Testimony of Alan Paller[1] of the SANS Institute[2]
Before the U. S. Senate Committee on Homeland Security and Government Affairs

Cyber Security: Developing a National Strategy
April 28, 2009

A Brief Summary:

Our nation is facing a wave of increasingly sophisticated cyber attacks that overwhelm the defenses established under the GISRA and FISMA legislation. Congress can reduce the threat of damage from these new cyber attacks both against government and against the critical infrastructure by shifting the government's cyber security emphasis from report writing to automated, real-time defenses implemented through strategic use of the $70 billion of annual federal IT buying power. DHS cannot make that happen; only active White House leadership will get the job done.

Five Findings That May Help Inform Congressional Options in Cyber Security

Part I: Defining the Problem

1. Hackers and nation states have more deeply penetrated civilian government agencies and the critical national infrastructure computer networks than the public and most members of Congress have been told.
2. The attackers are improving their techniques far faster than the US government is improving its defenses. In other words, the threat is increasing at an accelerating rate.

Part II: Promising Options Than Can Turn the Tide Against the Attackers

3. There is strong evidence that federal cyber security can be radically improved through strategic use of federal buying power.
4. Four huge unintended errors make it almost impossible for agencies to make big improvements in IT security. This Committee can fix all four.
5. If you do make these corrections in government, you will, at the same time, be making cyber security much more effective for the critical national infrastructure and the general public.

Part I: Defining the Problem

1. Hackers and nation states have more deeply penetrated civilian government agencies and the critical national infrastructure computer networks than the public and most members of Congress have been told.

Testimony before the House Homeland Security Committee in April 2007 revealed that both State Department and Commerce Department computers had been penetrated, most probably by government-funded actors in China. Although the State Department found the attackers and rooted them out, a Commerce official testified that the department did not know how long the attackers had been controlling department computers nor did they know how far and wide the infections had spread. As a result they had no confidence that the attackers' hold on their systems had been broken. The question of why any nation-states would want to control Commerce Department computers is worth considering. The part of Commerce that was attacked, the BIS division, or the Bureau of Industry and Security, decides which technologies are too sensitive to be exported. Commerce keeps all the data a nation state needs to determine each new technology that matters to us, why it is sensitive, how it works, and who is developing it – giving the attacker a near-perfect roadmap to steal the sensitive technology itself through further attacks on the commercial developers' computers. The defense industrial base is also weak in cyber security, as Time Magazine's 2005 disclosures about the Titan Rain attacks proved, but we'll get back to that later.

State and Commerce attacks were widely reported. What has not been reported is the number of additional sensitive federal agencies that have been just as deeply penetrated by the same attackers. In one department, I was told privately, the damage was so widespread that the department's CIO had to invite the NSA Blue Team experts in to help isolate and eradicate the problem. Additional private communication with cyber security and IT managers in government leads me to conclude that nearly every militarily and economically sensitive element of the government, including the offices of important Congressional Committees, have now been penetrated, sensitive data taken, and in many instances back doors are still open for those attackers to return at will to gather or change information.

One example of this kind of manipulation, and the vulnerability in federal defenses was discovered in a Department of Homeland Security Web site where visitors were redirected to a site set up to take over the visitors' computers. The malicious sited attempted to place keystroke loggers on those unsuspecting citizens' computers and to use the data from the keystroke loggers to steal money from bank accounts or stock trading accounts.

But weaknesses in government cyber defenses are only a third of the problem. A second area that deserves this Committee's attention is the degree to which government contractors and the defense industrial base have also been deeply penetrated, with grave effects.

Government relies on contractors to build and sometimes operate its military and civilian systems. Forbes magazine, Business Week magazine and the Wall Street Journal have revealed that nation states using the same types of advanced attacks used to penetrate government computers successfully attacked computers at key defense contractors. The victims are many of the same contractors that charge hundreds of millions of dollars to tell the government how to secure federal systems.

What has not been reported is that those same contractors have lost some of America's most sensitive new technologies -- and I have been told that those nation states already have put these new technologies to use.

The final important objective, beyond the government, contractors, and the defense industrial base, is protection of the critical national infrastructure, such as the electric grid, the financial system, and the Internet itself. A few weeks ago Americans awoke to learn that the computers that control electric power generation and distribution had been penetrated, most probably by unfriendly nation states. What was not reported was that those same utilities' control systems had been taken over before, by another nation state, and because of the sensitivity of the sources of that information, most utility executives are totally in the dark about those earlier (and probably continuing) infections. We now also know that there are ways to use remote network access to disrupt the power – for days, weeks or even longer. Internet-based attackers have already remotely cut the power in multiple cities outside the US as part of cyber extortion schemes in which they apparently demonstrated their remote control of the power systems in order to collect large amounts of money.

2. The attackers are improving their techniques far faster than the US government is improving its defenses. In other words, the threat is increasing at an accelerating rate.

Three types of highly-motivated and well organized groups are behind this acceleration: nation states looking for strategic information and advantage, organized crime groups looking for profits, and terrorist groups looking for political gain.

China, as just one example, runs a national competition for college and grad school students who may currently be hacking illegally, but who could be effectively employed in creating and using new attack techniques. In 2005, for example, Tan Dailin, a graduate student at Sichuan University who was found hacking into Japanese computers, was recruited for the "Chengdu Military Militia Information Sub-Unit Network Attack and Defense Contest." His team won and, after attending an intensive 16-hour-per-day, 30-day workshop to learn to develop sophisticated attack techniques, his team also won a larger multi-regional competition run by the People's Liberation Army (PLA). The team won 20,000 RMB and set up a company to develop and deploy new attack techniques. By December Tan's signature was found in several hacks into the US DoD. In the summer of 2006, his hacking crew was found to be behind a half-dozen zero-day exploits of Microsoft PowerPoint and Excel used to great effect to penetrate sensitive commercial, military and civilian government sites all over the world and steal tens of thousands of documents. The PLA's competition continues to recruit and develop ever improving talent.

At the same time, organized crime groups in Eastern Europe use money and lies to recruit some of the most sophisticated hackers, and then use terror (credible threats of killing their families) to keep them working even when they decide they do not want to be criminals. These organized crime groups earn hundreds of millions of dollars from cyber crime every year. In one recent case, an organized crime group stole more than $10 million from ATM machines in less than 30 minutes, using stolen data to replicate 45 customers' ATM cards and active control of the bank's computers to increase the withdrawal limits on each of the accounts. The thefts stopped only when the targeted ATMs ran out of cash. With all their money, organized crime groups can afford to pay huge amounts to acquire the best talent and build increasingly powerful new attack tools.

Terrorist organizations also have run hacking schools in Afghanistan and in other countries and use other methods to teach their recruits to hack into computers. On October 12, 2002, Imam Samudra, a senior Al Qaeda operative, planted bombs that killed 202 people including 164 young Australian and New Zealand vacationers on the Indonesian island of Bali. Before he was executed earlier this year, Samudra, known as the "Bali Bomber" wrote his autobiography detailing how others could benefit from hacking. He was a hacker in addition to being a mass murderer. In a chapter in his autobiography called "Hacking, Why Not?" Samudra wrote, "If hacking is successful, get ready to gain windfall income for just 3 to 6 hours working, greater than the income of a policeman of 6 months work. But, please do not do that in the sake of money alone! I want to give motivation to the youth and men who are granted perfect mind by God. I want America and its cronies to be crushed in all aspects." Samudra used hacking to raise money for his cause; we know because one of our graduates in Australia did the forensics on his computer. His chapter on hacking revealed a remarkable understanding of how new recruits can develop the advanced hacking skills needed to break into seemingly sophisticated networks.

The CSIS Commission Report on Cybersecurity for the 44th President has additional examples of the damage that is being done to the nation through cyber attacks and the CSIS proposals for a more effective national strategy are right on target. The remainder of my testimony focuses on two of those proposals that I believe are most in need of this Committee's early action.

Part II: Promising Options Than Can Turn the Tide Against the Attackers

3. There is strong evidence that federal cyber security can be radically improved through strategic use of federal IT buying power.

The most illuminating and encouraging story in federal cyber security is the one that began six years ago when the NSA red team was briefing the CIOs of the Army, Navy, Marines, and Air Force. Red teams test security by attempting to break into networks. NSA's red team was able to penetrate the four military services' systems quickly. The only good news for three of the CIOs was that it took longer to break into their systems than into the fourth CIO's systems.

John Gilligan, CIO of the Air Force at the time, took one of the key NSA executives aside and said, "We will fix every problem you found, but we know you'll come back in a few months and break in just as fast. You are not helping us. Can you get your best attackers together and tell us the most important things we should do, across the Air Force, to make it much harder for you and other attackers to break in?"

NSA agreed and came back saying that when their red teams get in quickly, it is nearly always because of configuration and patching errors. Mr. Gilligan asked if NSA could help the Air Force develop a standard configuration that would block at least 85% of all attacks and still allow Air Force computers to work well. NSA did, with help from DISA and the Air Force and Microsoft. The Air Force has deployed that standard configuration across more than 500,000 computers. In the process, the Air Force saved more than $100 million in procurement costs, that same amount annually in operational costs and tens of millions more in energy costs (because the standard configuration allowed power-saving use without impacting performance.) But even more important is that security patches are now installed in less than 72 hours, instead of the 57 days it took before. And surprisingly, the users are much more content – with help-desk calls reportedly down by 50%.

So here we have a case where security was radically improved, costs were lowered, and the users are happier, as well. Other federal agencies and commercial companies are following in the Air Force's footsteps, deploying that same set of configurations. The federal government's leadership-by-example led Microsoft to make a much more secure configuration template available to many more organizations without charging them any more money.

The Air Force case offers three key lessons:

First, effective defenses can be designed only by people who have comprehensive understanding of how attacks actually work. This is the theme echoed often by Melissa Hathaway of the National Security Council when she says, "Offense must inform defense." Mr. Gilligan has repeatedly said that the Air Force standard configuration project would never have worked were it not for NSA's willingness to translate its understanding of attack techniques into defensive configurations. One of the most common reasons for the federal government's security failures is reliance on the security advice of people who do not know how attacks are executed.

Second, only massive procurement power can persuade vendors to deliver safer systems rather than the standard systems they sell at retail to businesses and consumers. Dozens of customers had asked Microsoft for more secure configurations and all were refused or were asked to pay large amounts of money for consulting services to develop customized settings. The Air Force was about to spend $500 million on Microsoft software over six years. That was enough to get the company to deliver systems with secure configurations baked in, to make it available across all of government, and to build infrastructure to support the Air Force and other users of the secure configurations. When vendors are able to make large sales, they will often lower the costs for each user. This was proven in the GSA/DoD encryption purchase in which software that cost $243 retail and $97 under GSA contract was purchased by the Department of Agriculture, in large volume, for less than $12 and by DoD for less than $6. The vendors still make a great deal of money because the volume is so high. Despite Federal Acquisition Rules that require security to be baked into procurements at the beginning, most times it is not. There are no penalties or even checks and balances to ensure security is part of the acquisition strategy. Microsoft's support for the Air Force should be a model for other operating systems and other software widely used by the government. Microsoft, with support from DoD and the NSA, recently issued secure server configurations, as well, extending the desktop benefits more deeply into the network.

Third, the most important ingredient in effective security automation is integration with IT automation. The Air Force success in reducing patch time came from baking security into every system configuration and into its automated IT management process. Under attack, the Air Force can change the configuration of nearly every system in minutes. That doesn't happen in agencies where security is considered a separate responsibility from effective IT management. Thus effective security in today's threat environment is a CIO responsibility – not one that can be delegated to a security officer. Only the CIO has the resources, authority and tools to implement enterprise-wide configuration management and other automation measures so critical to security.

4. Four huge unintended errors make it almost impossible for agencies to make big improvements in IT security. This Committee can fix all four

Error 1. We're measuring security the wrong way.

The predecessor to the Federal Information Security Management Act (FISMA) was written by this committee in late 2000 (under the name GISRA). It was a powerful force for improved visibility for security across government. That law, along with a continuous flow of news stories about viruses and worms, awakened government to the security issue. Once the government realized the extent of the cyber problem, it needed to act. Your committee had set a sunset date after two years. By 2002, when the law came up for reauthorization, it was time to shift from writing reports about security problems to implementing effective security solutions – based on knowledge about how the attacks work. One small change was implemented in the 2002 FISMA bill, requiring agencies to establish standard configurations. That one change did a great deal of good and actually enabled the Air Force to implement its game-changing secure configurations and other agencies to begin following the Air Force lead. But now the attacks have become much more sophisticated, and FISMA needs an even greater update. The need is supported by repeated testimony of the GAO's Greg Wilshusen in which he says that the current FISMA reporting does not measure security effectiveness.

You can make FISMA much more effective by empowering OMB to measure agencies on how well they implement and automate the controls that stop known attacks, and how well they demonstrate effectiveness in identifying and mitigating damage from attacks that get through their defenses. Reporting can be an artifact of effective automation. Progress and effectiveness should be monitored, to the maximum extent possible, electronically. The State Department CISO and CIO have begun implementing such a system – they can show other agencies how it can be done.

However, federal agencies cannot move effectively to more secure systems unless you shift the emphasis of the FISMA assessments from paper reporting to automated monitoring of essential controls. If agencies are asked to implement critical controls and to automate reporting but still are forced to produce the current FISMA paper reports, they just won't be able to do so. Two weeks ago, a federal CIO told me, "I have a CISO who always gets me to green on my FISMA grades, but the reports he produces have no impact at all on security of our computers or networks, I am setting up a separate group to do real security." This CIO can do both because of a surge of funding his organization has received from the new stimulus bill. Most CIOs do not have enough money to pay for both the FISMA reports and the important security improvements.

This committee can fix that error by authorizing and empowering agencies to move to continuous monitoring of critical controls. In moving the agencies to continuous monitoring, the most valuable asset this Committee could give the agencies is a legislatively approved way to answer the questions the Air Force asked NSA: what are the most critical controls that must be implemented first to ensure government systems are protected from known attacks and that can mitigate damage from attacks that get through? And how can agencies measure those controls reliably? You can make that happen simply by telling DHS, through US-CERT, to produce that list (with help from NSA), along with measures of effectiveness, and to keep it up to date. Only US-CERT and NSA have sufficient combined knowledge of how attacks work to make the answer useful. A project led by John Gilligan (the Air Force CIO who did so much to improve security), and sponsored by the Center for Strategic and International Studies, is already helping get such a list started. Mr. Gilligan brought together experts from US-CERT, NSA, the Department of Energy Nuclear Labs, and DoD agencies that understand offense, to define the 20 most critical security controls and to draft a consensus audit guide (CAG) that could be the starting point for transforming federal cyber security. If the government leads the way, the defense industrial base and the critical national infrastructure will willingly follow. They want to stop the attacks just as much as the government does.

Error 2. Missing the opportunity to use federal procurement to buy security "baked-in'."

Technology buyers cannot cost-effectively secure technology they purchase. Had the Air Force staff tried to implement the critical security configurations changes itself they would have had to change the configurations of 500,000 computers, one by one. The cost would have been astronomical even if the skills had been available. Instead, they purchased computers with the secure version of Windows already installed.

Further, most users of technology are unwilling to make changes to systems - even critical security changes - because they fear the changes will disable important features. Only the people who build and sell technology to government can configure that technology securely. The $70 billion in annual federal IT spending is enough to get radically better security baked-in, but most agencies - other than the Air Force - are not yet using that procurement leverage to ensure systems come with security baked in. Every new contract that is let, without specific security language in the contract specifications, is another opportunity lost and another boost for our country's enemies.

There is a particularly troubling example of this problem plaguing agencies right now. Many agencies are hiring contractors to develop web sites, often to give the public access to information about their parts of the new stimulus bill. The contractors employ programmers who do not write secure code, or who use existing code building blocks which haven't been fully vetted for security purposes, and deliver flawed web sites that may cause the agency to lose data and or even to infect visitors who come to their site. When the agency discovers the problem and tells the contractor, the contractor usually charges the agency to fix the contractor's own programming errors. In some cases the extra charges are greater than the cost for writing the original, flawed application.

This Committee can help solve this problem by instructing agencies to specify security elements in every procurement and task order. The minimum set of requirements would be that the application is configured securely, operates effectively on securely configured versions of operating systems and databases, and is free of the NSA/Mitre/SANS Top 25 most dangerous programming errors. Putting that language in the Federal Acquisition Regulations (FAR) will not work. If the requirements are not in the specific language of each contract, most contractors will not implement them.

Error 3: Allowing the claim, "one size does not fit all," to derail purchases of more secure technologies

When the government tries to use its procurement power to buy software at better prices and with security baked in, vendors often scream. "One size does not fit all." And it usually works. BUT It's wrong!

Microsoft sells one size of Windows to tens of millions of people. Cisco sells one size of IOS (Cisco's operating system inside each of its routers) to hundreds of thousands of people. Oracle sells one size of its database to tens of thousands of people. Hundreds of vendors sell only one size. One size, to all these vendors, clearly fits all.

By using federal procurement to buy securely configured systems, you do not constrain agencies from innovation or from making modifications. Instead you make them safer from the outset. The Air Force proved that. Loud claims to the contrary were dead wrong. Your Committee can encourage other agencies to do so, as well.

Error 4: Expecting DHS to manage security across the civilian government without active support from a White House Cybersecurity office.

Civilian government agencies do not work on a command and control basis across agencies. If someone from one agency tells someone from another agency to implement an action, (regardless of legislative authority), the person in the second agency is likely to say "I don't work for you. If you want me to do that, have your Secretary call my Secretary and then, when I get word from my boss, I'll think about doing what you ask." You need look no further than the federal agencies' Conficker response earlier this month, for a telling example. When the US-CERT requested status reports on important mitigation actions from the agencies, their requests were met with silence from the majority of agencies. US-CERT may have provided excellent information, but US-CERT was unable to determine whether the agencies acted effectively on that information. When an attack starts to cause real damage, that lack of control will be catastrophic.

The bottom line is that without a White House office actively and intelligently forcing the agencies to work well together, and to spend money on the right security controls, DHS will fail in its federal cyber security role. That office must have command and control over civilian federal computers in time of emergency, but there is no need to place DoD cyber security under that White House office. At DoD command and control is already in place and works reasonably well. The White House cyber security office would implement its operational control over civilian agencies only when national emergency events occur, or when agencies need to act to be ready to respond to such national security events; otherwise it would play a coordinating and monitoring role working through other parts of OMB. Unless you put the power to reconfigure and unplug computers and networks in the hands of a White House office, the nation will not be able to respond quickly or effectively to a major cyber attack.

5. If you do make these corrections in government, you will, at the same time, be making cyber security much more effective for the critical national infrastructure and the general public.

The Air Force procurement has led Microsoft to bake security into the products it sells to many other buyers. A large part of the nation's infrastructure assets are run by companies and operations that use many of the same business, database, and web applications that the government uses. If vendors step up to meet minimum government mandates on security, there will be a critical ripple effect on software development and security practices used by the private sector companies.

So if those mandates are made clearer, and agencies are authorized and empowered to purchase more secure technologies, and to automate the monitoring of critical security controls, the committee in effect will be serving to prime the pump of broader adoption of effective security practices.

In Closing

Many useful cyber security initiatives were started during the past eight years – from the common secure desktop configurations, to the information security line of business, to DNS security, just to name three. But they are not nearly enough. CSIS concluded accurately, “America’s failure to protect cyberspace is one of the most urgent national security problems facing the new administration. It is a battle fought mainly in the shadows. It is a battle we are losing.”

The key to turning the tide against the attackers is strategic use of federal IT procurement. If procurement is not fixed, nothing else really matters.

[1] Alan Paller

Alan Paller is the director of research for the SANS Institute, responsible for the Internet Storm Center (the Internet's early warning system with 500,000 sensors around the world) and SANS' other consensus research projects such as the summary of the most critical new vulnerabilities discovered each week. He chairs the Application Security Summit and the SCADA Security Summit and edits NewsBites, the summary of the most important news stories in security that goes to 205,000 people twice each week. He says his most satisfying activity is finding people who have solved important security problems and helping others learn about those people and their discoveries. In 2000, President Clinton named Alan as one of the original members of the National Infrastructure Assurance Council. In 2005 the Federal CIO Council chose him as its annual Azimuth Award winner recognizing his singular vision and outstanding service to federal information technology, and in 2009 Alan was selected as one of the Fed100 winners. Earlier in his career Alan was one of five entrepreneurs who built the first large computer graphics software company that earned listing on the NASDAQ exchange and then merged it into a New York Stock Exchange company. He is the author of "The EIS Book: Information Systems for Top Managers" (Dow Jones, 1990) and "How to Give the Best Presentation of Your Life" (ISSCo, 1981). Alan earned degrees in computer science and engineering from Cornell and MIT.

[2] The SANS Institute

SANS is the largest source for information security training and certification in the world, with more than 95,000 alumni in 66 countries. SANS is also a degree granting institution licensed to grant Master of Science degrees in Information Security Engineering and Management.

SANS courses teach how to do the essential tasks necessary for securing modern systems and networks. Among its fifty courses are SANS Security Essentials; Intrusion Detection In-Depth; Network Penetration Testing and Ethical Hacking; Web Application Penetration Testing; Computer Forensics, Investigation and Response; Reverse Engineering Malware; Secure Coding in JAVA; Secure Coding in .NET; Securing Windows; Wireless Ethical Hacking and Penetration Testing; Hacker Techniques, Exploits, and Incident Handling; Log Management In-Depth; Introduction to Information Security; and Auditing Systems and Networks.

The SANS (SysAdmin, Audit, Network, and Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 225,000 security professionals around the world each week. A range of individuals from auditors and network administrators to chief information security officers and CIOs use SANS to share the lessons they learn and to find solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations, from governments to corporations to universities, working together to help the entire information security community.

Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center (the Internet's early warning system), the bi-weekly news digest (NewsBites), the weekly vulnerability digest (@RISK), flash security alerts, security policy templates, monthly online threat updates, case studies of what works in a dozen categories of security tools, draft procurement language for buying security baked into applications, and more than 1,200 original research papers written by security practitioners as part of their SANS certification and degree programs.