Cybersecurity Progress after President Obama's Address

July 14, 2010

I. Introduction

In his address in May 2009, President Obama announced his intention to make cybersecurity a priority for his Administration with a "new comprehensive approach to securing America's digital infrastructure." In the 14 months following that address and the release of the President's Cyberspace Policy Review (CPR), the Administration has taken concrete steps to achieve that goal, making cyberspace more secure.

The Cyberspace Policy Review included a number of near-term action items which built upon the Comprehensive National Cybersecurity Initiative (CNCI). The following is a progress report related to those action items and high-priority CNCI initiatives, and additional achievements of the past 14 months.

II. Cyberspace Policy Review

The President appointed a cybersecurity policy official and a Cybersecurity Directorate was created within the National Security Staff.

President Obama appointed a Cybersecurity Coordinator to provide White House leadership on cybersecurity issues. The Cybersecurity Coordinator leads a new Cybersecurity Directorate within the National Security Staff (NSS), works closely with the economic team, and has created a close partnership with the Office of Management and Budget (OMB) and the Office of Science and Technology Policy. In turn, this White House team works with Federal departments and agencies, State, local, and tribal governments, international partners, and the private sector.

The NSS Cybersecurity Directorate is preparing an updated national strategy.

The Cybersecurity Directorate of the NSS is developing an update to National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). NSPD-54/HSPD-23 established the CNCI and identified key cybersecurity roles and responsibilities across the Federal Government. This revised Presidential Directive will further elaborate and advance implementation of the strategy outlined by the CPR and executed through the CNCI and the actions laid out below.

Cybersecurity is being incorporated into the Administration's agenda as a key management priority.

Enhancing cybersecurity is a central component of the Administration's Performance Management Agenda. The Federal Chief Performance Officer has targeted key performance strategies for improving government operations, which include moving to real time monitoring and integrating cybersecurity into system design rather than bolting it on as an afterthought.

NSS and OMB released new guidance this year for the Federal Information Security Management Act (FISMA) on April 21, 2010. This new guidance shifts the focus from departments and agencies developing static, paper-based compliance reports to continuous, real time monitoring of Federal networks. Risk-based performance metrics are being established based on this real time monitoring, and these metrics will eventually be incorporated into senior official performance plans. This change means that agencies will be able to identify vulnerabilities faster and actively protect against attacks. The new approach builds on government and industry best practices that will make our cybersecurity efforts more effective.

RELATED BLOG POSTS

July 14, 2010 6:35 PM EDT
Progress Report on Cybersecurity
Cybersecurity Coordinator Howard Schmidt gives an update on progress since the release of the President's Cyberspace Policy Review last year.

June 25, 2010 2:00 PM EDT
The National Strategy for Trusted Identities in Cyberspace
Cybersecurity Coordinator Howard A. Schmidt releases the draft National Strategy for Trusted Identities in Cyberspace and asks for your input.

May 24, 2010 11:12 AM EDT
Recognizing our Government's Cybersecurity Experts

Special Assistant to the President and Cybersecurity Coordinator Howard A. Schmidt attends an awards ceremony at Fort Gillem, Georgia for one of the nation's top cyber-defenders.

April 21, 2010 7:48 PM EDT
National Collegiate Cyber Defense Competition
Howard A. Schmidt, Special Assistant to the President and Cybersecurity Coordinator, discusses his trip to the fifth annual National Collegiate Cyber Defense Competition in San Antonio, TX.

April 21, 2010 1:47 PM EDT
Faster, Smarter Cybersecurity
Federal CIO Vivek Kundra the new Federal Information Security Management Act guidance

March 02, 2010 3:52 PM EDT
Transparent Cybersecurity

Cybersecurity Coordinator Howard A. Schmidt reports that starting today, as part of the Administration's commitment to openness,

A privacy and civil liberties official has been designated.

Cybersecurity initiatives have been undertaken with greater transparency and with careful attention to privacy and civil liberties. The White House designated a privacy and civil liberties official to the NSS and released an unclassified description of the CNCI, which can be found at whitehouse.gov/cybersecurity. The Department of Homeland Security (DHS) released a Privacy Impact Assessment of the initial exercise preparing for enhanced network intrusion prevention capabilities – as part of the EINSTEIN program – using technology designed by the National Security Agency (NSA). The Department of Justice (DOJ) released opinions from its Office of Legal Counsel stating the deployment of the EINSTEIN intrusion detection and mitigation program to protect executive branch ".gov" networks is consistent with the Fourth Amendment and various privacy statutes. This Administration has regularly engaged with the privacy and civil liberties community and other stakeholders to ensure that appropriate protections are implemented at every step.

A national public awareness and education campaign is underway.

The Administration has pioneered new education initiatives and enhanced public awareness of cybersecurity. In March 2010, the Administration released the National Initiative for Cybersecurity Education (NICE) to enhance the recruitment, training, and retention of cybersecurity professionals, to raise public awareness, and to enhance cybersecurity education in our schools, building on and going beyond the CNCI initiative to expand cyber education. NICE consists of four tracks of work: a national public awareness campaign that is being led by DHS in partnership with the National Cybersecurity Alliance and other Federal agencies, formal cybersecurity education, Federal workforce development, and national workforce training.

U.S. positions for international cybersecurity policy framework are being developed, and international partnerships are being strengthened.

The United States is leading the way in an international dialogue to achieve greater cooperation among nations to defend against cyber threats. In partnership with like-minded nations and allies across the world, the United States has taken a lead role in international institutions, such as the United Nations, to make cybersecurity an international priority. The 64th U.N. General Assembly passed a unanimous resolution encouraging nations to evaluate their efforts to protect their critical information infrastructure, and providing a self-assessment questionnaire to assist in that review. In the U.N. Group of Governmental Experts (GGE) on cybersecurity, the United States is working to build understanding around the applicability of international law to conflict in cyberspace. The United States held several major cybersecurity bilateral discussions, initiated high-level dialogue with key partners, and joined with partners to combat cyber-enabled intellectual property theft.

At the same time, the United States has championed freedom on the Internet, including freedom of expression, association, religion, and the "freedom to connect" as an essential element of human rights in the 21st century. The United States is assisting human rights activists, journalists, and citizens around the world in their efforts to exercise these freedoms in the wake of some governments' attempts to thwart free expression.

A cybersecurity incident response plan is in final draft and will be exercised in September.

The National Cyber Incident Response Plan (NCIRP) should ensure a coordinated national response to a significant cyber incident. DHS is completing this plan on behalf of the Federal Government this summer, in consultation with Federal, State, local, and private sector partners. The plan will first be tested in September 2010 as part of the Cyber Storm III exercise, and revised based on lessons learned from that exercise.

A framework for research and development has been developed, with opportunities for continuing improvement.

The Administration has initiated game-changing research to counter growing and diverse cybersecurity threats. Building on CNCI Initiatives to coordinate and strengthen research and development and to promote leap-ahead technology, and in cooperation with the commercial and academic communities, the Administration has put forward a research and development strategy focused on three key themes: moving target (systems that move in multiple dimensions to disadvantage the attacker and increase resiliency), tailored trustworthy spaces (security tailored to the needs of a particular transaction), and cyber economic incentives (incentives that reward good cybersecurity and ensure crime does not pay). An opportunity for public input on the strategy was made available on the Networking Information Technology Research and Development (NITRD) program blog. This input will be used to develop concepts for budget initiatives expected to emerge in the fall 2010.

A draft cybersecurity-based identity management strategy and vision has been released for public comment.

The Administration has conducted an intense, year-long examination of how to ensure that identities of people,

all Americans now have access to the Comprehensive National Cybersecurity Initiative.

December 22, 2009 8:30 AM EDT

Introducing the New Cybersecurity Coordinator

Today the White House announced the President's new White House Cybersecurity Coordinator, Howard Schmidt. With some 40 years of experience in government, business and law enforcement, Howard brings a unique and deep experience to this important issue. Watch this video to learn more about his background and approach.

November 03, 2009 5:21 PM EDT

Cybersecurity Awareness Month Part V

Cybersecurity Awareness Month has wrapped up, and Assistant to the President for Homeland Security and Counterterrorism John Brennan reports on the success of a government-sponsored competition to identify future cybersecurity experts.

RELATED VIDEO

December 18, 2009 5:11 PM

A Commitment to Cybersecurity

FROM THE PRESS OFFICE

October 01, 2009 2:26 PM EDT

Presidential Proclamation - National Cybersecurity Awareness Month

May 29, 2009 11:54 AM EDT

Remarks by the President on Securing Our Nation's Cyber Infrastructure

May 29, 2009 10:18 AM EDT

Cybersecurity event fact sheet and expected attendees

organizations, and devices in cyberspace are trusted in collaboration with key government agencies, business leaders, and privacy advocates. The White House has released to the public for comment a draft National Strategy for Trusted Identities in Cyberspace (NSTIC) that outlines this vision to reduce cybersecurity vulnerabilities through the use of trusted digital identities. The NSTIC calls for the creation of an online environment where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential from a variety of service providers – both public and private – to authenticate themselves online for different types of transactions. The draft strategy includes important privacy protections and is based on a user-centric model that allows users more control of their private information.

III. Comprehensive National Cybersecurity Initiative

Implementation of the CNCI is strengthening the security of Federal networks. In addition to the CNCI initiatives mentioned above, notable items include:

Federal civilian networks are being secured.

Through the TIC and EINSTEIN programs, DHS has reduced the number of Internet access points in Federal networks and deployed intrusion detection technology at those points. Currently, this technology is operational at 12 of the 19 major Federal agencies, providing visibility into more than 278,000 indicators of potentially malicious activity per month.

DHS is testing more advanced capabilities as part of an intrusion prevention system (EINSTEIN 3). This system will respond to cyber intrusions in real time and leverage the advanced capabilities of the NSA within a robust oversight framework that protects privacy and civil liberties.

The cybersecurity operations centers are being connected.

New cybersecurity centers are integrating and providing real time situational awareness to combating cyber threats. DHS has established the National Cybersecurity and Communications Integration Center (NCCIC), integrating and eventually synchronizing the work of existing cyber and communication incident response mechanisms into a unified operations center. DHS also opened the Industrial Control System – Computer Emergency Response Team facility to address cybersecurity threats to critical infrastructure control systems. The National Cyber Security Center (NCSC) at DHS chairs a monthly meeting of the directors of the cyber centers across the Federal community and has initiated a significant cyber event conference call that all center directors can use 24 hours a day, 365 days a year.

A cyber counterintelligence plan is being implemented.

The National Counterintelligence Executive is coordinating the implementation of the new cyber counterintelligence plan. The plan adopts a variety of new mechanisms to reduce the threat to our networks from insiders and efforts by foreign intelligence services and other adversaries to compromise our networks.

The classified networks are being secured.

Various efforts are underway to increase the security of our classified networks.

Efforts are underway to better manage global supply chain risks.

The Administration has initiated significant changes to the DOD acquisition process to better manage cybersecurity risks stemming from an insecure supply chain. In the past year, DOD has revised its acquisition and program protection processes to require that risks affecting the integrity and pedigree of products, supplies, and services is considered and managed throughout the DOD acquisition lifecycle. Pilot programs have also been undertaken to ensure that supply chain risks to major systems are considered during the production phase. In addition, the National Institute for Standards and Technology (NIST), the General Services Administration (GSA), DHS, and DOD have been working with experts in industry and across government to standardize both government and commercial supply chain risk management best practices.

IV. Additional Progress

In addition to making progress on the near-term action items in the CPR and the initiatives of the CNCI, the Administration has had a number of other successes in the past year.

The establishment of the United States Cyber Command is unifying and strengthening the Defense Department's efforts to defend military networks and ensure integration of cyberspace operations.

With the confirmation of General Keith Alexander – who remains the Director of NSA – as the head of the U.S. Cyber Command, the Defense Department will achieve greater unity of effort across a full range of cyberspace operations, allowing commanders in the field to better defend the networks on which our

Soldiers, Sailors, Marines, Airmen, and Coast Guardsmen depend.

The Administration is leading the way in better securing the Internet's Domain Name System (DNS). The National Telecommunications and Information Administration (NTIA), with support from NIST and DHS, has worked since 2003 to spearhead the implementation of a security technology known as DNS Security or "DNSSEC." In July, the most significant step in that process will be completed, when the authoritative DNS root is signed. GSA and DHS have also worked to ensure that the ".gov" domain adopts better security practices, including DNSSEC, that assist in thwarting hackers and help Internet users reach correct and valid Internet sites. In addition, NTIA approved the implementation of DNSSEC within the U.S. top level domain (.us) and the domain used by academic institutions (.edu).

The United States Government is deepening its cybersecurity cooperation with the private sector and State governments, with a special focus on the Defense Industrial Base (DIB) and critical infrastructure. This effort builds on the CNCI and work previously underway by DHS, DOD, and others. DOD and DHS, in coordination with the Department of the Treasury, have initiated a pilot program for more in-depth sharing of cyber threat and technical data with private sector critical infrastructure partners – including classified or sanitized intelligence data. In another pilot program, the State of Michigan's government network is now monitored by the EINSTEIN 1 system. In the State of Washington, the National Guard Bureau conducted vulnerability assessments at the request of Governor Gregoire as part of an interagency partnership in furtherance of DHS's cybersecurity mission.

DHS has integrated cybersecurity into facility security and vulnerability assessments. These assessments capture data on facility systems vulnerable to cyber attack. Additionally, DHS conducts 50 cybersecurity assessments of critical infrastructure annually. DHS has also conducted cyber assessments in support of its Regional Resiliency Assessment Program and major national events including Super Bowl XLIV.

The United States Government is standardizing cybersecurity controls across national security systems and the rest of the executive branch. The National Institute of Standards and Technology published Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." This standard will make it easier for industry to help government, and for government best-practices to be used by industry.

The United States Government is coordinating the investigative response to cyber threats. Through the National Cyber Investigative Joint Task Force (NCIJTF), the Government identifies and mitigates cyber threats by integrating the counterintelligence, counterterrorism, intelligence, and law enforcement activities of 18 Federal agencies or departments. An alliance of peers, the NCIJTF is managed by the Federal Bureau of Investigation (FBI) and composed of agents, operators, and analysts from multiple agencies whose unified efforts result in actionable intelligence and successful investigations and operations that reduce, mitigate, or disrupt numerous cyber threats. During the last year, the NCIJTF completed a strategic shift, moving cyber threat investigations from a fragmented, reactive posture to a proactive, coordinated and highly successful national program.

Hackers and cyber criminals are increasingly being brought to justice. The FBI and United States Secret Service have worked to bring criminals to justice. The Secret Service has resolved over 1,100 cases and cracked the Heartland Payment Systems case that compromised over 130 million credit cards. Albert Gonzalez, a main defendant in that case, was sentenced to 20 years in prison. The FBI led an international law enforcement group which dismantled several international cyber criminal organizations. Two examples include the take-down of a Russian-led organization which penetrated over 300 financial institutions, including the Royal Bank of Scotland (RBS), where the actors coordinated the withdrawal of nearly $10 million in less than 24 hours from more than 2,100 ATMs in 280 cities around the world. Another FBI investigation brought down the perpetrators of a scheme that executed more than $4 million of unauthorized transfers from over 5,000 victims' accounts; this investigation culminated with the arrest of more than 100 conspirators by the FBI and Egyptian law enforcement. A third FBI investigation, conducted jointly with Italian authorities, led to the arrest of five Pakistani nationals who operated an Italian-based money transmitter company that supported the 2008 Mumbai attacks by funding the terrorist acts and activating the VoIP (voiceover IP) accounts that the terrorists used during the attacks.

Government and the private sector are partnering to reduce the financial risk from cyber threats. The United States Government and the private sector are working to educate businesses in reducing and mitigating their financial risk from cyber threats. The FBI collaborated with the Financial Services Information Sharing and Analysis Center to issue a timely, ground-breaking joint publication on cyber threats and mitigation strategies involving Automated Clearing House transactions.

Government and the private sector are working together to identify and reduce vulnerabilities for new devices like smart phones. Working together, NIST, NSA, and the private sector have created a checklist to identify vulnerabilities in smart phones. Many new phones are actually unified communication platforms that incorporate web browsing, still camera, video, and other functions, but the integration of these platforms creates

an ever more vulnerable system by multiplying each unique platform's vulnerabilities. The use of this checklist can reduce these vulnerabilities.

Government and the private sector are partnering to enhance the security and protection of industrial control systems. The Chemical, Dams, and Nuclear Sector-Specific Agencies within the DHS Office of Infrastructure Protection, in collaboration with public and private partners, have coordinated the development of control systems roadmaps aimed at providing owners and operators with a comprehensive framework and recommended protection strategies for improving the security and protection of control systems within critical infrastructure sectors, including tools, guidelines, and mechanisms focused on mitigating, preparing for, responding to, and recovering from a possible cyber event.