

**Testimony of Robert D. Jamison,  
Former Under Secretary of the Department of Homeland Security  
for the National Protection and Programs Directorate**

**Before the  
U.S. Senate Committee on Homeland Security and Governmental  
Affairs**

**Hearing on  
“Protecting Cyberspace as a National Asset: Comprehensive Legislation  
for the 21<sup>st</sup> Century”  
June 15, 2010**

Chairman Lieberman, Ranking Member Collins, Senator Carper and Members of the Committee, I appreciate the opportunity to testify before the Committee on the issue of Protecting Cyberspace as a National Asset. I also appreciate the Committee’s continued interest and activities in this vital area of national and homeland security.

Today, I will share with you my perspective on some of the key issues surrounding how we secure cyberspace and how I think your legislation can assist the effort. As you may recall, I have a diverse private sector, not-for-profit, and government background that impacts the way that I look at the complicated issue of cyber security. I spent over fifteen years at the United Parcel Service and the American Red Cross in senior management roles. This experience in the private and non-profit sector prepared me to enter government service during the last administration. I began my career in government service with the Federal Transit Administration at the Department of Transportation under the leadership of Secretary Norman Mineta. In addition to my normal duties as Deputy Administrator of FTA, I also had the opportunity to work helping to lead the Department’s recovery efforts in lower Manhattan immediately after the September 11<sup>th</sup> attacks, as well as lead the Department’s transit security efforts. That work led to my transition to the Transportation Security Administration (TSA) at the Department of Homeland Security (DHS), as the Deputy Assistant Secretary.

I was then confirmed by this Committee to lead the National Protection and Programs Directorate at the Department of Homeland Security. NPPD was a DHS component in transition from Preparedness Directorate to a risk-based, resiliency organization dealing with the critical issues of identity management, infrastructure protection, and cybersecurity and communications.

In this capacity, I led the Department’s efforts in the area of cybersecurity and communications. I was the senior Department official who assisted in the drafting of HSPD-23 and the Department’s implementation of the Comprehensive National Cybersecurity Initiative (CNCI). What I found when I arrived at NPPD in April of

2007 was an organization at a crossroads. The National Cybersecurity Division was staffed with bright hard working people tasked with the mission of securing our Federal government networks and working with the private sector to secure our nation's critical infrastructure and key resources. The US-CERT – United States Computer Emergency Readiness Team – had a small government staff and the tools they had deployed to detect malicious activity on our government networks were looking at flow analysis – but only after the fact. This limited capability, deployed on less than 40 of the civilian government's internet access points, augmented the security efforts of less than 1% of the government's internet traffic and data communications.

The Comprehensive National Cybersecurity Initiative had a dramatic impact on this limited DHS role. Not only did it solidify a common government strategy consisting of twelve specific initiatives across government aimed at improving our nation's cybersecurity and communications posture. It launched an execution plan to put our critical networks in a more defensible posture and initiated the deployment of critical automated monitoring capabilities and the dynamic, real-time sensors needed to defend against our cyber adversaries. It also, as you know, called for a more robust DHS cybersecurity role similar to its role in other homeland defense areas; outlined education and awareness programs; required supply chain security strategies, and much more.

The CNCI and the subsequent Cyberspace Policy Review ordered by President Obama acknowledge cybersecurity as one of the most pressing national security areas in a generation. And it called on the government, private sector, academia, and our international partners to work cooperatively together to begin to take the necessary steps to enhance the cybersecurity of our nation.

## **Cyber Landscape**

If you scan the cyber landscape today, what you find is a very diverse operating environment for an agency like DHS. An environment composed of operational networks, informational networks, and customer focused organizations with databases full of personal identifiable information.

You need only look to the Federal government to see we have multiple agencies with different missions, networks, authorities, and capabilities. US-CERT at DHS is primarily focused on operationally securing the dot gov networks. The Department of Justice is not only concerned with the law enforcement aspect but also the legal authorities that any agency has to execute its mission. The Department of Defense and the National Security Agency are focused on protecting our military networks, employing offensive measures, and determining what constitutes an act of war in cyberspace and how our government responds. The Department of State is focused on our international efforts. Department of Commerce is working on several fronts including issuing standards and guidelines through the National Institute of

Standards and Technology and working with the National Science Foundation and National Telecommunications and Information Administration on the educational, research, and governance fronts.

All of the Federal agencies are responsible for the protection of their respective networks and many, like the ones mentioned above, have responsibilities as it relates to our national cybersecurity strategy. Our Federal department and agencies are all on different evolutionary paths of cyber readiness and defense. Yet, they must all work together, cohesively and in partnership, to improve our nation's ability to prevent, detect, and respond to the cyber threats facing our great nation. The executive branch must continue to work with Congress to ensure we are on the right path in securing this vital national asset. And together we must ensure that as we proceed in this arena we are taking privacy and civil liberties in account at every step.

### **The Bill**

As Under Secretary of the National Protection and Programs Directorate, I was faced with many challenges and some persistent obstacles. My directorate in many ways did not have sufficient infrastructure in place to sustain the growth mandated by the Comprehensive National Cybersecurity Initiative (CNCI). The bill introduced last week by the Homeland Security and Governmental Affairs Committee directly addresses many of the challenges I faced and has the potential to leave the Department of Homeland Security better positioned with the necessary tools to execute its mission.

I believe one of the most important parts of the bill is the clarification of authorities, roles and responsibilities of various departments and agencies.

While conducting my duties as the senior official at the Department of Homeland Security on cybersecurity and communications issues, I can honestly tell you that I had authority I needed and the support of the leadership from DHS and the interagency. It may be old school, but I always encouraged my staff to step into the authority as outlined in HSPD-23 and execute the mission accordingly. However, I found it challenging at times to motivate my staff to embrace this charge. They often told me that they lacked the definitive clarification of authority to execute their mission and this sentiment was often echoed by many of our interagency partners. Sometimes you need that conviction of authority to drive the necessary actions and acceptance of the responsibility.

This seemingly minor nuance of authority and roles is a critical piece that must be addressed to position DHS for continued success. DHS and its partners have critical work to complete. We must ensure that we have the mechanisms in place to ensure that the nation's strategies are current and effective and ensure the rights of our citizens. **However, continued debate of roles and responsibilities and the reevaluation of cyber policy is delaying the execution of the most important**

**issue facing the United States government when it comes to cybersecurity: the continued consolidation of internet access points and ramped up deployment of dynamic, real-time sensors and capabilities that will position government networks to be more effectively defended.** Your legislation goes a long way to putting these authoritative issues to rest. It is clear that Federal civilian departments and agencies must work with the new National Cybersecurity and Communications Center at DHS to secure our government networks.

One of the most important management fundamentals that I have adopted in my professional career is ensuring the implementation an effective performance measurement and management program. Good performance management and the use of quality metrics have the potential to rapidly drive progress in both the private and public sector.

The capabilities that DHS and the government are deploying will result in an improved defensive posture and a much-improved situational awareness picture across the government domain. Commonly referred to as Einstein 2 and Einstein 3, these systems will also uniquely position DHS to have access to real-time network performance data that will be critical to driving compliance, spurring continuous improvement, and detecting anomalous network behavior.

With these systems, DHS will now be able to show Federal departments and agencies another perspective on their networks. DHS will be able to provide them with individual agency data, comparative data from the dot gov networks, and data from the private sector and our international partners. This comprehensive common operating picture will help to inform the CIOs and CISOs on what network security measures need to be evaluated and taken throughout their enterprise architecture. It significantly raises the baseline of cybersecurity across the Federal government. Having a performance management system to take advantage of that data is the key to success.

The Federal Information Security Management Act (FISMA) requires many practices that are fundamental to good network security such as inventory management, change management protocols, documentation, and testing. However, measuring network performance and security should be continuous and timely. Your bill allows us to move from a delayed audit based approach to the utilization of more timely, operational, and actionable information. It moves us from an annual “snapshot in time” approach to a continuous monitoring approach for the security of our networks with the performance responsibility resting with the cabinet level appointee, Chief Information Officer, and Chief Information Security Officer. Having the ability to look at what you call the “composite state of security” on a daily and ongoing basis will improve our defenses. And knowing and understanding the data will give us an opportunity to measure our improvement and success.

I draw particular attention to the improvement of cybersecurity for the Federal government and its systems, because it is difficult to speak with credibility to the

private sector when our own systems are significantly vulnerable. The work done under the CNCI and the subsequent Cyberspace Policy Review, coupled with your legislation lays the foundation to begin a more serious dialogue with the private sector. As the government works to secure its own networks, it will concurrently work cooperatively with the private sector to enhance the cybersecurity of our nation's critical infrastructure and key resources.

### **Hiring and procurement authorities**

Perhaps the most overwhelming challenge I faced when I moved from the Deputy at TSA to the Under Secretary of NPPD, was being able to quickly identify, recruit, and bring onboard a skilled cybersecurity workforce. While at TSA, I came to appreciate the TSA hiring authorities not only for their flexibility to allow the quick stand up a 60,000 plus workforce around the country to respond to transportation security threats, but for their ability to combine fairness with a more expeditious process. Similar flexibilities are needed to successfully execute the cybersecurity mission responsibilities at DHS, particularly as they rapidly ramp up their staffing. I can tell you from personal experience that some of my best employees and senior leaders were lured away by not only the private sector, but by other Federal agencies. It was difficult to compete with the compensation flexibility and incentives that other agencies and the private sector were able to offer. Going forward, DHS will need to heavily rely on these hiring flexibilities and incentives you have provided them to successfully execute the additional responsibilities in this bill.

The amount of time it takes to complete the hiring process, particularly the time from selection of a candidate to their first day of work was also a persistent problem. In a competitive environment, many candidates will not wait for the process to be completed. Our government must be able to not only hire the best and the brightest through an effective and efficient hiring process; but we must be able to bring them on board onto our watch floors and into our labs without an extended delay to clear the vetting and security clearance processes. Since the overwhelming majority of these jobs require security clearances, I firmly believe this issue needs to be addressed by this legislation.

The demand for cyber professionals is growing and will continue to grow. The nation must have a comprehensive hiring strategy and understand the changing demands for Federal government workers moving forward. We must get ahead of our workforce challenges and this legislation helps us do that. By asking OPM to investigate, identify and help provide solutions that agencies can use when it comes to internships, training, and part-time work, we will look to create a new generation of cyber warriors not just in Washington, D.C., but in every school and community in America. As we look at our hiring priorities as a nation, I would also encourage that we prioritize our most pressing needs and that we give the agencies with the most critical missions and staffing needs not only a focused strategy, but the competitive advantages to fill their vacancies.

## **Infrastructure Protection**

While I was at the Department of Transportation and while Deputy at TSA I became familiar with the work of the Office of Infrastructure Protection and its important mission. As the former Under Secretary of NPPD, I more than most understand and appreciate the linkages between the Office of Infrastructure Protection and the cybersecurity mission of the Department of Homeland Security. Through the National Infrastructure Protection Plan, commonly referred to as the NIPP, our government has developed a coordinated process to work with the nation's eighteen critical sectors. I suggest, as you do in your bill, that we need to continue to support this process and the vital coordination that it brings. The NIPP allows various agency responsibilities and sector needs to be coordinated giving us a comprehensive security plan that minimizes confusion and overlapping requirements and responsibilities.

If we think about the next generation FAA program and the smart grid deployment, we quickly realize that cyber issues permeate our daily lives. Cyber issues are not limited to communications or the information technology industry. They touch nearly every aspect of our lives from the time we wake up until the moment we arrive back home. Given the omnipresence of cyber in our society, DHS should continue to leverage the Office of Infrastructure (OIP) field presence, through their Protective Security Advisors, their important sector relationships – our government and DHS in particular can use years of foundational work to leverage private sector partnership to improve cybersecurity across eighteen sectors. One need only look to the success of the industrial control systems partnership between OIP and the National Cyber Security Division or the Cross-Sector Cybersecurity Working Group to realize the criticality of the relationship between these two DHS entities. Your committee held a hearing last year about cybercrime where you heard learned that not only are we facing nation state adversaries but organized criminal enterprises who are capable of carrying out large scale cyber intrusions against many sectors including our financial sector and many small and medium sized businesses. It is imperative we work with all sectors to ensure they are improving their cybersecurity baselines to confront the changing nature of the threats.

Your bill also recognizes the important relationship between the National Communications System (NCS) and the US-CERT. The NCS mission to ensure the redundancy and resiliency of our communications networks goes hand in hand with the critical mission of network and critical infrastructure defense. By working in partnership with industry through its major carriers and with the Federal Communications Commission, DHS through the National Coordinating Center has provided a 24/7 watch communications capability for this country. This capability augments the situational awareness and defense capabilities of US-CERT to more effectively understand the full common operational picture and to defend our networks.

As the nations communications infrastructure continues to migrate to internet based communications and as the cybersecurity mission matures, we are confronted with the inevitable convergence of these two areas. I am pleased that you recognize that these mission sets are inextricably linked.

### **Establishment Of NCCC As An Operational Entity**

The establishment of the National Cybersecurity and Communications Center as an operational component of DHS will place the necessary focus and emphasis on this mission area that it merits. As the former Deputy of TSA, I understand what it means to be an operational entity within DHS. It means not only having an operational mission, but more control over the critical support functions that are vital to your success. The mission and responsibilities of the NCCC demands that type of control. In addition, giving the NCCC hiring and procurement authority will assist their rapid growth as they step into their new responsibilities.

Before I close, I would like ask you to take a few issues under advisement. First, DHS must be careful not to divert key resources from the building of critical capabilities at the Department. I know from personal experience that the disparate demands of the mission and the magnitude of DHS's responsibilities can challenge the resources under your control. It is of vital importance that DHS maintain its focus, attention, and resources on quickly securing the dot gov domain. We must remember that it took the Department of Defense several years to ramp up their capabilities both in terms of node consolidation and the deployment of an effective perimeter defense. While their accomplishments should be commended, today, they still have work to do. As quickly as we want DHS to consolidate the nodes and establish a robust perimeter defense, we must allow them sufficient time to do it. This mission area is clearly within their capability and given the time and resources they should meet the challenges successfully.

Second, the diversity and magnitude of our critical infrastructure and key resources creates many challenges in effectively deploying capabilities and resources. This creates a resource challenge for DHS and I ask that the appropriate Congressional committees work with DHS and the Office of Management and Budget to determine what will be needed to carry out these responsibilities.

Finally, as this legislation moves through both chambers of Congress, we must remember that the dot gov defenses will and must evolve. This evolution will yield valuable lessons that will certainly impact critical infrastructure key resource standards and most likely will change and improve the requirements imposed by DHS. DHS must be nimble and build in flexibilities to its processes and procedures to account for that inevitable change.

## **Closing**

In closing, I think this important piece of legislation will improve the ability of the U.S. government and DHS to carry out its cybersecurity mission. You empower DHS by giving them critically needed authorities in the areas of hiring and procurement. Your bill clarifies the roles, responsibilities and authorities of the Federal departments and agencies. It moves the government to end debate on who should be doing what or who can do what and mandates progress. Finally, and to me most importantly, it lays the groundwork to accelerate the ramp up of Federal capabilities necessary to protect our nation's networks and critical infrastructure.

Again, I thank you for the opportunity to testify before you and I look forward to answering any questions you may have.