McConnell INTERNATIONAL

Written Statement of

Bruce W. McConnell

President
McConnell International, LLC
www.mcconnellinternational.com

before the
Subcommittee on Information Policy, Census, and National Archives
and the Subcommittee on Government Management, Organization, and Procurement
of the Committee on Oversight and Government Reform
U.S. House of Representatives

Federal IT Security: A Review of H.R. 4791

Thursday, February 14, 2008

Thank you, Mr. Chairman and Members of the Subcommittees, for the privilege and opportunity to testify today on the critical topic of federal information security. The jurisdiction of this Committee is wonderfully broad, and its work is so critical to the effective functioning of our federal government.

My name is Bruce McConnell, and I served in the Office of Management and Budget from 1985-2000, under three Presidents. During that time I was the Chief of Information Policy and Technology, which was the most senior position at OMB concerned primarily about federal information technology matters, and in particular, IT security. In that role I had the opportunity to work with this Committee on many occasions, most notably in the development and passage of the Computer Security Act of 1987, the Clinger-Cohen Act, and several iterations of Paperwork Reduction Act. I also had the responsibility to oversee the implementation of these statutes in the federal agencies, and to develop policies to assist the agencies in performing their missions with the support of IT.

Since 2000, I have been president of a small, eponymous consulting company that works with government and industry to find private sector solutions to pressing federal mission support requirements. I am presently a member of the Commission on Cybersecurity for the 44th Presidency, which is co-chaired by Congressman Jim Langevin and Congressman Michael McCaul, and has been convened by the Center for Strategic and International Studies.

Finally I should mention that, while I was at OMB, I co-chaired the Interagency Working Group on Encryption Policy. Made up of representatives of the intelligence community, the State, Defense, Justice, and Commerce Departments, this group was responsible for reforming U.S. export control policy to enable the use of strong American-built encryption on the global information infrastructure, increasing the security of information that resides there.

You have asked that I provide you with policy recommendations for potential legislative consideration, and to comment on the state of the Federal Information Security Management Act (FISMA) compliance government wide and the provisions of H.R. 4791.

Policy Recommendations

The Nation finds itself at a momentous time. We are ever more dependent on information systems for our livelihood and survival, yet we are falling behind in terms of keeping the systems, both public and private, secure in the face of increasingly sophisticated threats. As a result there is growing attention to the importance of information security. This welcome increase in awareness can be seen on numerous fronts.

- This Committee continues to step up its leadership efforts.
- The Administration has requested a marked increase in funding, and has underway several initiatives, including the Information Systems Security Line of Business, the Trusted Internet Connection program, the Federal Desktop Core Configuration program, the Common Identification Standard for federal computer access, and the Einstein monitoring program.[1]
- A vast number of efforts are underway in the private sector, including the excellent work of the SANS Institute and the CSIS Commission.
- And, on February 5, 2008, the Director of National Intelligence, J. Michael McConnell, provided the outlines of what is known as the "Cyber Initiative."

I want to begin my discussion of policy by examining the Cyber Initiative, because it is the most significant development in the federal information security arena in many years. My discussion is based on the DNI's testimony, and on statements by OMB officials in a public briefing on the IT budget last week. My analysis is somewhat limited, as the details of the Initiative remain classified for national security reasons.

The Cyber Initiative

On January 8, 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. This order establishes a comprehensive, national cybersecurity initiative. The issuance of this order shows that information security is receiving attention at the highest levels of the federal

[1] *See*, variously: Fiscal Year 2009 IT Budget Rollout Presentation, Proposed IT Security Spending, http://www.whitehouse.gov/omb/egov/documents/FY09_IT_Budget_Rollout.pdf, pages 3-4; Budget of the United States Government, Fiscal Year 2009, Table 9-9, "Lines of Business Update," http://www.whitehouse.gov/omb/budget/fy2009/pdf/ap_cd_rom/9_9.pdf; "Implementation of Trusted Internet Connections," OMB Memorandum M-08-05, November 20, 2007, and, "Planning Guidance for Trusted Internet Connections," undated memorandum to chief information officers from Karen S. Evans; "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," OMB Mamorandum M-07-11, March 22, 2007; Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; Budget of the United States Government, Fiscal Year 2009, Analytical Perspectives, Homeland Security Funding Analysis, page 27.

government, a most timely occurrence. In addition, its issuance as a national security order shows an additional seriousness of intent. I believe this is good news.

The initiative recognizes the serious threats to the infrastructure by state and non-state adversaries, including sophisticated criminal elements. It lays out the need to deter hostile action in cyber space by making it harder to penetrate our networks. And it makes clear the need to take proactive measures to detect and prevent intrusions from whatever source, as they happen, before they can do significant damage.

These tenets are important, yet they leave many questions unanswered. For example:

Coverage: The initiative clearly includes government systems, both civilian agency systems and national security systems. But how much further does it go towards protecting the national information infrastructure and the critical private sector systems that are part of it?

Activities: Real time monitoring of systems is included, as is preventative response. But how far does the preventative response reach, what does it involve, and how are trade-offs evaluated in terms of potential damage to the national infrastructure from retaliation from the attackers or collateral damage from our own actions?

Roles and responsibilities: There is clearly an increased role for the intelligence community in protecting systems. But how are agencies such as DHS, the FBI, and OMB involved, what procedures are used to authorize specific activities, and who is responsible for oversight?

Authorities: How does the initiative fit into existing statutory frameworks including the Protect America Act, the Foreign Intelligence Surveillance Act, the wiretapping statutes, FISMA, and the Privacy Act?

Let me explain why I believe these questions are important to the Nation, and germane to this Committee's work.

This Committee's Leadership in Ensuring Open Government

This Committee has long been a leader on government information and information security policy. Indeed, no other Committee has paid attention to these matters so consistently and thoroughly over the years.

The Cyber Initiative relates directly to two statutes under this Committee's jurisdiction, FISMA and the Privacy Act. The Initiative deals directly with federal systems security, the domain of FISMA, and it reaches into areas of the Privacy Act because of the personally identifiable information that is collected during the monitoring of federal networks.[2]

[2] In addition to these policy points, there are potential operational security impacts of more extensive network monitoring. Recently a group of six renowned computer security professionals wrote about unauthorized breaches in Greek and Italian monitoring systems, noting that surveillance technology is an "architected security breach" that "creates serious security risks: the danger of exploitation of [cont., p.4]

At this moment in our Nation's history, a particularly important area of policy is brought into focus by the Cyber Initiative:

How do we, as a Nation, balance effective security with openness in government?

When this Committee wrote, and the Congress passed, the Computer Security Act of 1987, you gave the Office of Management and Budget policy and general oversight authority for civilian agency systems, vested the National Institute of Standards and Technology (NIST) with authority to issue binding guidance, and entrusted agencies to make decisions about implementing and monitoring their networks – balancing the risk and potential magnitude of harm posed by threats against the need to operate systems critical to achieving the agency's mission. Congress also specified the role of the National Security Agency (NSA) with respect to civilian agency systems – one limited to providing technical assistance to NIST.

There were several reasons for this differentiation of responsibilities.

Foremost in the mind of Congress was the potential chilling effect on the free flow of information between government and the citizenry, including the information technology industry, if a military agency became too closely involved with civilian agency systems. With respect to the effectiveness of the NIST standards program, the Committee's report noted:

> "While the Committee was considering [this Act], proposals were made to modify the bill to give NSA effective control over the computer [security] standards program. * * * This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. [NIST] has performed this kind of activity very well over the last 22 years. NSA, on the other hand, is unfamiliar with it.[3]

Later, on the broader issue of citizen-government information flows, the report observes:

> "Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information." [4]

---

the system by unauthorized users, danger of criminal misuse by trusted insiders, and danger of misuse by government agents." Bellovin, Blaze, et.al., "Risking Communications Secuity," IEEE Security and Privacy, 2008, www.computer.org/security.

[3] U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. 100-153, Part II, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), pp 25-26.

[4] Ibid., p. 29.

Indeed, the NSA operates under a different set of norms and authorities than the civilian agencies do. These norms and authorities are properly drawn against foreign and terrorist threats, and support monitoring and response activities against such threats. Likewise, the mission of numerous classified systems properly requires the analysis, identification, and targeting of suspect actors; accordingly, these systems build in many features that limit open access and anonymity.

Conversely, civilian missions, such as those at the Census Bureau, the Internal Revenue Service, and the Centers for Medicare and Medicaid Services, depend on the trust of the American people to operate successfully. The systems that support these missions operate primarily in the domestic environment, where the mission often requires the free and efficient flow of information and open use by the public in order to deliver important public benefits and programs.

Concerns were also raised during the debate on the Computer Security Act about potential risks to privacy and civil liberties if the intelligence community became actively involved in the management of civilian agency systems. In part to address this concern, the Congress established the Computer System Security and Privacy Advisory Board as a senior advisor to OMB, NSA, NIST, and the Secretary of Commerce. Congress emphasized the importance of this concern in 2002 by renaming the Board as the Information Security and Privacy Advisory Board (ISPAB) as part of FISMA.[5]

Thus it was the view of the Congress in 1987 that the importance of maintaining citizen trust in government systems was best served by giving a civilian agency the leadership role.

This statutory framework has been confirmed and strengthened three times in the last two decades – first in the Clinger-Cohen Act of 1996, again in the Government Information Security Reform Act in 2000, and most recently in FISMA. One notable addition to the framework was Section 3544(e) of FISMA, "Public Notice and Comment," which provides that:

> "Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public."

To date, this provision of law has received scant attention from OMB or the agencies, even though it is broadly consistent both in its requirement and its intent with similar provisions in the Paperwork Reduction Act, the Clinger-Cohen Act, and the E-Government Act of 2002.[6]

---

[5] At its most recent two-day meeting in December 2007, the ISPAB reviewed such topics as the role of the Inspectors General, the Einstein program, the state of identity management in the Department of Defense, and status of the National Communications System. *See*: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2007-12/Dec-2007.html

[6] *See:* Paperwork Reduction Act, Section 3517(a), (44 USC 3510 17(a)); the Clinger-Cohen Act (40 U.S.C. 1131(d)(2)); and Section 207 of the E-Government Act of 2002 (relating to the availability of information to the public via agency websites), subsection (f)(2)(A)(i)).

Has The Policy Outgrown Its Usefulness?

It may be that the world has changed so much that the historic distinction between civilian agency systems and national security systems no longer serves the Nation's interest. Certainly, the current computer security regime in government is not working adequately. While progress is being made, it is happening far too slowly. In a networked world where the system is only as secure as the weakest node, progress is far too uneven. Further, as discussed below, FISMA implementation has proven to be a mixed blessing with respect to computer security. As one computer security professional put it recently, "It was pretty clear last year that 100% FISMA compliance does not bother the Chinese spies."

One of the key weaknesses of the historic distinction has been that the Computer Security Division at NIST, while being entirely well intentioned and staffed by dedicated professionals, has never been positioned or resourced in a way to make it an effective leader in federal computer security. Buried within a research bureau of the Department of Commerce, it is no match—in terms of the depth of its capabilities and influence—for a well-funded, high-tech, operational entity like NSA. As a result, the civilian agencies have received less technical assistance than they need to protect their systems in the current threat environment.

Similarly, the effectiveness of the Department of Homeland Security in this arena has, to date, been a considerable disappointment to most observers. For example, the placement of the policy official responsible for cybersecurity activities was criticized both for its fluidity following the creation of the Department, and for not sitting at a very senior level within the Department; DHS' own cybersecurity performance under FISMA has been consistently graded at F or D; and, recently, a House Homeland Security Committee hearing cited a newly released GAO report that found "pervasive and systemic security problems at the DHS."[7]

Of course, the effectiveness of NSA's information security program is debatable as well. NSA is responsible for "protecting all classified and sensitive information that is stored or sent through U.S. government equipment."[8] Traditionally the agency has focused on Department of Defense systems. However the DOD has not demonstrated itself to be consistently strong on information systems security, at least for the systems that handle unclassified (including sensitive) information.

A gap like this provides an ideal environment for attackers to enter and damage government systems, with potential effects both on those systems and other government systems, including national security systems, which they may communicate with. It also can enable attackers to reach beyond the public information on civilian agency systems, and gain access to such highly sensitive information as

[7] Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program, Statement of Gregory C. Wilshushen, Director, Information Security Issues, US Government Accountability Office, GAO-07-1003T, June 20, 2007.

[8] NSA website, "Introduction to the National Security Agency/Central Security Service," http://www.nsa.gov/about/index.cfm, February 12, 2008.

unreleased economic data, taxpayer records, law enforcement information, and health information.

And the gap extends beyond government systems. In the view of Mike McConnell, the Director of National Intelligence:

> The US information infrastructure--including telecommunications and computer networks and systems, and the data that reside on them--is critical to virtually every aspect of modern life. Therefore, threats to our IT infrastructure are an important focus of the Intelligence Community. As government, private sector, and personal activities continue to move to networked operations, as our digital systems add ever more capabilities, as wireless systems become even more ubiquitous, and as the design, manufacture, and service of information technology has moved overseas, our vulnerabilities will continue to grow.[9]

There is, therefore, a substantial argument that national and homeland security of the U.S. require additional resources to be devoted to information security, and further, that the majority of governmental resources for that purpose reside today in the national security community.

Of course, as illustrated by today's panel, there is also substantial private sector capability in this area. Indeed, as is often said, our Nation's critical infrastructures are largely privately owned. What is needed is an effective partnership of trust between the government and private sector to address the Nation's information security needs.

I encourage the Committee to examine this question of roles and responsibilities from a policy standpoint, to determine whether changes in the law are needed. More specifically, the Committee might be interested in exploring the following topics:

1. To the extent that the President's "cyber initiative" gives leadership to the national security community for civilian agency information security, is this change permanent, or is there a transition plan to grow the capabilities of DHS and NIST and return responsibility to them?

2. How will the public be involved in defining security standards and practices of the federal agencies?

3. To the extent that monitoring on government networks involves the collection of information about the public, what safeguards are in place for that data's storage, what minimization procedures are in place to limit such collections, and what governs access to the data that is collected?

4. What procedures are followed to authorize any response activities, and what safeguards are in place to avert "collateral" damage to private sector systems that could occur in retaliation for a response?

5. How does the new policy square with existing statute?

[9] Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence, February 5, 2008, p. 16.

State of FISMA Compliance and H.R. 4791

In addition to providing these general policy recommendations, I want to turn now more specifically to the state of FISMA compliance and in particular H.R. 4791.

Mr. Chairman, there are many in the computer security community who believe that FISMA is a mixed blessing. On the plus side, it has had two good macro effects:

- It has increased awareness of the importance of computer security among CIOs and their bosses.
- It has improved the agencies' knowledge of and control over what is connected to their networks and what needs to be managed.

However, in the years since its passage, it has also generated a culture of compliance that often distracts attention from strong operational security measures. In some agencies, more attention is paid to creating a reporting architecture that will increase FISMA scores than to creating a security architecture that will reduce vulnerabilities and minimize the effect of attacks and breaches.

In this context, H.R. 4791 should be looked at from the standpoint of its likely effect on operational security in the federal agencies.

To begin with, Section 7, which changes the currently required "independent evaluation" into a required "independent audit" is potentially problematic and could foster adversarial relationships and not cooperation. This issue was the topic of much discussion during the original development of FISMA. By calling for an evaluation and not a formal audit, the FISMA authors wanted to give to Inspectors General maximum flexibility in assessing their agency's security program, promote cooperation between the IGs and agency officials, encourage resource and information sharing throughout the year, avoid competition for scarce expert security personnel, and insulate agency employees from negative audit "findings" for efforts designed to improve security. I understand that the intent of this provision is to encourage the use of standardized evaluations across all agencies. I believe this could be accomplished within the framework of evaluations, without requiring formal audits. For example, OMB and the IGs could be encouraged to work together to develop such a standardized set of evaluation criteria within a specific time frame.

While the provisions for protecting personally identifiable information (Section 8 and 9) and the risks of peer-to-peer file sharing (Section 6) are important (and have for the most part already been addressed administratively by OMB), they may be too specific and too media/technology dependent to be appropriate for such detailed consideration in statute. The technology environment is changing ever more rapidly, and, in my experience, it is useful to provide the agencies with flexibility to address risks as they deem most appropriate, subject to strong oversight. The inclusion of these detailed provisions could suggest that these risks are the highest priorities that should be addressed in terms of sensitive information. Even if that is true today, it is unlikely to be the case tomorrow.

In addition, while agency relationships with and use of data provided by data brokers is a significant and growing issue, and the definition of Personally Identifiable Information a is a critical question, I am concerned the bill invokes only the limited procedural requirements required by section 208 of the E-Government Act, and not the more fundamental requirements of the Privacy Act. The Privacy Act is of course an important area of this Committee's jurisdiction. That Act forms the principles and program for how the Executive agencies are to acquire, safeguard, use, share, and dispose of personal information pertaining to U.S. citizens. Establishing separate and perhaps incomplete privacy controls and requirements outside the Privacy Act potentially undermines the Act and could create confusion, reducing the effectiveness of the new controls. I encourage the Committee to consider the broader implications of its legislative agenda in this area.

Indeed, given the changes in technology and the world, it may be time to update the Privacy Act of 1974. This major undertaking might usefully be begun by chartering a commission to examine the field and provide recommendations to this Committee.

# # # # #