HPSCI White Paper on Cyber security
December 10, 2008

Securing America's cyberspace is a national security priority. Increasingly sophisticated foreign adversaries are accessing sensitive U.S. computer networks to covertly obtain military technologies. Foreign competitors and everyday criminals are stealing trade secrets from American pharmaceutical, biotech and information technology (IT) firms at little to no cost or risk. Even critical services are vulnerable to disruption through cyberattacks against financial, utilities, transportation and logistics systems. The lack of cybersecurity poses a far greater danger than theft and espionage in the short-term; the foundation of America's power and status in the world is at risk of erosion if cyberspace is not secured.

**Definition of the Problem**

**Cyber Attacks:** In April 2007, Estonia was the victim of large-scale Distributed Denial-Of-Service (DDOS) attacks that crippled key government ministries. According to published accounts, websites that normally received 1,000 visits a day were bombarded with approximately 2,000 visits per second, causing the sites and the servers that hosted them to crash. Similarly, in August 2008, Georgian government websites and communication systems were overwhelmed by unattributed attackers during the brief conflict between Georgia and Russia. As reported by CNN, the Department of Homeland Security and Idaho National Laboratory demonstrated that a directed cyber attack can cause an electric generator to self-destruct, verifying the threat cyberattacks poses to civilian infrastructure. Whether it is a government's communication systems, websites or utility providers, in an increasingly digitized society critical infrastructure is vulnerable to cyber attack.

**Cyber Espionage:** In addition to cyber attack, foreign adversaries have recognized the potential to leverage the internet for political espionage. In June 2007, U.S. Representatives Wolf and Smith, both outspoken critics of China's human rights record, disclosed that their congressional office computers were compromised by hackers traced to a computer in China. According to the German Magazine *Der Spiegel* in August 2007, German Chancellor Angela Merkel learned that three computer networks in her own office had been penetrated by Chinese intelligence services. Most recently, on November 5, 2008, *Newsweek* reported that the computer systems of both the Obama and McCain presidential campaigns were victims of advanced cyberattacks by an unnamed foreign entity.

Cyber intrusions by foreign nations are a grave threat facing the U.S. military as well. In November 2007, the U.S. Naval War College's network was forced offline for several weeks in order to prevent hackers from penetrating secured government computers. One month later the *New York Times* reported that a cyber attack originating in China attempted to access classified information from the nuclear weapons lab at Oak Ridge National Laboratory in Tennessee.

In August 2006, Gen. William Lord, director of information, services, and integration in the Air Force's Office of Warfighting Integration publicly stated that "China has [already] downloaded 10 to 20 terabytes of data from the NIPRNet," the Department of Defense's unclassified network.

Today, foreign hackers do not need to develop sophisticated techniques to access protected government data. During testimony before this Committee, Paul Kurtz, a national cybersecurity expert, stated that an insider with authorized access could exfiltrate more than one million pages of material with a microelectronic memory device the size of a hearing aid. He further noted that while a decade ago such technology was available to only a few intelligence organizations, today similar devices are widely available.

In order to maintain American prominence and influence, the U.S. government must recognize and confront the myriad cybersecurity challenges facing both the private and public sectors.

**Description of Comprehensive National Cybersecurity Initiative**

In January 2008, the Bush Administration announced the Comprehensive National Cybersecurity Initiative (CNCI, or "the initiative"). When first presented to Congress, most of the details were classified, including the Presidential Directives, budget, and underlying programs. At the urging of Congress and others, the Bush Administration released an unclassified summary of the initiative. The initiative is focused on increasing the security of the federal government's networks. It does not include specific proposals for increasing the security of private sector networks, including those that may be responsible for critical infrastructure. The Bush Administration stated they will address the security of the private networks at a future date.

Under the initiative, the Department of Homeland Security (DHS) leads the effort to secure the civilian Federal government networks. In addition, the Director of National Intelligence (DNI) will oversee the implementation of other classified aspects of the initiative. The Bush Administration divided its efforts under the initiative into three main focus areas:

- Focus Area I: Establishing Front Lines of Defense
- Focus Area II: Defend Against Full Spectrum of Threats
- Focus Area III: Shape the Future Environment

***Focus Area I: Establishing Front Lines of Defense***

Currently, the Federal information technology infrastructure has thousands of points where it accesses the internet, and hundreds of entities responsible for the security of the network. This diffusion of access points and responsibility has created a patchwork of systems, posing challenges to security. The intent of the initiative is to move towards a single network enterprise with responsibility for the CNCI divided between DHS and the DNI.

Deploy Trusted Internet Connections: The initiative's goal is to: (1) limit points of access to the internet to 50 or less; (2) expand DHS's U.S. Computer Emergency Readiness Team (US-CERT) with a 24x7 capability to oversee these access points; (3) support "e-Gov" initiatives; and (4) create a center for collaboration; the National Cybersecurity Center.

Deploy Passive Sensors Across Federal Systems: The initiative funds an Intrusion Detection System using passive sensors to analyze all internet traffic entering Federal systems. US-CERT's EINSTEIN program has this capability, and is already used within the Federal government. DHS is developing EINSTEIN 2, the next generation of the system, which, when deployed, will scan the content of internet packets to determine whether they contain malicious code.

Deploy Intrusion Prevention Systems: The initiative recognizes that malicious code must be stopped, not just identified. Intrusion prevention systems with real-time prevention capabilities will assess and block harmful code.

Connect Cyber Centers to Enhance Situational Awareness: The initiative proposes linking existing cyber centers to create a common operational picture. This will discourage agency-specific stovepipes, and lead to greater integration and understanding of the cyber threat.

***Focus Area II: Defend Against Full Spectrum of Threats***

Develop Government-wide Cyber Counterintelligence plan: The initiative recognizes that in order to address foreign state-sponsored cyber threats against U.S. interests, the Federal government must (1) improve the security of the physical and electromagnetic integrity of U.S. networks and (2) help assure the integrity of information that is housed in or transits U.S. networks.

Increase Security of Classified Networks: The initiative understands that the improper disclosure of information contained on the government's classified networks would gravely harm national security.

As a result, the initiative seeks to identify national security and mission critical systems, improve risk assessments and system interconnection management, coordinate incident detection and share vulnerability information across the Federal government.

Develop a Multi-Pronged Approach for Global Supply Chain Risk Management: The initiative seeks to better manage the United States' globalized supply chain, which is increasingly being targeted for exploitation, modification and potential disruption by a growing community of state and non-state actors.

***Focus Area III: Shape the Future Environment***

Expand Cyber Education: Today, the United States does not have a sufficient cadre of cybersecurity experts, nor an established cybersecurity career path for cybersecurity experts. The initiative plans to construct a comprehensive Federal cyber education and training program, with instruction including offensive and defensive skills and capabilities.

Coordinate and Redirect Research and Development (R&D) Efforts: To more effectively leverage government-wide research and development efforts, the initiative plans to better coordinate both classified and unclassified R&D for cybersecurity.

Define and Develop Enduring Leap-Ahead Technology, Strategies and Programs: The initiative calls for the U.S. government to invest in high-risk, high-reward research and development to achieve transformational change, working with both private sector and international partners.

Define and Develop Enduring Deterrence Strategies and Programs: The initiative tasks the Justice, State, Defense and Homeland Security Departments to develop a comprehensive cyber defense strategy that reduces vulnerabilities and deters interference and attack in cyberspace.

Define the Federal Role for Extending Cybersecurity into Critical Infrastructure: Recognizing that over 90% of the U.S. IT and telecommunications infrastructure is owned and operated by the private sector, the initiative seeks to define new mechanisms for the Federal government and industry to work together to protect the nation's critical infrastructure.

**Future Administration Position**

The Committee expects that the incoming administration will maintain this emphasis on cybersecurity. As a candidate, President-elect Obama spoke about the importance of cybersecurity, recognizing the United States' dependence on cyberspace. He also discussed ways to address this threat:

> "As President, I'll make cyber security the top priority that it should be in the 21st century. I'll declare our cyber infrastructure a strategic asset, and appoint a National Cyber Advisor who will report directly to me. We'll coordinate efforts across the federal government, implement a truly national cyber-security policy, and tighten standards to secure information – from the networks that power the federal government, to the networks that you use in your personal lives."

Following the election, President-elect Obama has declared his intention to name a Chief Technology Officer. In addition, a statement on the campaign website indicated that the incoming administration would "develop next-generation secure computers and networking for national security applications."

**Committee Actions**

The Committee has focused a great deal of attention on the emerging issue of Cybersecurity and the Administration's CNCI. In the 110th Congress, the Committee held three full committee hearings and two private industry roundtables, both in closed session, and one open hearing on this issue.

The roundtables included participants from internet service providers, internet security companies, software development firms and defense contractors. Generally, the participants were unsure how the individual components of the CNCI would collectively achieve the initiative's larger goals. Further, the internet service providers and software development firms consistently stated that in order for a new public and private sector partnership to succeed, the government must be willing to share more information.

In the report to accompany the Fiscal Year 2009 Intelligence Authorization Act, the Committee expressed its conditional support for this long overdue initiative. The Committee agrees with the initiative's broad approach but notes that some components of it do not seem well-connected and lack adequate governance mechanisms. Further, for the initiative to be successful, a new public sector and private sector partnership will need to be created, yet the excessive classification of the CNCI hinders necessary collaboration between the public and private entities. Chairman Reyes reiterated these concerns in his initial remarks to the HPSCI's open hearing on Cybersecurity held on September 18, 2008.

**Recommendations**

Threats to cybersecurity must be addressed by all elements of national power: diplomatic, military, economic, and intelligence. The Committee's recommendations focus on what can be executed in the Intelligence and, to a lesser extent, military arenas. This is not to say that these other areas are less important, to the contrary, the problem cannot be addressed without robust efforts in all areas.

This Committee's area of expertise is in the national security arena, and thus our recommendations are concentrated in this area. The Committee has assessed the current initiative and made recommendations on how it should proceed and has identified key debates for the future.

A comprehensive, national approach to the growing problem of cybersecurity is long overdue. While the Bush Administration should be commended for addressing the problem, it was started late in the Administration. Consequently, some of the more difficult policy and implementation issues have been left for the next Administration.

The Committee's recommendations are divided into those that focus on near-term issues and long-term issues.

**Near-term Issues**

In the near term, the CNCI, as defined by the Bush Administration, addresses the challenges of securing the government networks only, and not the private sector networks. Securing the government networks is no small task.

**Budget priorities may change, but funding priority should continue.** The Bush Administration established a baseline for resources for cybersecurity across the future year defense program (FYDP) through FY 2013. This eases the new Administration's task of allocating resources towards this important program. The incoming Administration will want to make adjustments to how that money will be spent and may reduce or slow funding until a future direction is better defined, but it should resist the temptation to reallocate all or most of the money for non-cybersecurity projects because the overarching cybersecurity plan is not in place. The temptation will be strong, with fiscal pressures growing stronger every day, but if the funding is reallocated it will be difficult if not impossible to restore, and there is much that is currently proposed to be funded in the CNCI that needs to be immediately implemented, no matter what changes might be made to the initiative's details.

**The initiative should contain clear goals and metrics to enhance program and Congressional oversight.** Many members of the Committee expressed frustration that the funding requests in the budget were ill-defined to ensure effective program and Congressional oversight. Smaller, manageable projects with discernable, achievable goals would enhance program oversight and lessen the risk of program delay or cancellation—as the Committee has seen with some larger, more complex government programs.

Programs should be sufficiently well-defined to ensure, both to higher levels of agency leadership and to Congressional oversight committees, that the money is being spent appropriately. A lack of definition of program goals may result in reductions of funding from Congressional committees, or in a failure to meet program goals. This is especially true in the Intelligence Community, which does not have the same layers of oversight and outside watchdogs that exist for agencies in the unclassified realm.

**Governance structure should be unified and government-wide.**
Currently, responsibility for the security of the network is fragmentary. The government network is only as secure as its weakest link, and therefore should be managed by a single entity. The scope and complexity of the problem demand clear leadership from the White House. The next Administration should appoint an officer within the Executive Office of the President who has the responsibility to evaluate and approve all cyber-specific and cyber-related funding across the Federal government agencies.

**Excessive secrecy hinders success of government efforts.**
Private industry has not been sufficiently consulted or informed of the details of the CNCI. Given that private industry has largely constructed and maintained much of the United States' IT infrastructure, the next Administration should leverage the private sector's knowledge of cybersecurity. The private sector can be an invaluable partner in securing America's cyber infrastructure if the U.S. government shares sufficient details of the CNCI and current, timely threats to cybersecurity.

## Long Term Issues

**Public-Private Partnership**
Private industry needs to actively partner in developing layers of broader solutions and longer-term approaches, such as working in international fora to change the infrastructure of the internet itself to make it more secure.

While some components of a comprehensive national strategy must remain classified (especially as pertains to U.S. capabilities to penetrate and/or attack foreign networks, so-called "sources and methods"), the preponderance of a successful cybersecurity initiative must be unclassified and transparent. This is especially true when it comes to securing the critical infrastructure networks that are run by private sector entities. Securing the financial system, the electrical grid, air traffic control and other civilian functions will require the cooperation and buy-in of both private industry and the public to be successful.

In this regard, the current initiative does not have a sufficient forum for sharing information with the private sector. The incoming Administration should develop a method of sharing information that appropriately balances the need to ensure that our private sector is properly informed of our vulnerabilities and the necessity of not allowing our adversaries to know our weaknesses. As the government works with the private sector, it must proactively work to allay concerns about privacy and the protection of civil liberties in order to gain that public buy-in.

**Legal authorities – technical capabilities will outstrip legal authorities.**

The government has tremendous technical capability to conduct electronic surveillance, some of which may exceed the legal authorities under the Fourth Amendment of the Constitution. This is not to say that the government exceeds these authorities, but without proper restraint and oversight it is technically possible. When the government does not restrain itself within constitutional boundaries, it raises concerns with the American people.

There is a risk that future Administrations might use the government's technical capabilities developed to prevent cyber intrusions to conduct surveillance that is beyond the Fourth Amendment's protections against warrantless searches. The Committee urges the incoming Administration to review existing legal authorities and propose legislation that meets the twin goals of preventing cyber intrusions while protecting the privacy of US persons. In proposing legislation, the Administration should consider whether there are sufficient oversight mechanisms and penalties for violation of the law. Such authorities should be considered before the American people's faith in their government is tested again.

**Clearer doctrine is needed for offensive cybercapabilities.** While elements of offensive capabilities must remain classified, a public discussion of cyber doctrine is necessary as part of a holistic approach to cyber space. Some of these pieces need to be developed by other elements of the national security establishment with the input of the Intelligence Community.

As part of the international community, the United States needs to begin to distinguish between cyber-crime by criminals and non-state actors, and cyber-attacks by foreign powers. At a minimum, as a policy goal, the United States should seek international cooperation to increase internet security so that critical infrastructure is not vulnerable to the equivalent of "guerilla" attacks by non-state actors and asymmetric threats. The international community has a serious interest in the stability and security of the internet for global commerce, communication, and security.

In this debate, there are many unanswered questions. Does the United States have "cyber red lines?" How does the United States define a "cyber attack?" What is U.S. doctrine on "first use" of cyber weapons against an adversary? The doctrine, policy and technology for offense and defense are inextricably intertwined and need to be dealt with in a coherent manner.

In answering these questions, the Intelligence Community's role is critical. The IC can develop indications and warning of cyber attack, understand the doctrine of other nations for use of cyber attacks against adversaries, and provide assessments on what forms such attacks are likely to take.

Within that debate, the United States must make some decisions about how an offensive cyber capability will be handled by the Federal government. The U.S. must reach some consensus over whether developing a cyber offense is a traditional military activity that should be handled under Title 10 authorities, or would be handled by the Intelligence Community under Title 50 authorities. Retaining offensive capabilities in the Intelligence Community may complicate efforts to persuade other nations to be overt about their own cyber warfare capabilities. On the other hand, in the military arena, the United States has encouraged other nations to be transparent about their capabilities, and a similar approach should be considered for cyber warfare capabilities. If an offensive military approach is selected, civilian agencies under Title 50 authorities will still play a key role because, in this arena, the defense and offense are inextricably linked.

**The CNCI provides a start, but long-term investment is needed to address the problem.** The investment in the foreign intelligence aspects of understanding and penetrating the threat is critical, as is the investment in cryptanalysis. It is important that our intelligence services and law enforcement agencies receive sufficient funding to improve their efforts to attribute cyber attacks.

Investment in R&D is also critical—and seriously under-funded at this point. The key is that investment in R&D needs to occur across a broader spectrum of network activities, in conjunction with the private sector, and not focused solely on the National Security Agency's requirements to implement the current CNCI technological approach.

In addition, the Administration needs to begin developing a cybersecurity workforce to help defend the nation against cyber attack. This is a long process, which could take a generation, but the U.S. needs to know what the training and education requirements are for such individuals, as well as what the size of such a workforces should be.

**Finally, the nature of Cybersecurity challenges Congressional oversight.** Currently, jurisdiction is shared by at least four authorizing committees and as many appropriations sub-committees. Each committee may have a different perspective on the problem, and may try to balance the issues towards their own equities. As with many complex issues, fragmentary Congressional oversight may hinder efforts at a uniform approach to the problem. A clearly articulated strategy for Congressional oversight will improve the effort.


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu