The House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
"Reviewing the Federal Cybersecurity Mission,"
James A. Lewis
Center for Strategic and International Studies
March 10, 2009

I thank the Committee for the opportunity to testify on the Federal Cybersecurity Mission. I believe that the new administration has a real opportunity to make a significant difference in improving our nation's security in cyberspace, but there are many difficult issues that it must address. The work of this committee will be essential for helping to guide that effort

As you know, the President directed that the National Security Council undertake a sixty-day review of the U.S. approach to cybersecurity. Federal officials involved in the review have told me that this is a forward-looking effort with a broad scope. It looks beyond securing Federal networks, which was the focus of the last administration's efforts, and will endeavor to lay out a strategic framework for the United States.

The decision to undertake this broad review is an important step forward for our nation. Cyberspace has become one of the central pillars of our economy and our national security. The adoption of network technologies since the 1990s by the United States has been a source of both competitive advantage and the rapid growth. The digital infrastructure is now essential. More importantly, expanding our digital advantage offers the possibility for continued increases in productivity and innovation. Securing cyberspace will help enable recovery and future growth.

Reaping the full advantage of digital technologies will require real improvement in cyber security. Estimates of the damage to our economy are imprecise, but millions of dollars are lost each year to fraud and theft, millions of dollars worth of intellectual property lost to foreign competitors, with the totally easily reaching into the billion. One of my fears is that as we increase spending on research and science as part of the stimulus package, we are actually subsidizing the research of our economic and military competitors since they can easily access work that cost us millions to develop for only a few dollars.

There is of course additional risk that insecure digital networks could allow foreign militaries and intelligence services, criminals, or other groups, to disrupt the provision of crucial services that are either provided by or depend upon digital technologies. It is easy to overstate the consequences of this sort of attack, and much of the discussion of cybersecurity over the last decade has involved some very silly and exaggerated scenarios for national disaster, but the risk is real and growing, and any national security strategy that does not address it is inadequate.

Where are we today in cyber security? From one perspective, we are in remarkably bad shape. In the last year, we have seen the networks of the two Presidential campaigns, secure networks at the U.S. Central Command and computer networks in Congress and other Federal agencies penetrated by outsiders. 2007 saw a number of significant penetrations of major Federal agencies by an unknown foreign power. The Secretary of Defense's unclassified email was hacked. The Department of Commerce's Bureau responsible for high tech exports off-line for more than a month. The networks of the Departments of State and Energy, NASA and other federal agencies were penetrated and according to public reports, immense quantities of information downloaded. The networks of federal contractors, the defense industry and other leading companies were also penetrated. Again, our statistics on this are imprecise, as companies prefer to conceal their losses or in many instances may not even be aware they have been hacked. Poor cybersecurity damages national security and drains our economy.

In response to this crisis, the Bush Administration created its Comprehensive National Cybersecurity Initiative (known as CNCI). This initiative made real progress in securing Federal networks. CNCI included Einstein, a technology that monitors federal networks for intrusion. It included the Trusted Internet Connection initiative, TIC. It looked at the question of how to use Federal procurements to improve cyber security in an effort know as the Federal Desktop core Configuration – FDCC. The CNCI included several other initiatives and projects, some of which were underway by the time the Bush administration ended. Overall, it was a major step forward.

However, the CNCI had several major drawbacks. It began in the last year of the Bush Administration. This late start was a serious impediment and one advantage for the Obama administration is that it came into office understanding that securing cyberspace is a major strategic issue. The CNCI was highly and unnecessarily classified. A few of its elements deserved being labeled top secret, but most did not, and the difficulties that over-classification created for coordinating with the private sector and with our allies seriously impeded the Bush administration effort. Finally, and most importantly, the Comprehensive National Cybersecurity initiative, despite its name, was not comprehensive.

This was its greatest failing. The CNCI focused on the “dot gov” space, on government networks, and while this is important, it is inadequate for cyber security. The task involves a global network largely operated by the private sector. The CNCI did not have a serious international component and it did not adequately address how to secure critical infrastructure or the “dot.com” space where most commercial activity takes place. These were serious shortcomings, and they point to crucial areas for work by the new administration.

At the same time that the previous administration began work on the CNCI, the Center for Strategic and International Studies created a commission to develop recommendations for the 44th Presidency on how to improve cyber security. CSIS is a nonpartisan, nonprofit research center organization headquartered in Washington, D.C. with more than 200 staff and a large network of affiliated experts. Its research focus is on security in a changing global environment. CSIS has been working on cyber security issues for many years and this work led us, in the face of the damaging events of 2007, to establish this Commission. When we began our work and for many months afterwards, we did not know of the CNCI. Officials involved in the CSNI initially declined our invitations to participate in order to preserve the initiative’s secrecy.

The report produced by this commission – I note that the other private sector witnesses on this panel were members of the group - laid out a truly comprehensive approach to securing cyberspace. Thirty eight thousand copies have been downloaded from the CSIS website. We were guided by the conclusions that Federal disorganization and an over-reliance on voluntary efforts had damaged our national security. To summarize our recommendations:

- Create a comprehensive national security strategy for cyberspace that uses all the tools of U.S. power in a coordinated fashion – international engagement and diplomacy; military planning and doctrine, economic policy tools and the involvement of the intelligence and law enforcement communities. .
- Publish a public doctrine for cyberspace. The President should state publicly that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the U.S. will protect it, using all instruments of national power.
- Clarify governance and responsibility for cyber security and establish White House leadership for cybersecurity based on Presidential Strategy and Directives.
- Use regulation to set minimum standards for securing cyberspace, to ensure that the delivery of critical services can continue when we are attacked.
- Mandate strong authentication for access to critical infrastructure**.** Strong authentication can significantly improve defense, if it is done in a way that protects privacy and civil liberties.
- Use acquisitions policies and rule to drive security, to encourage .the development and use of products and services that are secure, based on standards and guidelines developed in partnership with industry.
- Build human capital and improved technologies for securing cyberspace by expanding research, training and education.
- Refocus and strengthen public-private partnerships and focus them on action, not information sharing. Build on the CNCI effort, as part of a larger and more transparent comprehensive effort to secure cyberspace.

It is a lengthy list, but this reflects the overarching importance of cyberspace to our nation and the complexity of the problems involved in securing it. I believe that the issues we identified are central for improving national security and the sixty-day review must address them.

Two recommendations deserve additional scrutiny in the context of the sixty-day review. These are governance and regulation. We had a lengthy set of discussion in the CSIS commission on how best to organize for cyberspace. We considered many agencies for the lead role, including the Departments of Defense and Homeland Security, the FBI, the General Services Administration, and the Intelligence Community.

Three problems drove us to reject an agency-led approach. First, the mandate of any one agency would have to be greatly expanded to fully cover cybersecurity. Agency legal authorities differ widely and none - law enforcement, military or intelligence – are by themselves adequate for the range of cyber problems. We did not think that a super agency with broad domestic and international powers made sense. Public perception is important. Giving the intelligence community the lead in cybersecurity, although initially attractive to some of us because of the strong capabilities these agencies possess, would trigger powerful antibodies in the privacy community and the public, particularly after the experience of the previous administration's warrantless surveillance program and the struggles over FISA renewal.

The previous administration gave the Department of Homeland Security a central role in cyber security. We concluded that this was a mistake. While DHS has an important role to play, it lacks the competencies to deal with the range of issues involved in cybersecurity or to successfully engage in conflict with foreign militaries and intelligence services. DHS also lacks the interagency stature to direct other, more powerful agencies.

Giving DOD the lead could be interpreted as “militarizing’ the internet and would likely also provoke a reaction from both the privacy and the international communities. Foreign nations track U.S. policies closely and a decision to give DOD the lead in securing cyber space would be interpreted as a decision by the U.S. to make military action the focus of its cyber efforts. This would not be in our interest, as we will need to build a collaborative international approach to improve security.

At the end of the discussion, we concluded that only the White House had the authority to bring many large and powerful agencies to follow a common agenda and to coordinate with each other. A successful approach to cybersecurity blend intelligence, law enforcement, military, diplomatic and domestic regulatory functions. Coordinating these various functions can be best done from the White House. In recommending a White House lead, we emphasized that a “cyber czar” is not the right solution. The new administration went through a brief fascination with czars of various shapes and flavors for different issues; our view is that for cyber security, the overly centralized approach implied by a czar will fail. The White House and only the White House can set strategy and policy, ensure that agencies are following them and resolve agency disputes.

Regulation is the second issue that deserves extra attention. Our report concluded that the market would never deliver adequate security and the government must establish regulatory thresholds for critical infrastructure. We proposed a new, more flexible approach to developing regulation that was based on close cooperation with industry in developing standards and an avoidance of prescriptive regulations that spell out in precise detail what companies must do.

Regulation poses a number of challenges. The United States does not need regulations that are costly to implement yet deliver little in the way of improved security. Nor does the United States need regulations that are so diluted as to be meaningless. Finding the required balance will be difficult, but if we fail to use regulation to improve our national cyber security, if we do not identify mandatory actions to secure the digital infrastructure, the Obama administration will have no more success than any of its predecessors.

The stimulus package has inadvertently complicated the issue of regulation. The package includes significant funding for infrastructure projects, such as the Smart Grid. The package envisions that spending on infrastructure will build security into new projects. All this is good, but we then come to the question of what precisely needs to be done to make these new projects secure? Unfortunately, we do not know the answer to this and we do not have the time or people needed to develop that answer. A failure to invest in infrastructure modernization for more than a decade has makes it impossible to build both quickly and securely.

“Smart Grid” projects are an example of this problem. It uses advanced meters to measure the flow of electricity and allow it to be better managed. These new meters are based on internet technology. Unfortunately, if the new “smart” meters are not secure, they can be “hacked,” taken over by attackers, and used to disrupt the delivery of electricity. The United States does not have the guidelines it needs to guide make infrastructure secure.

I am not recommending that we delay stimulus investments while we sort out the requirements for cyber security. The most pressing task facing the new administration is to mitigate the suffering that the recession has brought and to take the steps needed to reduce unemployment and restore growth. Infrastructure investment is an important part of this. Years of underinvestment in infrastructure have put us in this unfortunate situation. However, regulation can play a role in remedying this problem, by giving government the ability to identify and mandate actions that mitigate new vulnerabilities. For example, a requirement that electrical companies strengthen authentication of identity on their control networks would improve security. But if we do not build the regulatory foundation now, the U.S. will be put at risk, and the task of laying the foundation falls squarely on the sixty-day review.

Regulation can also help reshape and strengthen public private partnerships. For more than a decade, the public dialogue has revolved around threadbare ideas on the need to defer to the private sector as it owns and operates the bulk of the critical infrastructure and on information sharing as an alternative to government mandates. In fact, the result has been to make public-private partnership less attractive or less important. The partnership groups often serve a largely "representational" function rather than one that is oriented towards action. Companies do not have "skin in the game." Regulate them, and they will come. Regulation is the key to improving public private partnerships, particularly if these partnerships are tasked with developing and maintain the standards upon which regulation must be based.

This administration has a unique opportunity. The U.S. has pursued a market-led approach to cybersecurity for more than a decade. This approach is inadequate. Now is the time to identify where regulation is needed to improve cyber security. Our recommendation was to begin with critical infrastructure – if a service is truly critical, we should not be afraid to require action to secure it.

I began by asking where we are today in cyber security and answered that, from one perspective, we are in remarkably bad shape. From another perspective, however, we are at a moment of tremendous opportunity. This administration can define an integrated and comprehensive Federal approach to securing cyberspace, something no previous administration has been able to do. The complexity of the problem means that it will take much longer than sixty days to put in place the policies, structures, and regulations we will need. However, if the sixty-day review can establish a clear governance structure led from the White House, if it lays out a broad plan of action for moving ahead, including the development of a comprehensive national security strategy and the use of regulatory authorities to secure critical infrastructure, and if this administration acts upon it, the review will be a success.