

**Remarks by Melissa E. Hathaway, Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils As Prepared for Delivery At the RSA Conference 2009, San Francisco, California**

April 22, 2009

As many of you know, I am Melissa Hathaway, the Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils. It has been my great honor to serve the President of the United States and the nation as part of the 60-day cyberspace policy review completed last week. I feel that it was just yesterday when we were celebrating New Years, and that was only "2" sixty-ish day periods ago! The days have been long and the task at hand has been the most challenging of my career.

**Introduction**

All humor aside, the United States really is at a crossroads. The globally-interconnected digital information and communications infrastructure known as cyberspace underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety and national security. This technology has transformed the global economy and connected people in ways never imagined. For example, my boys are 8 and 9 and use the Internet daily to do homework, blog with their friends and teacher, and to feed their Webkinz. As their mom, I stand before you today with no less than 3 blackberries and a pager! One of which will, apparently, self-destruct soon. I just have to figure out which one.

**The Threat and What's at stake**

Despite all of our efforts -- and I know that many of you understand well the challenges -- our global digital infrastructure, based largely upon the Internet, is neither secure enough nor resilient enough for what we use it for today and will need in to the future. This poses one of the most serious economic and national security challenges of the 21st century. The design of today's digital infrastructure was driven more by considerations of interoperability and efficiency than of security.

Consequently, a growing array of state and non-state actors are able to compromise, steal, change, or destroy our information. We have witnessed countless intrusions that have allowed criminals to steal hundreds of millions of dollars and allowed nation states and others to steal intellectual property and sensitive military information. They even have the ability to threaten or damage portions of our critical infrastructure.

One recent example from November 2008 illustrates both the speed and the scope of these challenges. In a single 30-minute period, 130

automated teller machines in 49 cities around the world were illicitly emptied.

These and other risks have the potential to undermine our confidence in the information systems that underlie our economic and national security interests.

A few hours south of here, there are creative Hollywood writers and actors who have imagined and produced stories that capture the essence of the problem, including: Matthew Broderick in War Games, Robert Redford in Sneakers, Sandra Bullock in The Net, and Bruce Willis in Live Free and Die Hard. These and other movies present the types of issues that we should care about and solve together.

Previous attempts to deal with cybersecurity in isolation have failed, in no small part, because they were perceived to be in conflict with the broader societal goals of progress and innovation, civil liberties and privacy rights. However, cybersecurity only succeeds in the context of broader economic progress. At times, it was a destination in itself, rather than a compass that guides us toward our objective. If treated in a broader context, cybersecurity will enable higher and far-reaching national goals, have better acceptance, and as a result, a greater chance for success. Our goals depend on trust, and trust cannot be achieved if people believe that they are vulnerable to fraud and theft or if they cannot depend upon the resources (infrastructure services, i.e., water, power, telephone service) being available when needed most. At the same time, security has no meaning if the application that serves society no longer is practical or usable. Stated differently, progress and security must not be viewed in a zero-sum fashion.

History has taught us that security, when pursued properly, enables innovation and growth and protects existing investments. In no small part, security is about protecting what already exists, creating a safe environment where innovation thrives unthreatened, and enabling the unencumbered natural growth for the future. Harmonized innovation and security are mutually reinforcing ideas; and policies, including our government's policies, must recognize and treat them as an integrated and synergistic whole.

It can be said that the Federal government is not organized appropriately to address this growing problem because responsibilities for cyberspace are distributed across a wide array of federal departments and agencies, many with overlapping authorities and none with sufficient decision authority to direct actions that can address the problem completely. We need an agreed way forward based on common understanding and acceptance of the problem.

This is why the President requested the clean-slate review.

Recognizing the challenges and opportunities, the President identified cybersecurity as one of the top priorities for his Administration and directed an early 60-day, comprehensive review to assess U.S. cyber policy and structures. The review addressed all missions and activities associated with the information and communications infrastructure, a.k.a. digital infrastructure. It included the missions of computer

network defense, law enforcement investigations, military and intelligence activities, and the intersection thereof with information assurance, counter intelligence, counter terrorism, telecommunications policies, and general critical infrastructure protection. I am not sure many people at the outset and possibly even now, understood the breadth of our task...and we had, effectively, two months to complete it! By the way, sixty days included the Saturdays and Sundays.

I assembled a team of experienced government cyber experts and in our first week we inventoried relevant presidential policy directives, executive orders, national strategies and studies from government advisory boards and private sector entities. We identified over 250 needs, tasks, and recommendations. We also solicited input from government departments and agencies on their specific cyber activities, authorities, and capabilities and requested them to identify any new or existing requirements that may not have been identified as part our initial inventory.

Scores of legal issues emerged during this review, such as the aggregation of authorities, data sharing with third parties within the Federal government, and liability protections for the private sector.

We successfully engaged a wide array of stakeholders inside and outside of the Federal government, including some of you here today. We engaged industry, academia, the civil liberties and privacy communities, State governments, international partners, the Legislative Branch, and others in the Executive Branch.

We know there are opportunities for everyone -- academia, industry, and governments -- to work together to build a trusted and resilient communications and information infrastructure. We engaged you and asked to be informed by you. We had more than 40 meetings with different stakeholder groups during those 60 days and received and read more than 100 papers that provided specific recommendations and goals. You helped us identify key requirements, illuminated policy gaps, suggested areas for improved collaboration, and framed the decision space for cyberspace policy. You will see your influence in our report when it is released in the coming days.

Our outreach involved unprecedented transparency and engagement for a National Security Council initiative and having come from the private sector myself, I recognized it was vital to the review's overall success.

When the report is made public you will see that there is a lot of work for us to do together and an ambitious action plan to accomplish our goals. Cyberspace won't be secured overnight and on the basis of one good plan. As they say, this is a marathon not a sprint. But with this review, we have taken the first steps to make real and lasting progress.

Sixty days' work is just the beginning of the beginning, and the pace for this marathon we're now running is one that we'd best set to ensure we have the legs to make it over the finish line. Being in security,

I've learned that security is just that, a marathon...and here in San Francisco, you can well appreciate it being an uphill run.

### **The Report**

Last Friday, April 17th, we completed our report and it summarizes our conclusions and outlines the beginning of a way forward in building a reliable, resilient, trustworthy digital infrastructure for the future. It provides the President with recommendations for a White House organizational structure that can effectively address cyberspace-related issues and include, as I have mentioned, an action plan for identifying and prioritizing further work in this area. After the President and his Administration have had an opportunity to carefully review our report, we will begin discussing the results publicly.

**Having said that, I am able to share with you the 60-day movie trailer— if you will...**

It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and to ensure that the United States and the world can realize the full potential of the information technology revolution.

This responsibility transcends the jurisdictional purview of individual departments and agencies because, although each agency has a unique contribution to make, no single agency has a broad enough perspective to match the sweep of the challenges.

It requires leading from the top -- from the White House, to Departments and Agencies, State, local, tribal governments, the C-Suite, and to the local classroom and library. The national dialogue on cybersecurity must advance now. We need to explain the challenges and discuss what the Nation can do to solve problems in a way that the American people can appreciate the need for action.

The United States cannot succeed in securing cyberspace if our government works in isolation. Cyberspace knows no boundaries. There is a unique opportunity for the United States to work with countries around the world to make the digital infrastructure a safe and secure place that drives prosperity and innovation for all nations.

The Federal government cannot entirely delegate or abrogate its role in securing the nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that government and private sector use in concert. The public and private sector's interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses

and government services depend. Information is key to preventing, detecting, responding to and recovering from cyber incidents. Again, this requires evolving our partnerships together. Government and industry leaders, both here and abroad, need to delineate roles and responsibilities, balance capabilities, and take ownership of the problem to develop holistic solutions. Only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution.

Building toward the architecture of the future requires research and development that focuses on game-changing technologies that could enhance the security, reliability, resilience and trustworthiness of our digital infrastructure. We need to be mindful of how we, government and industry together, can optimize our collective research and development dollars and work together to improve market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services. The White House must lead the way forward with leadership that draws upon the strength, advice and ideas of the entire nation.

**Please get involved and have a view**

It takes a combination of strategies aimed at a handful of vital behaviors to solve weighty and persistent problems. The tasks we face are many and interdependencies profound.

During this 60-day review I had a chance to read the book "Influencer." The authors argue that peer pressure can help create social support and harness the power of everyone to make change. People who are respected and connected can propel people to act in ways that are hard to imagine.

I can think of no better venue and more connected people than all of you here today.

Can we call for changes in widely shared norms?

Are we ready to talk openly about the challenges we face and how we share the responsibility for reversing the trend? Can we create the conditions where innovation and security are mutually reinforcing and treat them as an integrated and synergistic whole? Can government and the private sector, national and international parties, accelerate the changes we need? And, if not us, then who? If not now, then when?

I worry about these questions every night; they infiltrate my dreams. And since the theme of this year's conference relies upon the influence of Edgar Allan Poe, I cite you words from his work, "A Dream. "

"A few evenings since, I laid myself down for my night's repose. It has been a custom with me, for years past, to peruse a portion of the scriptures before I close my eyes in the slumbers of night. I did so in the present instance. By chance, I fell upon the spot where inspiration has recorded the dying agonies of the God of Nature. Thoughts of these,

and the scenes which followed his giving up the ghost, pursued me as I slept."

I often wake up at 2:30 or 4:30 in the morning having "worked" the problem in my sleep...and sometimes even develop a good idea.

We need to sow the seeds for a national dialogue, nurture them, even see them in our dreams, to help this critical conversation grow.

Cybersecurity isn't only the responsibility of governments and corporations, but that of individuals, including each of us here today, as well.

### **Closing**

Protecting cyberspace requires strong vision and leadership and will require changes in policy, technology, education, and perhaps law. We need to demonstrate abroad and here at home that the United States takes cyberspace issues, policies, and activities seriously. Achieving this vision requires leadership and commitment from the highest levels of government, industry, and civil society. That leadership and commitment will allow the United States to continue to innovate and adopt cutting edge technology, while enhancing national security and the global economy.

I am proud of the momentum that we have garnered in the last two months and I believe that we have a strong view of what is needed to drive change. As Ralph Waldo Emerson said, "who shall set a limit to the influence of a human being?" Today, I ask each of you, who shall limit our influence if we work together? Only ourselves and as a testimony to that, I want to thank you for the opportunity to speak here today.

Oh yes, I almost forgot, this speech will now self-destruct, but don't worry... this is the Internet-age, there are already hundreds of copies which you can download online. Thank you.