STATEMENT FOR THE RECORD
BY THE HONORABLE MICHAEL CHERTOFF
CO-FOUNDER AND MANAGING PRINCIPAL OF THE CHERTOFF GROUP
AND FORMER SECRETARY OF THE
U.S. DEPARTMENT OF HOMELAND SECURITY
FOR THE UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
FEBRUARY 16, 2012

I want to thank Chairman Lieberman, Senator Collins and members of the Committee for inviting me to submit a Statement for the Record and for the opportunity to contribute to this important effort that will ultimately determine how we protect our nation from today's growing and persistent cyber threat. I want to state clearly that I am submitting this Statement for the Record in my personal capacity, although, for the record, I am Co-Founder and Managing Principal of The Chertoff Group, a global security and risk management company that provides strategic advisory services on a wide range of security matters, including cybersecurity. Additionally, I am Senior of Counsel to the law firm of Covington and Burling, LLP.

The Internet as we know it today has evolved into a global system that is an essential element in our daily lives, global commerce and national security. From a remarkable technical achievement supporting a limited number of users, it is now a massive network. Because so many of our daily operations are now conducted in cyber space, they become a valuable target for daily attack by a variety of actors ranging from modern-day criminals interested in pure financial gain to nation states seeking to steal our technology or potentially to cripple our war-fighting or infrastructure. In my opinion, these cyber threats represent one of the most seriously disruptive challenges to our national security since the onset of the nuclear age sixty years ago.

But it is not my voice alone describing the importance of cybersecurity. The Director of National Intelligence Jim Clapper, our nation's most senior intelligence advisor to the President, elevated the discussion of cyber space in his recent testimony on the worldwide threat assessment calling it "one of the most challenging [threats] we face.[1]" FBI Director Robert Mueller expressed similar concern, stating "I do believe that the cyber threat will equal or surpass the threat from

[1] Remarks as delivered by James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment to Senate Select Committee on Intelligence, January 31, 2012.

counterterrorism in the foreseeable future.[2]" He continued by equating the challenge posed by today's cyber threat to that of terrorism by stating "the efforts that we put on counterterrorism, the same intensity, the same breaking down [of] stovepipes and the like [has to] be undertaken [with] regard to the cyber threat."

In 2007 and 2008, as Secretary of the Department of Homeland Security during the Bush Administration, I worked closely with the Directors of National Intelligence and the National Security Agency (NSA) to put forward the Comprehensive National Cybersecurity Initiative (CNCI), a now-declassified twelve point strategy to address cybersecurity threats across the civilian and military, government and private domains. Shortly after taking office, President Barack Obama ordered a review of the CNCI, and subsequently strongly reaffirmed the mandate to proceed with a national cyber initiative. President Obama appointed a White House official to coordinate strategy and Congress has taken up possible legislation.

Despite various government efforts, cybersecurity has become an increasingly urgent problem. Over the past year, there have been multiple reports of cyber intrusions across both industry and government, yet each presents different concerns and requires different levels of response. Nevertheless, there is still no comprehensive legislative architecture for cyber defense and security in place today. As I did recently when I signed a joint letter with seven other former executive branch national security officials, I again urge Congress to quickly act and pass comprehensive legislation that will quickly strengthen our nation's cybersecurity.

Looking across a spectrum of areas where legislation can help strengthen our ability to deal with the cyber threat, there are a number about which there should be little controversy. These include:

FISMA Reform – The federal government must continue to apply information security controls for Federal operations commensurate with risk, to ensure federal agencies and departments are consistently monitoring systems, evaluating information security protections and strengthening supply chain security.

Continued Investment in Cyber Education – In order to confront today's cybersecurity threats in both the near and long term, we must have a skilled workforce within government and

[2] Remarks as delivered by Robert Mueller, Director of the Federal Bureau of Investigation, Worldwide Threat Assessment to House Select Committee on Intelligence, February 2, 2012.

throughout the private sector. In addition, we should begin cybersecurity education efforts with the newest Internet users at an early age.

Research and Development – The Federal government needs to continuously support research and development to help us defend against the cyber threat. We need to make investments with innovative technologies that can become quick wins that will help us leap ahead and counter future threat evolutions, as opposed to playing catch up to attacks we have already seen.

But, in my view, in order to really make a difference and confront the growing cyber threat, we need to go further. There are three areas that I believe should be emphasized as a part of any comprehensive cybersecurity legislation: (1) risk-based security standards for our critical infrastructure, (2) information sharing, and (3) liability protections. These areas are reflected in the Lieberman/Collins/Rockefeller/Feinstein "Cyber Security Act of 2012" introduced in the Senate, as well as in a number of House bills and the Administration's own proposal.

Malicious cyber intrusions on privately owned networks may well be carried out – and even mounted – from or through platforms that are privately owned and domestic. These attacks currently steal billions of dollars in intellectual property. Worse yet, crippling of our privately owned transportation networks or our major financial institutions could have a catastrophic national impact, comparable to the effects of a major physical attack.

Some argue that cyber defense and security in our private sector are best left to the market and individual initiative and innovation. While it is true that the private sector has unleashed enormous creativity in developing aspects of our cyber economy, it is far from clear that market incentives will be sufficient to spur adequate investment in cybersecurity. Left to their own devices, few private companies would invest more in securing their cyber assets than the actual value of those assets. Yet in an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems. Thus, the market place is likely to fail in allocating the correct amount of investment to manage risk across the breadth of the networks on which our society relies.

Accordingly, responsibility for cyber security should be shared with the government for those privately owned networks and systems which are deemed critical infrastructure based on

interdependence or the essential nature of the services provided. Ownership and control of these networks should remain in private hands, but government is a particularly important partner because it can leverage what former Defense Deputy Secretary William Lynn previously described as "government intelligence capabilities to provide highly specialized active defenses."[3]

In this regards, the approach taken in the Lieberman/Collins/Rockefeller/Feinstein bill to securing private critical infrastructure is important. These proposals do not seek to impose detailed security regimes, but recognize that for identified highly critical infrastructure outcome-based performance standards are necessary. Such performance standards allow private owners the flexibility to innovate in achieving security, but also require in the end that the owners demonstrate that they have attained that appropriate level of security. Similar performance based approaches work well in promoting physical security in our ports, transportation networks, and other key infrastructure.

Will a standards-based mandate impose some cost on owners of essential infrastructure? Probably. But for those responsible owners already investing in adequate security, the marginal cost will be negligible. And for those who are not investing in sufficient security, the price of massive failure – and the collateral damage – will be far more costly.

Beyond setting standards and metrics for securing the most critical infrastructure, Congress must act to promote broader information sharing. In order to better protect our networks from known and emerging threats, both government agencies and private sector companies must have timely information, such as identification of signatures or patterns of behavior that are characteristic of malware. This allows faster detection of ongoing attacks before significant damage is done. We need appropriate guidelines to ensure information can be shared safely between the government and the private sector, so that the government can apply its capability to detect adversaries and convey that information to the private sector. By the same token, private enterprises also gain unique information about the threat as a result of the direct intrusions they are facing daily across multiple sectors. These also need to be shared broadly within the private sector and with the government. All of this must be done in a safe harbor without fear of legal impediments. The "Cybersecurity Act of 2012" includes limitations on liability in order to help facilitate voluntary information sharing for cyber threats. Information shared through appropriate channels cannot be used to trigger regulatory

[3] "Defending a New Domain: The Pentagon's Cyberstrategy," by William J. Lynn III, *Foreign Affairs*, September/October 2010.

enforcement or be the cause for civil or criminal action when such cyber security threat information is shared by a provider of cybersecurity services to a customer, shared with a government entity that manages critical infrastructure or provided to an appropriate cyber security information-sharing exchange.

The legislative efforts currently pending in Congress are important and long-awaited. Cyber attacks are costing us intellectual property and economic growth. One day, they may cost us lives. Congress should not wait to enact remedial legislation.

Thank you again for the opportunity to contribute my personal views on such an important topic that affects both our economic and national security.

###