Testimony of Alan Paller

Director of Research, The SANS Institute

Before the

Subcommittee on Government Management, Organization, And Procurement of the

Committee on Oversight and Government Reform

Hearing on

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

March 24, 2010

Introduction

Chairwoman Watson and Members of the Subcommittee, this is a banner day for information security in government. After more than a decade of waste and lost opportunities caused by flaws in the legislation, the changes you are considering today promise to transform federal information security.

One of the most important goals of any federal cyber security legislation must be to enable the defenders to act as quickly to protect their systems as the attackers can act. We call this continuous monitoring and it is single handedly the most important element you will write into the new law. Continuous monitoring enables government agencies to respond quickly and effectively to common and new attack vectors. The Department of State has demonstrated the effectiveness of this security innovation. Most major corporations use it. This model is the future of federal cyber security. As our response to attacks becomes faster and more automated, we will take the first steps toward turning the tide in cyberspace, and protecting our sensitive information. The original FISMA did just the opposite – it slowed down every process and took key resources away from projects that would allow agencies to act and react more quickly. What you're considering today is not just a new way of doing security, it's a new way of thinking about security; the right way, the only way to win.

I am Director of Research for the SANS Institute, the primary training organization for the front line technologists who battle every day to protect the computer

systems and networks in the global infrastructure. SANS alumni, more than 118,000 in all, are the intrusion detection analysts, security managers, security auditors, firewall analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers in government and industry. Their responsibilities include building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime, tracking down the criminals, and correcting flaws that allowed the attack to succeed. We also run the Internet Storm Center, an early warning system for the Internet, publish the industry's authoritative list of critical new vulnerabilities discovered every week, and develop the consensus of the most damaging new attacks that agencies and companies will face in the coming year.

SANS alumni are the front-line warriors in the constant fight against cybercrime and cyber espionage. Every day, they fight to maintain control of the systems that operate our government and our economy and provide the essential services on which we all depend. The effectiveness of security practitioners who understand how to fight back against cyber attacks have been sorely hurt by FISMA-enabled processes forcing their agencies to spend more on compliance than on actual security. In my testimony today, I will illuminate the multi-billion-dollar errors that were made in the name of FISMA (the Federal Information Security Management Act) and thereby show how critically important your proposed changes will be.

I do not want to over emphasize the war-like nature of the fight, but it does resemble an arms race in that each time the defenders build a new wall, the attackers create new ways to scale that wall. Cyber warfare is not like conventional warfare. In conventional warfare deployment takes time and money and is quite visible. In cyber attacks, when the attackers find a new weapon, they can attack a few key machines or millions of computers, and successfully infect hundreds of thousands, in a few hours or days, and remain completely hidden.

Four terribly damaging processes were institutionalized in the aftermath of FISMA and GISRA (the Government Information Security Reform Act that predated and is essentially the same as FISMA). These wasteful processes slowed down our defenses and threw away billions of dollars that were acutely needed to protect systems. They forced federal chief information officers to defer investments in enterprise security because their security budgets were being consumed buying 3-ring binders full of reports that were out of date when delivered and had no discernible impact on security.

To implement GISRA and FISMA, the government created a and audit process that regularly results in misleading reports to agency heads and Congress. That flawed process was adopted by the Inspectors General, as well, who also are producing reports that answer the wrong questions.

GISRA and FISMA rewarded ineffective behaviors and created a cadre of people who call themselves security professionals but who proudly admit they cannot implement security settings on systems and network devices or find a programming

flaw. Most of these paper-warriors have no depth of understanding of current threats, cannot do an effective risk assessment, nor select the right controls to protect systems against the increasingly sophisticated attacks.

If the federal government were the only organization being impacted by the FISMA-flaws, that would be bad enough. But increasingly state governments, radically short of money, are being forced to spend scarce funds on reporting rather than security. Even worse, the electric power industry has been caught up in the culture of compliance created by FISMA. The head of security at a major southern power company told me last Friday, "I had to hire a writer rather than a security person because writing compliance reports is seen by management as more important than actually securing the systems." FISMA has perturbed the entire security job market. In the federal contractor community, writers who know a few words about security and federal regulations now make 50-80% more money than the people who actually secure systems and networks and applications. It is as if we paid the compliance staff at a hospital more than we pay surgeons. The best and brightest technical people are being forced into compliance roles because they want to keep their jobs and earn more money.

This wasteful behavior had to stop. Your new bill will go a long way toward stopping the damage.

Flawed Processes

The four processes that were created in the aftermath of FISMA and caused so much waste were:

(1) The FISCAM (Federal Information System Controls Audit Manual) audit process.
(2) The annual report process implemented by CIOs and IGs under FISMA.
(3) The certification and accreditation report-writing process.
(4) The security controls assessment process under Special Publication 800-53.

In each of these areas the authors knew their work needed improvement and they made small positive steps over the past year, but the FISMA language kept them from making the big steps needed to make federal information security effective.

The damage done by numbers 2, 3, and 4 have been well documented elsewhere. For example Senator Carper, Chairman of the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, said in a hearing on this same topic:

> *"one wasteful and ineffective area . . . is known as the 'Certification and Accreditation' process." "If we look at the chart to my right, we can see three years worth of reports from the Department of State, which cost a*

total of $38 million dollars. These reports would be worth the price tag if the tactics that hackers used were as static as words typed on a piece of paper. But hackers change how they attack us daily and their numbers continue to grow. Billions of dollars are spent ... on ineffective and useless reports, similar to the ones pictured here." (http://www.votesmart.org/speech_detail.php?sc_id=505326)

Senator Carper did a great service to the country by illuminating the key problem of trying to use static and out-of-date reports to fight a dynamic adversary. This happens because the people who wrote FISMA, and the people who set up these wasteful processes did not and do know how the attacks are being carried out and how the threat is changing, so they ask the wrong questions. Their mistakes force agencies to focus resources on the wrong problems (generally problems that were most important a decade or more ago) and use up money that should have been target on more important activities targeted toward the current threat.

The one FISMA/GISRA-caused process that has not been widely discussed previously is the FISCAM audit process. GAO and the Inspectors General are powerful forces for good in this country. When they are forced by a flawed audit guide to ask the wrong questions, then they force agencies to spend scarce security money on the less important defenses, taking money away from what matters, and the country is less secure.

The following table shows evidence of how a recent FISCAM-based audit missed the most important controls. The table lists critical controls in the Consensus Audit Guidelines (CAG) published by the Center for Strategic and International Studies. These are the controls identified as most critical by the people who best understand the attacks (the NSA, US-CERT, the DoE Energy Labs, DoD Cyber Crime Center and others in government and the private sector who do the forensics to clean up after attacks and who actively penetrate systems on behalf of the nation.)

Sample Critical Controls Assessment Vs November 2009 FISCAM-Based Audit

(This is just four of approximately fifteen similar comparisons that will be published shortly with far more data, so agencies and auditors can see how to improve the processes.)

Critical Control (and sample test)	**Why It Matters**	**Was The Test Performed?**
Inventory of Authorized and Unauthorized Devices (sample test: determine how long it takes unauthorized systems to be recognized)	There is no way to manage a computer if you don't know it is there	NO
Secure configurations on operating systems (sample test: Install a	Vendors sell systems with weak configurations and	NO

system with a nom-FDCC compliant operating system and measure how quickly to agency finds and corrects the problem)	software vendors reset configurations; agencies have to harden the systems to stop attackers from do extensive damage to many systems	
Boundary defense (test: send a standardized set of benign attack traffic to random systems and test ability to block the traffic.)	Traditional firewalls do not stop the sophisticated attacks. The doors are wide open to attacks.	NO
Application Software Security (test: use both types of software testing tools on random applications to test the agency's application security effectiveness)	Federal web sites have been changed so they infected the computers of members of the public who visited the site.	NO

The Bottom Line

Both the guidance for implementing FISMA and the guidance for auditing compliance are focusing on out of date, ineffective defenses. What we need instead is a process that directs agencies to focus their cyber security resources on monitoring their information systems and networks in real time so that they can prevent, detect and/or mitigate damage from attacks as they occur. And oversight must be focused on the effectiveness of the agencies' real-time defenses. The bill that you have introduced, Madam Chair, does exactly that. Anything less continues to waste scarce resources and leaves us unacceptably vulnerable.

Thank you. I will be happy to answer any questions that you or other members of the subcommittee may have.

About Alan Paller

Alan Paller is founder and research director of the SANS Institute, a graduate degree granting college and security training and research institution with more than 118,000 alumni. At SANS, he oversees the Internet Storm Center (an early warning system); NewsBites, (the semi-weekly security news summaries that go to 210,000 people), @RISK (the authoritative summary of all critical new vulnerabilities discovered each week), and the identification of the most damaging new attacks being discovered each year. In 2000 President Clinton recognized his security leadership by naming him as one of the initial members of the President's National Infrastructure Assurance Council. The Office of Management and Budget and the Federal CIO Council named Alan as its 2005 Azimuth Award winner, a singular lifetime achievement award recognizing outstanding service of a non-government person to improving federal information technology. He has testified before both the House and Senate multiple times. Earlier in his career he helped build a software company and merged it into a larger company listed on the New York Stock Exchange.