Testimony of Marcus H. Sachs
Director, SANS Internet Storm Center

Before the House Committee on Oversight and Government Reform,
Subcommittee on Management, Organization, and Procurement

"Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems"

May 5, 2009

Madam Chairwoman and members of the Committee:

Thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing federal information systems. The Committee's interest in this topic is timely and crucial to the security of our nation's most sensitive information. After giving you a very brief background of my professional experience I would like to address the broad subject of securing federal information systems via the lessons I've learned from the perspective of a career military officer and federal civil servant, as the director of the SANS Internet Storm Center, and as a private sector professional working with the national security and emergency preparedness (NS/EP) community here in Washington.

I am a retired United States Army officer, and I spent the second half of my career designing, operating, and defending both tactical as well as strategic military computer networks. My last military assignment was with the Joint Task Force for Computer Network Defense (JTF-CND, now the JTF-GNO) where I was a member of the initial cadre and served for three years. Shortly after retiring from the Army at the end of 2001 I was appointed to the staff of the National Security Council and was part of the team that wrote the National Strategy to Secure Cyberspace.

After we published the strategy in February 2003 I joined the staff of the brand new Department of Homeland Security where I became the Cyber Program Director in the Information Analysis and Infrastructure Protection (IA/IP) Directorate. At first I was the only cyber guy on the staff of DHS, and immediately began trying to find other cyber experts around the Department to leverage into a virtual cyber security team. While building that team I developed the concept of what eventually became the United States Computer Emergency Readiness Team, or US-CERT, which was launched in September 2003 and today has a proposed 2009 budget of over $240 million.

When I left the federal government at the end of 2003, I asked the privately owned SANS Institute if I could direct their Internet Storm Center, a group of cyber security volunteers that I had been affiliated with while in the military and at the White House. The Internet Storm Center is a threat watch and warning organization that has no physical office or operations

center, in fact it only exists in cyberspace. It is staffed by over forty volunteer incident handlers around the world and is used by tens of thousands of system administrators, including many in the federal government, as an authoritative source of information about malicious activity online.

In addition to that volunteer work, since leaving government service in 2003 I was employed for three years by SRI International as the deputy director of their Computer Science Laboratory, primarily supporting DHS' cyber security research activities; and since 2007 I have been employed by Verizon as an executive director for national security policy. In 2007 and 2008 I was part of the CSIS Commission on Cyber Security for the 44th Presidency, and chaired two of the Commission's working groups. I will draw upon all of these experiences in my comments to the Committee today.

I would like to start with a look back over our shoulders at how we got to the troublesome position we are in today. Decisions made in the 1980s about government purchases of commercial off-the-shelf (COTS) computer hardware and software in lieu of expensive specially-hardened systems made sense when most home, business, and government computer users did not have access to networks but relied instead on floppy disks (the "sneaker net") to copy and transfer files between computers. At that time, malicious code inside the federal government's desktop computers was primarily in the form of disk-based viruses with names like "Brain" and "Concept" and was not much more than just an annoyance.

In fact, to gain access to a government desktop computer or file server you generally had to have physical access to it, or the ability to talk a government employee into granting the access. Theft of floppy disks, backup tapes, and printer outputs were the methods used by our adversaries to "steal" sensitive information contained on government computer systems. This changed in the mid-1990s as more organizations connected their computers to the global Internet and threats beyond the borders of the United States began to take advantage of the connectivity. The growth of government outsourcing and the increasing dependence on government contractors further added to the problem of protecting sensitive data since information was no longer uniquely stored on government computers, behind layers of rigid security barriers.

Also in the 1990s, the "dot-com explosion" happened, the Internet became a common household word, and millions of government and industry employees wanted to be able to do at work what they were doing at home (and vice-versa) with respect to desktop computing. Compared to today, threats online were generally unsophisticated in the 1990s. Nuisance viruses and website defacements were the common weapons used by both adolescents and political protestors as methods of expression. In fact, the government had to deal with hundreds of embarrassing website security breaches in the late 1990s, including defacements of www.cia.gov, www.congress.gov, www.faa.gov, www.doj.gov, www.senate.gov, www.speaker.gov, www.va.gov, and www.whitehouse.gov.[1] But while the website

[1] http://www.attrition.org/mirror/attrition/gov.html

defacements were a very visible sign of the difficulties the government was facing in meeting the new challenges of cyberspace security, a less visible conflict on two fronts was brewing that we continue to deal with today – organized cyber crime and nation-state cyber espionage.

After the fall of the Soviet Union the United States and other countries expected that the former Soviet countries would rapidly join the ranks of democracy and freedom. We believed that by encouraging capitalism and sharing our industrial know-how, in a short period of time Eastern Europe would be on par with Western Europe and there would be an increase in economic prosperity for all. Unfortunately that scenario did not play out as we expected. Instead, thousands of highly educated Russians, Ukrainians, Romanians and others were left unemployed as the governments shrank in size and new businesses failed. Being a central component of the Soviet political system, organized criminal groups began to fill the void of employment left by the shrinking job market.[2]

The growth of the Internet was an incredible break for these gangs, a "perfect storm" for cyber crime. The Internet offered a way to make money, an opportunity to put bread on the table. These groups fully understood the criminal prospects offered by an expanding and uncontrolled global computer network that has virtually no transaction taxes (and therefore no need for tax evasion), provides anonymous access to nearly everything online, has weak or nonexistent political and national boundaries, where criminal tools are functionally the same as lawful tools, that offers numerous opportunities for money laundering, has little or no cyber law enforcement present, and contains millions of victims that will believe just about anything they see. How could they pass this opportunity by? It did not take long for them to find it.

Between June and October 1994, an organized Russian crime gang successfully transferred $10 million from Citibank to different bank accounts around the world. Known as the "Citibank Caper," this incident was partially responsible for prompting the "Security in Cyberspace" hearings in the U.S. Congress chaired by Sam Nunn. After examining information security risk profiles of hundreds of major companies and several government agencies, the hearings found that computer security complacency was widespread across government, academia, and all economic sectors. Sound familiar? Fifteen years later we have made much progress, but if the same investigation were conducted today we would still find large pockets of complacency and ignorance, especially in those sectors where there is a general feeling that computers and information systems are isolated from the Internet and protected by imaginary barriers.

In fact, the Internet Crime Complaint Center found that in 2008 cybercrime was up 33% from 2007, making last year the worst on record. In 2008, there were over $250 million of reported losses in the United States from cyber crime, compared to $18 million in 2001.[3] Later in my testimony I will talk about what Verizon found by researching several hundred data breaches over the past five years. Criminals are bypassing our strengths and attacking our weaknesses. They know we are investing in security but they are taking advantage of simple mistakes we are

[2] http://www.ncjrs.gov/pdffiles1/nij/187085.pdf
[3] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

making. The fortunate lesson is that those weaknesses and mistakes are fairly easy to identify and fix, and do not cost a lot in terms of resources. All it takes is a willingness to tackle the problem at the senior leader level and not ignore it or delegate it to junior system administrators.

Cyber espionage has followed the same path as cyber crime, and in many cases is technically identical in terms of tools and access methods. During the Cold War and in the centuries prior to it, nations took great risks to recruit and train spies to operate on foreign soil. Today, the Internet has made spying as easy as opening up a web browser and querying a search engine, and has reduced the risk of loss of human life to nearly zero. Why spend hundreds of thousands of dollars to train and equip a spy when surfing to a foreign country's computers provides just as much information at practically no cost? Nearly all countries conduct foreign espionage and Internet access has simply made that process easier. Unfortunately many countries including ours "give away" secrets by allowing open access to research institutions, government contractors, and the government's own networks.

In the late 1990s several US government systems were found to have hidden accounts and large amounts of unauthorized activity. As the investigation[4] developed, more computers and systems outside of the federal government were found to have unauthorized accounts. "Data exfiltration" became the new buzzword, rather than "intrusion" or "unauthorized access." The targets seemed to be large databases that contained atmospheric data, bathymetric data, and other information that took decades to accumulate. The source of the attacks was not clear – the intruders used complex methods to route attacks through multiple compromised computers, and used "drop sites" as collection points for the data being stolen. In no cases were any signs of disruption present. It all appeared to be electronic espionage, a classic case of theft of intellectual property, only via the Internet rather than using microfilm and a spy camera as James Bond would have done.

During the Cold War the activity was clearly centered on US vs. USSR espionage. But in recent years the concern has moved from former Soviet countries to China in terms of espionage directed against the United States. What is unique about China, and which really complicates matters for us, is that the culture in China (and Asia in general) supports academic and scholarly achievement. Many students and professors treat the Internet as an experiment in human communications, and routinely gain access to remote systems or locate bugs in vulnerable software purely for academic purposes. Their findings are published in academic papers, and the researchers move along to the next project. Some, however, have found that there is incredible value in this research and have begun to make a business out of it, selling their findings to governments, criminal groups, and perhaps even terrorists.

A recent example of such a cyber espionage attempt coming from China shows how they gain access. In the spring of 2006, a government system administrator in the United States noticed that many of his users were receiving unexpected e-mails with Microsoft Word attachments

[4] The investigation was called Moonlight Maze

written in Chinese. When opened, Word would crash and sometimes the computer would have to be rebooted in order to function again. The problem was eventually traced to what we call a "zero-day vulnerability" in Word. This means that something was wrong with the software, and the defect allowed for remote access if exploited correctly. Even worse, at the time this was discovered there was no patch for the flaw. Somebody in China figured out how to take advantage of it and launched a targeted email attack against US government computers to gain remote access.

Eventually it was determined that the group behind the attacks was a gang of young Chinese hackers selling information they obtained from US and Japanese computers.[5] The only glimmer of good news in this story is that the ring leader of the Network Crack Program Hacker (NCPH) group, Tan Dailin (aka "Withered Rose" in hacker channels) was recently arrested and faces about seven years of jail time in China.[6]

I'm sure that the Committee is painfully aware of the "Titan Rain" intrusions that were made public over the past few years. Titan Rain was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003. The attacks were believed to be Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) remains uncertain. The designation "Titan Rain" was changed, and the current name for the attacks is itself classified. The attacks continue to the present day, and are the primary motive behind the Bush administration's Comprehensive National Cybersecurity Initiative launched in 2007.

The intrusions are not just aimed at government computers. In fact, nearly all of the government's prime contractors have been targeted, and many have fallen victim. The most recent account is unnerving – foreign intruders reportedly gained access to the plans for the Defense Department's Joint Strike Fighter program via the computers of a major defense contractor.[7]

In response to rapidly the growing threats in cyberspace, the government has been working hard to keep up with the problem. The "Security in Cyberspace" hearings in the U.S. Congress chaired by Sam Nunn were already mentioned. Shortly after those hearings, and largely in response to the 1995 Oklahoma City bombing the Clinton administration launched a series of initiatives to increase the security of our nation's critical infrastructure, including the soft underbelly of cyberspace. A new organization, the Federal Computer Incident Reporting Center (FedCIRC), was established by NIST in 1996 to bring together resources from the Defense and Energy departments in order to develop a cyber incident response capability for the federal civilian agencies. FedCIRC was transferred to the General Services Administration in 1998, and then was absorbed by DHS in 2003.

[5] http://www.time.com/time/magazine/article/0,9171,1692063,00.html
[6] http://www.thedarkvisitor.com/2009/04/withered-roselaw-done-come-and-got-him
[7] http://online.wsj.com/article/SB124027491029837401.html

Presidential Decision Directive 63, issued in May 1998, correctly identified the risks our nation faced not only in the physical world but also in cyberspace. It specified what sectors of the economy were deemed to be "critical" and set in motion the creation of several new government organizations needed to coordinate the protection of the nation's critical infrastructure, including the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO), and a public/private partnership called the Information Sharing and Analysis Center (ISAC).

Today, the NIPC and CIAO are gone, having been absorbed with the FedCIRC into DHS in 2003. The ISAC (singular) never happened, but instead several ISACs (plural) were established by the private sector to work with their government counterparts. About a dozen of the ISACs are still around, serving as a bridge between the private and public sectors in the coordination and dissemination of threat and vulnerability information. Policy coordination bodies, known as "Sector Coordinating Councils" were established as part of Homeland Security Presidential Directive 7 in 2003, and DHS also manages several cross-sector coordination groups including the Cross Sector Cyber Security Working Group and the Industrial Control Systems Joint Working Group. But even with all of the new organizations and an increased interest in sharing critical information between the public and private sectors, intrusions into federal systems continue to grow in the current decade.

The most recent effort to protect government systems is President Bush's Comprehensive National Cyber Security Initiative. Launched in the summer of 2007, and formalized in NSPD-54/HSPD-23, it consists of twelve major projects ranging from the creation of new monitoring systems to limiting the number of gateways between government networks and the public Internet. It also contains efforts to develop a stronger cyber security workforce in the federal government and attempts to strengthen ties between the federal government and the owners/operators of critical infrastructures that depend on computer networks. Earlier this year, President Obama tasked his staff to conduct a comprehensive review of all of the nation's cyber policies in order to develop a roadmap for improvement. The "60-day review" as many call it is not yet public but reportedly calls for a new position at the White House to lead the effort, and recommends changes for several departments and agencies.

The private sector is also engaged and over the past several years has developed and published numerous recommendations concerning the security of cyberspace. I was fortunate to be a member of the Center for Strategic and International Studies (CSIS) Commission on Cyber Security for the 44th Presidency. Our report was published at the end of 2008 and has three major findings: cyber security is a major national security problem for the United States; decisions and actions we take to protect ourselves in cyberspace must respect privacy and civil liberties; and only a comprehensive national security strategy that embraces both the domestic and international aspects of cyberspace will make us more secure. Our commission had several recommendations for the federal government including: create a comprehensive national strategy for cyberspace, lead from the White House, reinvent the public-private partnership, modernize authorities, use acquisition policy to improve security, and do not start over.

I would like to go beyond those recommendations with some of my own observations and thoughts. First, the government should lead by setting the example. Securing an organization's corner of cyberspace is hard. It normally does not generate revenue (unless you are selling security services) and it is difficult to show senior organizational leadership why it is important. If the government was to manage their own computer networks in a manner that can be an exemplar for others to follow, we in the private sector can point to the government and say, "follow them, do as they do." But when government computer systems are easy to break into and offer our adversaries an easy opportunity for theft of our nation's secrets, it is easier to say "don't follow them, don't do as they do." We need not only the government as a whole to lead by example, but we need an organization inside the government to take an internal lead and set the example for the rest of government to follow.

Second, the government must use its acquisition powers to improve everybody's ability to secure cyberspace. The story about the Air Force's use of procurement policy to insist that Microsoft develop a more secure version of the Windows operating system must be told over and over.[8] Today, thanks to the efforts of the Air Force, OMB, NSA, DISA, NIST, Microsoft, and others there is a very strong "Federal Desktop Core Configuration" standard that can be used not only by the federal government but by any organization that uses the Windows XP or Windows Vista operating systems.[9] But it cannot stop there. We need more secure software from all vendors, and we need the federal government to continue to use its acquisition and procurement policies to drive that effort.

Third, the federal government must develop a career field for cyberspace professionals, from initial entry all the way to SES. There are a few cyber scholarship opportunities available for college students, and we do a very poor job of managing their careers. We are too reliant on contractors and temporary employees to fill in gaps where we need career civil servant professionals. If we do not immediately address this problem, we will never be able to secure the federal government's networks. Security is not all about applying the latest patch, running updated antivirus software, or installing a new firewall. It is about culture, risk management, and leadership. Without a trained and dedicated workforce and leaders who are willing to lead through personal involvement in mandating cyber security in their organizations, we are sitting ducks for continued abuse coming from our adversaries.

Fourth, we must rethink the way we view cyberspace and in particular the Internet. It started as an experiment, a proposed way to link together expensive mainframe computers so that researchers and strategic military planners could share computing resources via the nation's communication backbones. For a couple of decades, the general public was largely unaware of its existence, but in academic circles it was mesmerizing and every university wanted to be a part of it. The military understood its importance too, and spent millions of dollars to build computer networks connecting nearly every military base world-wide. When general society was invited to participate, new uses emerged that today include a multitude of audio, video,

[8] http://hsgac.senate.gov/public/_files/042809Paller.pdf, pp. 4-5
[9] http://fdcc.nist.gov

and data services. Cyberspace is everywhere, we depend on it, and our nation cannot do without it.

But we cannot let the future of the Internet be driven by military, espionage, or criminal forces. It's important to maintain our military defenses, but a strong desire to use cyberspace as a battlefield is harmful to what it's really good for – becoming the essence of the nation's economic recovery. Like industrialism in the 19th century, cyberspace today is what fuels our economy. We cannot let it become a combat zone, and we certainly cannot let the criminals or spies take it over either. We need to change the conversation and argue that cyberspace is the cornerstone of America's global leadership and economic prosperity in this century. By looking at cyberspace through the lens of economics, we might find better approaches to securing it.

Fifth and finally, cyberspace exists because of the combined work of government and private sector scientists, researchers, investors, and leaders. It is not the single domain of either government or the private sector and must be protected from damage by both parties working in unison. We have come a long way over the past several decades in building strong public-private partnerships and we cannot let those relationships fall apart. It has been long understood in the physical world that defense of private property begins with the property owner, but in accordance with laws provided by the government. While the federal government provides for a national defense, it depends on private property owners to adequately secure their property from theft, as well as from natural threats such as wind, fire, or floods. It also depends on the private sector to provide materiel, labor, know-how, and innovation in order to adequately protect the nation from foreign adversaries. In cyberspace we should think the same way, with the federal government oriented on making and enforcing laws that permit a private property owner to adequately defend that property, while working with the private sector to provide a "national defense" oriented externally against threats coming from beyond our shores.

The last subject I would like to address is what Verizon's investigation teams found when they examined forensic information from several hundred data breaches over the past five years.[10] The latest report just came out last week and the findings can serve as a roadmap for where the federal government and others should be investing resources if they want to reduce or eliminate data breaches. In 2008 alone, the Verizon team investigated 90 confirmed data breaches that encompass an astounding 285 million compromised records.

The investigations showed that as expected, most of the breaches were from external sources, but a third of the breaches originated in trusted third-party connections that were used as a conduit to break into the victim's network. Nearly 90% of the breaches were preventable if system administrators had not made simple configuration mistakes, and over 80% of the victims were not compliant with the Payment Card Industry (PCI) standards. Other bothersome observations include the fact that in over half of the cases it took days, weeks, or months for the attacker to figure out how to break in. That's a lot of time for early detection. But in spite

[10] http://www.verizonbusiness.com/worldwide/products/security/risk/databreach

of that, in over 75% of the cases it took weeks or months after the breach occurred and data was stolen for the victim to figure out that they had been compromised. To make it worse, in nearly 80% of the cases it took another several days or weeks to stop the attack after it was discovered.

The bottom line is that nearly all intrusions are preventable and that we can make a lot of this problem go away (or at least make it harder for the bad guys) by following best practices and educating our users. It's inexcusable that in 2009 we seem to be unable to prevent our adversaries from breaking into our computer networks. It's also inexcusable that we continue to run our computer networks as though they are some magical enterprise only understandable by geeks and nerds. Cyberspace belongs to all of us, and we are all part of the solution to making it more secure.

Madam Chairwoman and members of the Committee, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing federal information systems. I look forward to answering any questions you may have.