Testimony of Alan Paller

Director of Research, The SANS Institute

Before the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Hearing on

"Protecting Cyberspace as a National Asset: Comprehensive Legislation for the 21st Century"

June 15, 2010

Chairman Lieberman, Ranking Member Collins, Senator Carper and Members of the Committee, you made last Thursday a very good day for improving the security of our nation. On that day, you introduced Senate Bill S 3480, and began the process of transforming federal information security so that the government can lead by example in making America's computers and networks much safer than they are today.

In support of that goal, my written testimony has two sections: one shows how much trouble the nation is in and exactly how the legislation you present enables the nation to correct the errors that got us into that trouble in the first place, and (2) what effective cyber security means, including how innovative federal employees and organizations are demonstrating that effective security can be implemented in government. This second part includes some small adjustments in S 3480 that would enable it to be more effective in transforming cyber security. The testimony also illuminates the misleading arguments put forth by interest groups determined to delay the critical improvements that your legislation enables, because it suits their own economic interests.

Part 1: How Much Trouble is the U.S. In? And Why?

Our country is by far more dependent on the Internet than its adversaries.; several of whom may be able to disconnect their systems from the Internet for a time and still operate; we cannot. That means our cyber defense must be near perfect. It is not even close. The systems that most Americans and American enterprises purchase and deploy on the Internet are full of programming errors that adversaries exploit to gain access and install remote control tools, or what General Alexander, Commander of the US Cyber Command, calls “remote sabotage tools.”

According to the Commander of the Navy’s 10th (Cyber) Fleet, Adm. McCullough, flaws and remote control tools could very well compromise our control over kinetic weapons. The US has a major advantage over its adversaries in that it can destroy enemy assets using missiles, bombs, planes, ships, artillery, and bullets. But that lead, says Adm. McCullough, disappears “if I don’t own my command and control computers.” While adversaries invest more in cyber weapons and cyber talent, the US keeps increasing our investment in kinetic weapons, and paying lip service to the cyber skills that will keep them within our control. “We are on the wrong side of the cost curve,” Admiral McCullough added.

Seven weeks ago, the Deputy Assistant Director of the FBI for Cyber provided a bracing description of the nation’s cyber risk. The cyber threat “can challenge our country's very existence,” said Steve Chabinsky. "How we rise to the cybersecurity challenge will determine whether our nation's best days are ahead of us or behind us.” Vice Admiral Mike McConnell, Director of National Intelligence under President George W. Bush, had already put a fine point on the problem, telling the Senate Commerce Committee on February 23, 2010, “If we went to war today in a cyberwar, we would lose.”

This is not just a problem in our military systems. The critical infrastructure on which we are so reliant and, indeed, the intellectual products that are critical to our place in world markets are in jeopardy. Computer systems supporting electric power generation and distribution are already infested with those remote control infections described by General Alexander, as are computers in federal and state government agencies.

The US is also losing its most sensitive intellectual property – the foundation of our nation’s economic and strategic advantages. A Commerce Department official testified to a House of Representatives panel in the aftermath of a cyber attack where the Chinese stole extensive technical data on all US technologies too sensitive to be exported. The official said that he and his experts had no idea how far the infections had spread through the Agency’s computers nor whether the infections had been found and removed.

Cyber attackers also penetrated the defense industrial base multiple times over several years. In one case, the target was a major defense contractor’s computers, where sophisticated attackers made off with electronics and design data on advanced weapons that were to be deployed on the Joint Strike Fighter, America’s most expensive weapons system costing American taxpayers around $300 billion. According to the Wall Street Journal, “Six current and former [federal] officials familiar with the matter confirmed that the fighter program had been repeatedly broken into.” The defense industrial base is the most valuable and fertile target for nations that want to steal military technology data rather than fund their own technology research.

Additionally, an epidemic of intellectual property cyber theft is plaguing companies and their law firms and their consultants, especially those doing business with Asian nations. You heard in January about the successful attacks on Google, Intel, Adobe, and Yahoo, resulting in the loss of extremely valuable intellectual property. They are not alone. Although US companies never were told of the scale of the threat, and who was at risk, British companies were. The head of MI-5 (the UK Security Service) sent a letter to the managing directors of the 300 largest companies in the United Kingdom in late 2008. The letter said that if they are engaged in any negotiations or business with a major Asian power, they are being attacked with the same cyber weapons that are used against military targets. The attackers' goal is economic advantage – to give their own countries' companies a leg up in negotiations or even eliminate the need to negotiate at all since they can get the valuable intellectual property through cyber exploits. That letter also told the British companies that their law firms were being targeted. Many hundreds of US companies have had their systems penetrated and their data stolen and remote control software installed. Some of the largest US law firms have been deeply penetrated with their entire databases of all client records having been stolen.

US government sites have been infected and used in criminal activities. Computers at the Department of Transportation delivered pornography for several weeks. News articles reported a web site at the Department of Homeland Security was sending Trojan horse software to web visitors' computers in an attempt to take over those computers and use them in financial cyber crimes. While some of these crimes are for financial gain and some just for what seems to be mischief, they demonstrate the extent of our vulnerability.

Cyber crime is also lucrative for terrorists – to get money to buy the bombs to kill innocents. Imam Samudra, the Bali Bomber, who exploded a bomb and murdered 200 young vacationers from Australia and New Zealand in October 2002, used cyber crime to get money to buy bomb-making supplies. He wrote his autobiography while on death row. In it, he gave Al Qaeda recruits detailed instructions for using cyber crime to "make more money in a few hours of work than a policeman can make in three to six months of work." He went on to say, "Please do not do that in the sake of money alone! I want America and its cronies to be crushed in all aspects."

How Did the Nation Become So Vulnerable?

The government and critical infrastructure organizations are terribly vulnerable because, in their successful quest for automation, they unknowingly purchase and deploy computer software and hardware that have design flaws and software bugs. Those vulnerabilities enable cyber spying and cyber crime, most of which could have been avoided. But, instead of working cooperatively with the IT industry to limit the risk and minimize the damage, agencies spend billions of dollars paying consultants to write reports that are out-of-date before they are printed and that have no substantial effect on reducing the security vulnerabilities. To demonstrate how important Senate oversight can be, this multi-billion dollar waste was uncovered by Senator Carper and his staff and illuminated in a Senate hearing last fall. His work has already moved the White House to begin reshaping federal cybersecurity, but your bill is still needed to empower and accelerate that change.

The continuing financial waste that Senator Carper uncovered amounts to about $400 million each year. That's enough, when combined with innovative use of federal IT procurement, to fund government-wide implementation of near-real-time situational awareness. In other words, if the bill you are considering is passed, and if you continue the kind of oversight Senator Carper demonstrated, the agencies will have enough savings from avoiding manual reporting to pay for the automation needed to significantly reduce their cyber risk.

Did the Old FISMA Actually Cause the Problem?

Here's the evidence. It begins with one of the contractors explaining why his company produces the "useless" reports and then tracks the authorities all the way back to FISMA.

(1) Mike Jacobs served as Information Assurance Director at NSA. When he retired from the NSA, he took a management role at a government contractor where he oversaw the work of 200 consultants who produced FISMA reports. He told a group of retired federal officials and his own staff, "You know, the only reason we write those stupid reports is that our government customers demand them."

(2) Government CISOs are the "government customers" who hire the contractors to write the FISMA reports. The CISOs told me repeatedly the reason they spend the money to produce the reports is that OMB demands that they do them. If they don't produce the reports, their Departmental deputy secretary will get chewed out by the OMB folks, and he'll come back and task the CIO and CISO with doing them. The pressure to pay for expensive reports causes real problems for the CISO. A CISO in one large agency told a reporter in 2004 that FISMA reporting was already consuming such a large part of her budget that she did not have the funds needed to build stronger defenses. Other CISOs repeat that statement in private.

(3) But why don't the CISOs fix the problem by focusing their limited funds on the most critical controls that can actually reduce risk rather than produce voluminous reports covering lots of old, less critical information? "Because," the CISOs say repeatedly, "FISMA states that NIST standards and guidance are mandatory. " That empowers the Inspectors General and OMB staff to demand CISOs do everything in the NIST guidance. When you demand that someone perform huge numbers of things, with limited budgets, you get dysfunctional results. One illuminating example is the department in which a

> full grade was lost on the annual FISMA scoring because the departmental IG demanded that every employee be given security awareness training. A full letter grade was lost because the department hadn't trained all the people who do the gardening and landscaping; meanwhile the IG never checked to see whether all systems were configured securely.

One last question for the dialogue: Since FISMA assigned NIST the unlimited power to set the standards, why did NIST not develop standards that enabled cost-effective vulnerability and risk reduction? The answer is that there are wonderful people at NIST, with great intentions, but most have never secured a computer (at least in the past decade), cleaned up after an attack, performed deep packet analysis or reverse engineering or memory forensics. In other words they don't know how the attacks work so they cannot know how to prioritize their guidance. How could a doctor prioritize treatment for patients if he or she had no experience with what works and what doesn't work? Perhaps even worse, NIST contracts out much of the guidance drafting. The very same companies hired to write the guidance then turn around and charge agencies tens or hundreds of thousands of dollars for reports that comply with NIST guidance, but are out-of-date and not useful.

Does Senate Bill S 3480 Fix the Other Problems With FISMA?

The legislation undoes the central error of FISMA by removing the requirement that FISMA guidance documents are mandatory. Ed Roback, now CISO at Treasury but who led the NIST team that developed most of the guidance documents, stated repeatedly that making NIST guidance mandatory was wrong.

Senate Bill S 3480 also presses agencies to stop spending money on out-of-date reports and instead focus their spending on continuous monitoring and risk reduction. It provides a Senate-confirmed cyber coordinator in the White House with the power to ensure NIST's documents do not mislead agencies into spending money on the wrong defenses. I hope that the White House office can also help focus inspectors general and GAO auditors on the important elements of NIST guidance so those auditors become part of the solution. That same White House office will also help OMB make certain that federal IT procurement ($80 billion per year) is used as an effective incentive for vendors to deliver software and hardware that has far fewer security holes and that is much easier to maintain securely than is currently being delivered.

Sadly, there are highly paid antibodies at work in Washington, who wrongly see their employers' wealth increasing if the implementation of S 3480 is delayed. That means that the critical changes envisioned by your bill won't happen unless you maintain vigorous oversight through the transition to dynamic, automated security. I'm not worried. You have phenomenal staff, on both sides of the aisle, as do several other committees. If your committee continues to work with the other committees on active oversight, I think you will be extremely proud of what you accomplish in making the nation a much tougher target for cyber attacks.

Other Remarkable Aspects Of S 3480

Four other aspects of S 3480 deserve recognition.

First your procurement and supply chain language is both important and innovative. It is important because the principal vector for positive control of an adversary's computers is to embed code while the technology is being manufactured. Finding hidden code is challenging and will require enormous resources. The issue really needed the language in your bill to raise its priority. It is missing one requirement: testing. You can't find flaws if you don't look for them and you find them by having the suppliers use a suite of automated testing tools that verify everything that can be tested is free of flaws – whether the flaws were accidental or intentional.

The language is also innovative because it avoids the mistake of requiring supply chain language in the Federal Acquisition Regulations (FAR) and instead requires that language to be made part of the actual contract specifications. The FAR demands more than any contractor can do; so, in nearly every case, contractors do what is in the actual contract specifications and hope no one calls them on FAR compliance. It's a strategy that has worked well for at least three decades.

Second, kudos to the drafters because this may be the only bill I have ever seen where a later draft requires fewer reports from the executive branch than earlier drafts. Reports chew up enormous amounts of time of the best people in government, taking them away from the tasks you really want them to accomplish. You have demonstrated a willingness to ask for reports only when you know what the value will be in having the report prepared. I hope other committees follow your example.

Third, the regulatory framework and the emergency measures you establish for the critical infrastructure is long overdue. Without it, there will be no defense of the critical infrastructure in place when a major cyber attack is launched against the United States. One caveat. The structure might not be as effective as it needs to be. Some of the language will lead to long delays in implementing effective defenses. Long delays do not help the nation, they help the vendors that sell IT products and services to government and want government to accept their products as they are without being asked to make sure those products are secure. The vendor representatives (and their associations) are employed by government affairs and marketing departments of vendors that sell billions of dollars of sometimes flawed technology to the government. Their ample salaries are paid for by corporate officers who usually tell them that they have only two jobs in Washington: (1) to make sure the government does nothing that will cost their company money and (2) that if they can find some extra federal revenue for their employer, that's a bonus. Their most effective tool in accomplishing their mission is delay, with their favorite delaying tactic being language in legislation that forces federal agencies to get IT industry review or consult with industry before acting. Notice that this tactic also gives the industry reps access to inside information that their sales people use to tap into new money the government will spend. If you agree the risk is real, perhaps it's time to stop acceding to their delaying tactics.

Fourth, the Manpower section will help DHS build its cyber employee base and help grow the workforce, but it needs one critical change. It calls for training of people with specialized security skills, but has no mechanism to assure the training was effective; that the trainer even knew how to do the job for which the trainees were being prepared and that the trainees came out of the training process with actual hands-on specialized skills to do the job. For too long people could read a book, pass a test and call them selves certified information security professions. Accepting unskilled people for important roles was a major cause of the nation becoming so vulnerable. If you add a requirement to validate the skills of each contractor employee and to prove those skills are the ones needed for each specialized job, you'll have a big impact. Without that, the Manpower section will lead to lots more people employed in cyber security, but without the necessary specialized skills. The best approach is to use procurement language. When the contractors can win new projects only with highly skilled people; they will act quickly to develop the skills the nation needs.

Part 2: Effective Cyber Defense; the Federal Initiatives that Show How It Can Work; and the Ways Private Economic Interests Attempt To Block It

Dynamic Defense

Dynamic defense automates cyber risk reduction and eliminates the manual processes that allowed our nation's networks and systems to become so vulnerable to cyber attack. Our adversaries are far too agile for us to rely heavily, as we have until now, on periodic human evaluations of the state of our systems and networks and human interventions after the fact. A far more effective approach to cyber security is called "dynamic defense." That's what Admiral McCullough, Commander of the 10th (Cyber) Fleet promised the Chief of Naval Operations he would deliver this year.

It has two parts as described by Admiral McCullough:

(1) Near-real-time situational awareness so we can see what is going on in the network just like we monitor an air warfare battlespace.

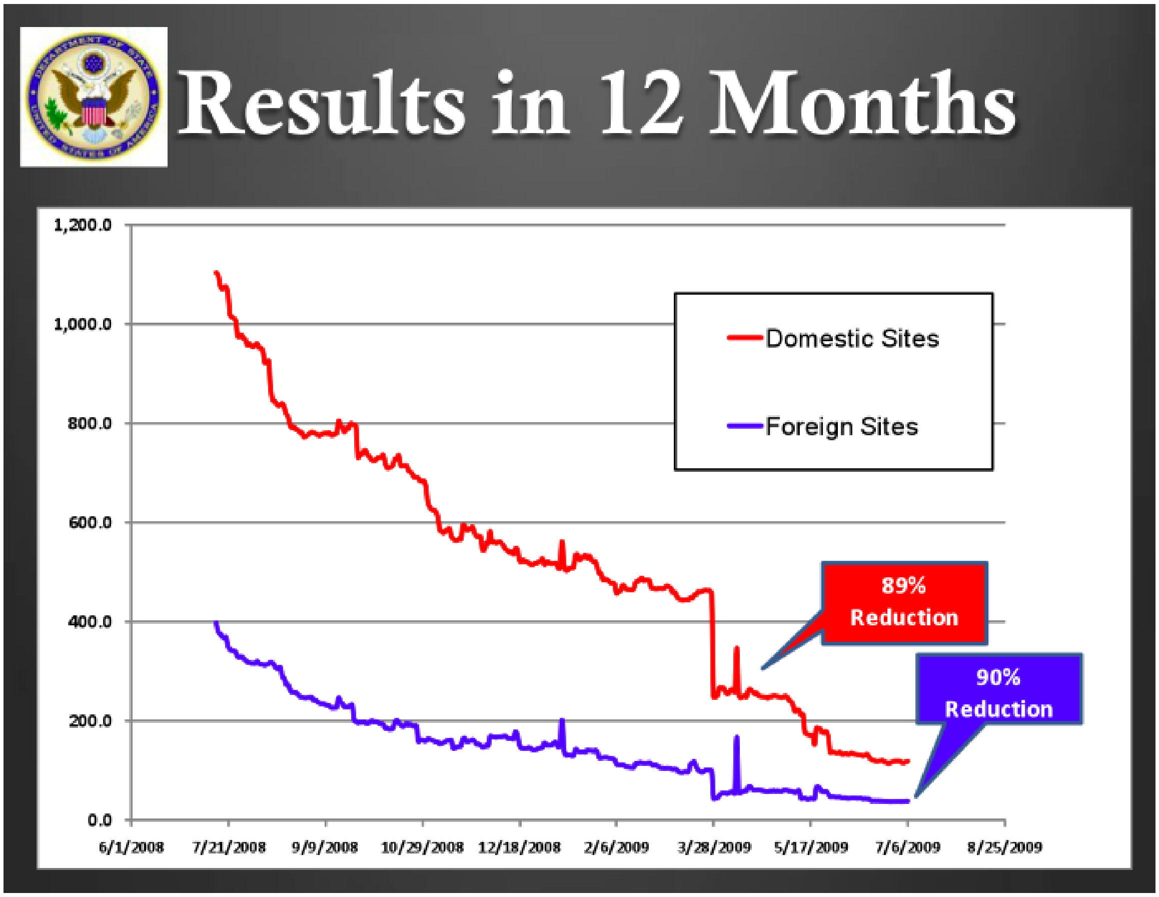
(2) Once we achieve near-real-time situational awareness, then we need to dynamically defend the network in near-real-time.

What he is describing is not a theoretical construct. We know that it can work. The U.S. Department of State Department proved that near-real-time situational awareness is both possible and powerful.   At the State Department, they call it continuous monitoring.

The State Department Proves Continuous Monitoring Works

Two of the most important benefits of dynamic defense are enabling the defenders to (1) minimize their vulnerability to attack, and (2) act very quickly to protect their systems when a new threat or vulnerability is discovered. Continuous monitoring, the first step in dynamic defense, enables both of those goals to be met much more effectively than FISMA-based quarterly or annual reporting. Strong support of continuous monitoring, in lieu of out-of-date report writing, is one of the most important elements you have included in Senate Bill S 3480. The State Department is the only agency that has implemented continuous monitoring so far, although there are credible rumors that the Army, NASA and NSA are moving that way. And the Navy doesn't seem to be far behind and the Air Force is leaning in the right direction.

Continuous monitoring works. Figure 1 shows that the U.S. State Department was able to reduce reliably-measured risk by over 85% in less than a year. State is continuing the process with equally impressive results this year. Look closely at the chart, and you will see what continuous monitoring means – the updated data comes in daily or every couple of days – not quarterly, or annually.   Had State used the longer time periods favored by the other agencies, many more State Department computers and networks would have been open to attack, for far longer periods,



Results in 12 Months

89% Reduction

90% Reduction

Continuous monitoring also radically reduces the time it takes agencies to fix important new security problems. Here's proof: When Google announced it had been penetrated and had lost sensitive data, it simultaneously illuminated a major vulnerability, nicknamed Aurora. Aurora was present on millions of machines across the government (those running Internet Explorer). Fixing Aurora turned into a positive case study of the effectiveness of State's continuous monitoring initiative.

Federal agency CISOs all learned from news reports or from US-CERT at DHS that most of their computers were at high risk of compromise from attacks using the Aurora vulnerability. Each CISO acted quickly, using the tools available. Nearly all of them sent out email notices to their distributed security officers who sent out email notices to system administrators. Sadly, many of those system administrators did not act. There was no centralized monitoring of patch status, so the civilian agency CISOs had no way of even knowing. If what gets watched gets done, then the CISOs' lack of near-real-time visibility into their networks makes them unable to protect the computers for which they are responsible.   DoD, on the other hand, demands that the recipients of the security patch orders (called IAVAs) confirm receipt and confirm whether the correction has been implemented. A DoD official told me the confirmation reports showed that fewer than 70% of the vulnerable machines were patched even five months after the mandatory Aurora order went out.

The State Department offers a stark contrast to DoD and other agencies, because State can tell, within a day, which systems have and have not been patched. When State's CISO learned of the critical problem posed by the Aurora vulnerability, he didn't have to send an email. He raised the vulnerability's risk factor (the value used to weight it in the overall risk score). Every office saw immediately that their security score had fallen and their bosses also saw the fall. Within 6 days 90% of all vulnerable systems in all embassies and in all State Department offices around the world had been patched and were safe from attacks. That's six days, not weeks or months. No emails had to be sent; the scoring risk system did all the work. A clear example of why daily continuous monitoring is so important: it causes rapid risk reduction with low overhead.

Every federal agency can have the same results or better. They already have the vast majority of tools they need to automate continuous monitoring of the most critical controls defined by NSA, DHS, DoD, and the DoE nuclear energy labs. Those are the same controls measured by the State Department to be certain they are doing the most important things first. And the State Department's CISO, John Streufert, generously provides copies of State's management and scoring software at no cost to other U.S. government and defense industrial base organizations.

You might assume from this discussion that the original FISMA enables such automation. The exact opposite is true. The CISOs tell me that they cannot follow in State's footsteps because their money is tied up paying for those out-of-date reports. As mentioned earlier, those reports are required, according to the CISOs, because FISMA made NIST guidance mandatory. What your bill calls for in continuous monitoring is a new way of managing federal security, one that has already proven it is far more effective than the old way.

How Private Economic Interests Fight Continuous Monitoring

Sadly, it is not only FISMA that is slowing down the move to near-real-time situational awareness through continuous monitoring. The contractors that charge federal agencies hundreds of millions of dollars for writing the out-of-date reports are fighting to stop the move to continuous, daily monitoring, even though they and their firms can continue to be employed to enable and manage the new way of doing business. Their rear-guard actions are being supported by federal officials who appear to be uncomfortable with change or afraid of taking responsibility for active risk reduction. Box 1 below summarizes the evidence.

Misleading Statement 1

"We are already doing continuous monitoring."

In a SecureAmericas meeting in Washington late last month, Hord Tipton, the host and ICS2's president, asked the 150 federal security contractors and information security officers in his audience, "How many of you are already doing continuous monitoring?" He told me that more than 130 people raised their hands. Both Hord and I know that they didn't mean continuous monitoring the way the State Department is doing it, so I did some research. It turns out that the people who raised their hands are calling manual data entry of quarterly or annual or tri-annual reports "continuous monitoring." This is how the consulting firms can continue to get paid hundreds of thousands of dollars for reporting out-of-date information; they'll enter it into a computer system rather than print it and put it in 3-ring binders.

What they call continuous monitoring is the opposite of what the State Department has done; it does not enable rapid risk reduction or rapid response to new threats. What it does do is give the people who want to continue writing useless reports a cover story. I wondered how so many people could justify the deception and learned that NIST was the source. Both at the NIST website, and in speeches by NIST executives, viewers and attendees are told that NIST's updated Special Publication 800-53 guidance enables continuous monitoring. The only way that could be true is if annual or quarterly manual information collection is renamed "continuous monitoring." Lo and behold, that is just what NIST did. NIST's 800-53 publication is employed by CISOs and contractors to guide and justify the $1,400 per page reports that have almost no impact on risk reduction. In other words, the people who are desperate to keep writing reports stole the term "continuous monitoring" to cover up their continuing antagonism to actually measuring and reducing risk. You can avoid having your new bill hijacked by the paper pushers if you add three words ("data entry and") to your definition of continuous monitoring [3551(b)(2)] and if you use oversight to shine a bright light on counter-productive behaviors.

Despite the delaying tactics describe above, many agencies are trying to follow the State Departments lead, and some, such as the Air Force, are finding other innovations in continuous monitoring.

The 24th Air Force Takes Continuous Monitoring A Step Further

The 24th (Cyber) Air Force has responsibility for securing the entire US Air Force network. A few months ago away teams from the 24th discovered that more than 30% of anti virus (AV) packages across the Air Force were not up to date. No amount of email cajoling was effective. So Colonel Diaz, Operations Director, and General Weber, Commander of the 24th, had their people build automated monitoring tools that continuously check AV updates. Their solution is different from what most other organizations use because it is open and works well with multiple antivirus tools, avoiding the vendor lock-in that is so damaging to innovation and cost-effectiveness. The Air Force system goes beyond testing. Every time it finds a computer with out-of-date anti-virus signatures, it immediately connects that computer to a special network where it gets an AV update. An out-of-date system is not reconnected to the main network until it is protected and cleaned if it has become infected. On General Weber's order, the technology is being deployed across all of the Air Force.

This innovation by the 24th Air Force extends a tradition of Air Force cyber leadership that began in 2002, as I describe in the next section.

Procurement is the Most Productive Public Private Partnership for Improving Federal Cybersecurity – The Air Force Standard Desktop Story

In 2002, US Air Force CIO John Gilligan determined that the Air Force was spending more to test and deploy patches and to clean up after the damage from flaws in Microsoft software than to buy the software, and he announced he was going to ask Microsoft to work with him to solve the problem. He tasked NSA and Air Force experts with determining a safe configuration of Microsoft Windows that would withstand common cyber attacks as well as attacks used by NSA's red teams, and still effectively operate Air Force applications. Once that was done, he negotiated a contract with Microsoft to deliver the secure version of its software to the Air Force, through its hardware suppliers, such as HP and Dell. Microsoft also agreed to test all new security patches on the Air Force secure configuration before the patches were released. More than 550,000 Air Force PCs had the secure desktop installed. Gilligan was succeeded in the Air Force CIO job by Lieutenant General Peterson, who told me that the innovative partnership between Microsoft and the Air Force saved the Air Force over $100 million per year in reduced system administration staff and reduced patch testing. He also said it reduced the average patch installation time from 57 days to 72 hours and is on its way to 24 hours. And he said that the help desk calls had been cut in half because the users were able to get their work done and they were much happier. The bottom line of this procurement partnership: huge savings, huge improvement in security, and huge improvement in user satisfaction. What is not widely known is that the secure configuration purchased by the Air Force also protects Air Force systems from most infections carried by the Advanced Persistent Threat that has plagued so many other federal agencies.

The Air Force secure Windows procurement cost about $100 million per year, and that was money they had to spend anyway for Windows updates. But by consolidating all Air Force procurement into a single $500 million multi-year purchase of Windows and Microsoft Office, they were able to persuade the vendor to deliver more secure software on 550,000 computers. The US Government spends over 800 times that much (a total of $80 billion each year) on information technology products and services. Leveraging a larger fraction of that $80 billion in security-focused public-private procurement partnerships can transform the security of the federal government and spill over to help the rest of the American computer users.

There are people who don't want the government to do what the Air Force did, and they use misleading statements to make their case. One of the false statements you may hear has been expressed many times by vendors who don't want to upgrade the security of their products. Box 2 provides the details.

Misleading Statement 2

"The federal government should not be telling industry how to secure its products. They do not know as much about security as the vendors do, and federal meddling will stifle innovation."

If industry actually knew how to secure systems better than the government did, Google would not have called the NSA when it was infected. It would have called one of the commercial companies whose Washington reps argue so strongly that government is incompetent at determining how computers should be protected.

The visceral antagonism to government specifying security for products it buys can damage the vendor just as much as it damages national security. The best illustration is from battle Microsoft waged to stop the government from specifying secure configurations for the software it purchased.

In 2002, the Government Information Security Management Act (GISRA) was sunsetting; that's what led the House Government Reform Committee to draft FISMA. A big controversy in the FISMA drafting process was whether to empower agencies to establish standard security configurations for the systems they operate and purchase. Both major IT industry associations fought the idea of government-specified configurations for many months. During the negotiations, Frank Reeder and I asked the president of one of those associations to discuss the issue over lunch. Frank had served as Assistant Director of OMB, led the Reagan Administration team that secured passage of the Computer Security Act of 1987, and served as Assistant to the President for Administration in the Clinton White House. We both asked the association CEO why he would not support government-defined secure configurations. After nearly an hour of discussion he said, "It is the right thing to do; but if I support it, Microsoft will kill me."

The IT associations continued to fight the concept of minimum security configurations for another two years, right up until the time of Gilligan's agreement. After that, Steve Ballmer personally monitored the project, and senior Microsoft executives spoke glowingly of the value of the more secure configuration of their software and fully supported government-wide adoption of the standard that was called the Federal Desktop Core Configuration.

So if standardized secure configurations were a wonderful idea in 2005 why were they a terrible idea from 2002 to 2005. The answer, I believe, is that the Washington reps got it wrong. They hurt Microsoft's business by fighting the idea of a safer standard version of Windows. Three additional years of being known as the company that sold very insecure software to federal agencies opened the door wider for UNIX to gain market share in government and also drove many government organizations into the arms of early cloud vendors like Citrix.

Government has to take the lead in specifying security settings not because it is smarter, but because only government (NSA, DoD, DHS, FBI, and the Secret Service) has access to the forensics and attack information that shows comprehensively how attacks are actually carried out. Almost everyone else is guessing. (The one non-government exception is VISA that has collected data about how credit card data thefts are carried out.)

So when you hear the Washington vendor reps and industry association reps telling you that government doesn't know how to secure systems, just remind them whom Google called when they needed help securing their systems.

One sad footnote must be added to the story of the Air Force's great procurement success. It has not yet been replicated in most other agencies. A lack of urgency, competence and leadership combined to grasp defeat from the jaws of victory. The new White House Office of Cyberspace Policy, acting in concert with OMB, can solve the problems very quickly. It is a perfect case study of why your bill and your continuing oversight are so essential.

Using Procurement to Enable Next-Generation Dynamic Defense

State Department's continuous monitoring tools generally collect data every day or two or three. The next generation of continuous monitoring will collect data almost continuously. To make that possible, NSA and NIST are creating standard protocols for security data and are working to help software vendors who sell to DoD and the federal government build in capabilities for minute-by-minute continuous monitoring using those protocols. These protocols, called S-CAP for Security Content Automation Protocols, must be imbedded in the software that comes with computers rather than being bolted on later. The government's strategy is to publish the protocols and then provide incentives to persuade software and hardware vendors to insure their tools are S-CAP enabled. The best incentive is a combination of Department of Defense and federal civilian government buying power. That creates a big enough market to enable IT vendors, system integrators, and ISPs to embed the necessary capabilities at costs that can be spread over many large clients. This is the same strategy as that used by the Air Force to buy secure versions of Windows. The strategy makes improved security profitable for the vendors and affordable for the user organizations.

The Manpower Imperative and the US Cyber Challenge

Dynamic security can stop many attacks, but not all of them. Some will get through. A lot of highly specialized people with advanced technical security skills are still needed. They are needed throughout government and industry to do deep packet inspection, and log monitoring, and disk forensics to find the attackers that get through the defenses; to reverse engineer malicious code that is found; to perform inspections of capabilities through penetration testing; and to audit automated and manual security operations. They are needed in every development organization to architect security into new applications and to write code that is free of security flaws. They are needed as security-savvy system administrators who can recognize and flag anomalies and become a human sensor network. They are needed in the military to find vulnerabilities in commercial software and hardware before adversaries do, to build new exploits, to conduct military operations. People with any of those skills are VERY rare and in high demand.

> *"There are about 1,000 people in the US who have the specialized security skills to operate effectively at world class levels in cyberspace. We need 10,000 to 30,000."* ***(Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA's Clandestine Information Technology Office, The Pentagon, October 3, 2008.*****)**

Security skills shortages extend from the federal government to the US defense industrial base, federal information systems contractors, utilities, telecommunications companies, and most other segments of the critical national infrastructure. In fact, wherever senior management has been made aware of a major, damaging cyber attack, the shortage becomes immediate and acute. For example right after Google got hacked and learned from the NSA what it takes to find evidence of the advanced persistent threat, reports filtered in from all around the US that Google was searching for strong specialized security talent. Sadly the talent shortages for people with specialized security skills are so acute that if Google gets one, some defense industrial base company probably loses one from a critical project. Highly skilled security people will be the most sought after weapon in any future war. Our nation needs to build a pipeline to fill the gap of 20,000 to 30,000 cyber guardians.

For the most part, our colleges cannot create the needed talent because the faculties in the vast majority of colleges are not skilled enough in the specialized, hands-on security tasks to be able to identify and nurture world-class talent. The US Cyber Challenge is the principal initiative aimed at filling that void. It uses five different progressively more challenging competitions, most of them on line, to entice and challenge and nurture talented young Americans. Thousands of young people have entered the competitions since the U.S. Cyber Challenge was announced 11 months ago, and many very-talented young people are being identified and supported. The program is now directed by Karen Evans who previously served as Administrator of e-Government at OMB. She has been doing an extraordinary job of getting industry support and leading the college faculties and state agencies and volunteers who are staffing summer cyber camps in Delaware, New York and California. Senator Carper deserves special thanks. He has given generously of his time to recognize winners and has empowered his staff to help the state employees and college professors make the Delaware Cyber Challenge very effective.

Your support for the US Cyber Challenge in S 3480 will go a long way toward closing the skills gap. If you add the small change I mentioned earlier for language in section 404, to make sure contractors with technical responsibilities must prove they have the right specialized skills to do the assigned jobs effectively, you'll have a huge impact on enabling the government to protect its systems.

The Bottom Line

By enacting the legislation before you, with a few small amendments to address the shortcomings I outlined, Congress can immediately change the way the cyber-security game is played to the benefit not just of government, but of the economy and the American people.

Thank you for your service and efforts on our behalf and for this opportunity to share my views with you.

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 120,000 alumni in seventy countries. At SANS, he oversees the Internet Storm Center (an early warning system for the Internet), 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. He also leads a global security innovation program that identifies people and practices that have made a measureable difference in cyber risk reduction, and illuminates those innovations so other security practitioners can take full advantage of them to improve security in their enterprises.

He has testified before both the US Senate and House of Representatives. In 2000 President Clinton recognized his 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 their 2005 Azimuth Award winner, a singular lifetime achievement award recognizing outstanding service of a non-government person to improving federal information technology. In May of 2010, the Washington Post named seven people as "worth knowing, or knowing about" in cyber security. The list included General Alexander who heads the US Cyber Command, Howard Schmidt, the White House Cyber Coordinator, other national leaders, and Alan.

Earlier in his career Alan helped build a software company, took it public, and merged it into a larger company listed on the New York Stock Exchange. His degrees are from Cornell University and the Massachusetts Institute of Technology.