal applications. Like FISMA, it is expensive, cumbersome, requires large amounts of documentation, and focuses on certifying processes rather than results. A more flexible approach that made the use of existing industry best practices for coding secure software one factor for consideration in acquisitions of commercial software could help to improve security. Part of any larger strategy for securing Federal Information systems should be to develop and implement new ways to use acquisitions to incentivize the IT industry to supply more secure products.

For example, commercial software that was produced using industry best practices for security could be given preference in acquisitions. These practices include security training for programmers, strong management procedures that provide oversight, an independent review of code for security issues (including the use of software assurance tools), and testing of products by red teams or penetration efforts. Many companies have adopted these practices, but acquisitions rules do not take this fully into account. The Federal IT acquisitions process can be a powerful source for change in creating secure commercial products.

Identifying the best practices for federal network security, turning those into common performance standards, and finding a better way to communicate and enforce those performance guidelines across agencies would improve security.

Although there has been progress in recent years, better Federal organization would improve information security. The Departments of Homeland Security and Defense, the Office of the Director for National Intelligence, the Federal CIO Council, the Homeland Security Council, the National Security Council, and the Office of Management and Budget all play a role in developing and overseeing policy for securing federal networks. Rationalizing and streamlining the governmental processes for cyber security is essential. The National

Security Council has created a new Policy Coordinating Committee for Cybersecurity, and making this become a focal point for driving strategy and implementation to improve security.

Let me conclude by noting that in looking at the security of Federal networks, it is fair to say that while the U.S. is better off than it was five years ago or ten years ago, not all agencies have seen equal improvement. Despite FISMA, security remains too low a priority and an afterthought for many domestic agencies. Much remains to be done.

We can draw some encouragement, however, from a similar challenge the U.S. faced in the 1980s. At that time, Federal government voice communications over telephone networks were not secure and our opponents were exploiting them to obtain sensitive information. In the mid-1980s, the federal government began a program to secure its sensitive and classified voice communications. Within five or six years, this program, which was implemented by the National Security Agency, had considerable success in securing the most sensitive Federal communications.

There are major differences, of course, between securing the telephone network of twenty years ago and what is needed to secure information today. There are many more networks and participants, much more data, and the technology is more complex and diffuse. That said, the lesson of identifying a problem, assigning its resolution to a competent agency, and moving aggressively with adequate funding and White House attention to fix it, offers a model on how to address information security.

The Federal government may be the most challenging environment in the world for cybersecurity due to its diversity and size. The U.S. will need to undertake a number of complementary measures to reduce its vulnerabilities, but with better organization and strategies, we can make federal information systems more secure. An improved FISMA could be an useful part of this effort. I thank the Committee for this opportunity to testify and will be happy to answer any questions.