Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016

February 2, 2016 at 6:07 PM ET by Lisa O. Monaco

Summary: Learn About How the Administration is Building on Past Successes and Driving Further Improvements in Our Nation's Cybersecurity.

Cybersecurity is one of the most important challenges we face as a Nation, and a top priority for this Administration. Since taking office, President Obama has made clear that as the cyber threat continues to increase in severity and sophistication, so must the pace of the Administration's efforts to counter this threat. As the President noted in his remarks at the White House Summit on Cybersecurity and Consumer Protection in February 2015, "we have to build stronger defenses and disrupt more attacks. We have to make cyberspace safer. We have to improve cooperation across the board...not just here in America, but internationally."

In 2015, the Administration achieved several important milestones in its efforts to protect the American people from cybersecurity threats and reinforce Federal networks against cyber intrusions. We know, however, that these achievements are not enough. In 2016, we will build on these successes and drive further improvements in our Nation's cybersecurity.

Raise the Level of Cybersecurity in Both the Public and Private Sectors

The cyber threat poses unique challenges with malicious actors able to ignore national borders, exploit benign systems and technology, and conduct harmful activity from hundreds or thousands of miles away. Many of our Nation's potential targets – much of our critical infrastructure; our financial and health information; and our own identities - are managed by private entities, rather than the U.S. government. Combatting the cyber threat is a shared challenge and a shared responsibility. Both the government and the private sector have developed extensive technical capabilities. Any effective response to this challenge requires close collaboration and coordination between the government and private sector.

That's why a key element in improving our cyber defenses is information sharing, not just within our government and between governments, but with the private sector. Over the past year, the Administration and Congress took several steps to enable improvements in information sharing. At the beginning of the year, the President signed an Executive Order promoting the creation of Information Sharing and Analysis Organizations (ISAOs) and sent Congress an information sharing legislative proposal. In February, the President directed the Director of National Intelligence to establish the Cyber Threat Intelligence Integration Center (CTIIC). And finally in December, Congress enacted and the President signed cybersecurity legislation that will make sharing information about cyber threats easier and more effective for the private sector and for the government. This legislation will help businesses better defend themselves and their customers from cybersecurity threats. It will also help the Federal Government better protect Federal networks and the nation.

In 2016, we will continue these efforts. We will implement the key element of the President's cybersecurity legislative proposal which was enacted by bipartisan vote— a single portal that will utilize the latest automation technology for the private sector to share cyber threat indicators with the Federal government. We will issue clear and transparent guidelines for companies and individuals on how to share information through the portal, and how the Federal Government will protect the privacy

of individuals. The information sharing community will also benefit from the release of standard practices guiding the formation and governance of ISAOs. And the CTIIC will bolster the government's cybersecurity capabilities by fusing intelligence and "connecting the dots" regarding malicious foreign cyber threats to the nation.

Of course, sharing or receiving threat information alone does not guarantee security. Businesses and the Federal Government must also take action. We continue to promote widespread adoption of baseline cybersecurity best practices through the use of the industry-built Cybersecurity Framework. In 2016, the National Institute of Standards and Technology (NIST) will evaluate whether updates are needed to the Framework based on stakeholder feedback it is collecting through a Request for Information (RFI), Views on the Framework for Improving Critical Infrastructure Cybersecurity. We will deepen our collaboration with key critical infrastructure sectors, such as financial services, energy, healthcare, transportation, and water, with the aim of broadening everyone's understanding of the threat and improving our ability to work together to thwart that threat.

We are committed to doing everything we can to share information and best practices with our private sector partners, and acknowledge that the Federal Government cannot confront this challenge alone. We will protect the critical infrastructure and information we safeguard and set the best possible example for those with whom we work. That's why in June 2015 the U.S. Chief Information Officer launched the 30-day Cybersecurity Sprint that identified a number of key cybersecurity actions for Federal departments and agencies. As a result, Federal civilian agencies increased their use of strong authentication for privileged and unprivileged users by more than 30 percent, and more than half of the largest agencies implemented strong authentication for nearly 95 percent of their privileged users. And we are following a Cybersecurity Strategy Implementation Plan to make sure that we continue to lead by example in hardening government networks. Finally, we intend to implement a series of improvements to Federal IT networks that will improve Federal cybersecurity in the short term and lay the foundation for the broad, systemic changes needed to truly make the Federal government more secure in the long run.

Disrupt and Deter Malicious Activity in Cyberspace

Raising our defenses is only one aspect of our efforts. We are also taking steps to disrupt our adversaries' malicious cyber activities and to deter them from carrying out those activities in the first place. In September, the United States and China agreed to a set of unprecedented bilateral cybersecurity commitments including that neither government will conduct or knowingly support cyber-enabled economic espionage for commercial gain. We also committed to establish a ministerial-level dialogue that will meet twice per year to provide accountability in ensuring the United States and China address significant cyber incidents of concern to both sides. The first U.S.-China High-Level Dialogue on Combatting Cybercrime and Related Issues took place in December 2015 and was a positive first step. While these are welcome first steps—we are not taking our eye off the cyber threat. As the President said in September, "the question now is, are words followed by actions. And we will be watching carefully to make an assessment as to whether progress has been made in this area."

We also achieved a major breakthrough on peacetime norms of responsible state behavior in cyberspace at the 2015 G20 Summit in Antalya, Turkey, where Leaders supported important principles that promote security and stability in cyberspace. The acknowledgement, acceptance, and adoption of these norms by the G20 are components of a successful deterrence strategy. In their Communique, Leaders affirmed that international law applies in cyberspace and that countries should not conduct cyber-enabled espionage for commercial gain. In 2016, we will encourage the implementation of these commitments and continue to promote an open, transparent, secure, and stable Internet that enables international trade and economic development, and fosters innovation and the freedom of expression.

However, even as we promote international cooperation, we must also hold accountable those who carry out malicious activity in cyberspace. Our cyber deterrence policy focuses on the development of improved defenses, more resilient architectures, and a range of options—cyber and non-cyber—to inflict costs and to hold accountable adversaries that choose to conduct cyber attacks or other malicious activity against U.S. interests. For example, in January 2015, the Treasury Department imposed new sanctions on North Korea for that country's involvement in the destructive and coercive cyber attack against Sony Pictures Entertainment. Last spring, the Department of Defense completed a new strategy to improve the military's capabilities to defend the Nation and deter aggression against U.S. interests in cyberspace. And in April, the President signed the Cyber Sanctions Executive Order, which provides a tool to impose economic costs on those who conduct certain types of malicious cyber-enabled activity that is likely to result in, or materially contributes to, a significant threat to the national security, foreign policy, economic health, or financial stability of the United States. The President has made clear that we will use these tools judiciously, but we will not hesitate to take action when needed to protect our interests.

Improve Incident Response and Resilience

Finally, we know that even with improved defenses and aggressive efforts to disrupt malicious activity, sometimes our adversaries may still succeed. Over the past year, we faced a wide array of intrusions, ranging from criminal activity to cyber espionage. We steadily applied the lessons learned from those events to improve our responses.

The vast majority of cyber incidents can in fact be classified as criminal activity – an intruder breaks in and steals something of value. For those incidents, we can make use of existing processes and capabilities. Other incidents, though, have a broad impact on our national security, economic security, foreign relations, public health and safety, civil liberties, or public confidence. And finally, there are incidents we haven't experienced yet, but that we should be prepared for: incidents that could resemble natural disasters, industrial accidents, or terrorist attacks by causing physical destruction. For these categories of incidents, we need to improve our structures and processes to handle them more effectively.

Companies, organizations, and government agencies should be prepared to respond to and recover from incidents. That's a best practice identified in the Cybersecurity Framework. But just as we are dedicated to sharing appropriate information with the private sector to better defend against cyber threats, we also stand ready to provide assistance to the private sector. For instance, the Federal Bureau of Investigation investigates malicious cyber activities; DHS provides technical assistance through its U.S. Computer Emergency Readiness Teams; and other sector-specific government agencies also stand ready to support private sector victims of cyber intrusions. In 2016, we will refine our policies and procedures to further strengthen our unity of effort response, whether it is helping a Federal agency or a private company. No victim should be left to respond alone.

Looking to the Year Ahead

Cybersecurity is a shared threat and a collective responsibility in this interconnected world. And it is a challenge that grows by the day, as we become increasingly reliant on our networks. The President issued a stirring call for action in his 2015 State of the Union Address, when he said, "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism…If we don't act, we'll leave our nation and our economy vulnerable. If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe." Our accomplishments in 2015 show that we can achieve a great deal through hard work and collaboration between governments,

industry, and private citizens. But there is much more to do. And we look forward to maintaining this momentum and making even more progress through the remainder of this Administration.