Statement for the Record
Of

Greg Schaffer
Acting Deputy Undersecretary
National Protection and Programs Directorate
Department of Homeland Security

James A. Baker
Associate Deputy Attorney General
Department of Justice

Robert J. Butler
Deputy Assistant Secretary of Defense for Cyber Policy
Department of Defense

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology
Department of Commerce

Before the
House Oversight and Government Reform Committee
United States House of Representatives
Washington, DC

July 7, 2011

Introduction

Chairman Issa, Ranking Member Cummings, and Members of the Committee, it is an honor for us to appear before you today to discuss the critical issue of cybersecurity. Specifically we plan to address the Administration's legislative proposal to improve cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

The Nation's digital infrastructure is fundamental to our economy, critical to our national security and defense, and essential for open and transparent government. Today, however, the same technologies that empower our citizens and organizations for good can be misused by some for harm.

The United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and limited comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Our critical infrastructure – such as the electricity grid, financial sector, and transportation networks that sustain our way of life – have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the last decade.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

Although the loss of national intellectual capital is deeply concerning, we increasingly face threats that are of even greater concern. We can never be certain that our information infrastructure will remain accessible and reliable during a time of crisis, but we can reduce the risks.

Recognizing the serious nature of this challenge, the President made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation." The President also highlighted the importance of sharing responsibility for cybersecurity, working with industry to find solutions that improve security and promote prosperity.

Over the past two years, the Administration has taken significant steps to ensure that Americans, our businesses, and our government are building better protections against cyber threats. Through this ongoing work, it has become clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated. We will never be fully insulated from cyber attacks. However, these proposals provide important steps in improving the cybersecurity posture of the United States. Members of both parties in Congress have come to the same conclusion as approximately 50 cyber-related bills were introduced in the last session of Congress. Senate Majority Leader Reid and six Senate committee chairs thus wrote to the President and asked for his input on cybersecurity legislation, while Members from both sides of the aisle have remained steadfast in their resolve to act. The Administration welcomed the opportunity to assist these congressional efforts, and we have developed a pragmatic and focused cybersecurity legislative proposal for Congress to consider as it moves forward on cybersecurity legislation. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace.

The proposed legislation is focused on improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers.

Protecting the American People

1) National Data Breach Reporting. State laws have helped consumers protect themselves against identity theft while also incentivizing businesses to have better cybersecurity, thus helping to stem the tide of identity theft. These laws require businesses that have suffered an intrusion to notify consumers if the intruder had access to the consumers' personal information. The Administration proposal helps businesses by simplifying and standardizing the existing patchwork of 47 state laws that contain these requirements with a clear and unified nationwide requirement. It also helps ensure that consumers receive notification, when appropriate standards are met, no matter where they live or where the business operates.

2) Penalties for Computer Criminals. The laws regarding penalties for computer crime are not fully synchronized with those for other types of crime. For example, a key tool for fighting organized crime is the Racketeering Influenced and Corrupt Organizations Act (RICO). Yet RICO does not apply to computer crimes, despite the fact that they have become a big business for organized crime. The Administration proposal thus clarifies the penalties for computer crimes, synchronizes them with other crimes, and sets a mandatory minimum penalty for attacks that damage or shut down computers that control our critical infrastructure.

Protecting our Nation's Critical Infrastructure

Our safety and way of life depend upon our critical infrastructure as well as the strength of our economy. The Administration is already working to protect critical infrastructure from cyber threats, but we believe that the following legislative changes are necessary to better protect this infrastructure:

1) Voluntary Government Assistance to Industry, States, and Local Government. Organizations that suffer a cyber intrusion often ask the Federal Government for assistance with fixing the damage and for advice on building better defenses. For example, organizations sometimes ask DHS to help review their computer logs to see when a hacker broke in. However the lack of a clear statutory framework describing DHS's authorities has sometimes slowed the ability of DHS to help the requesting organization. The Administration proposal will enable DHS to quickly help a private-sector company, state, or local government when that organization asks for help. It also clarifies the type of assistance that DHS can provide to the requesting organization.

2) Voluntary Information Sharing with Industry, States, and Local Government. Businesses, states, and local governments sometimes identify new types of computer viruses or other cyber threats or incidents, but they are uncertain about whether they can share this information with the Federal Government. The Administration proposal makes clear that these entities can share information about cyber threats or incidents with DHS. To fully address these entities' concerns, it provides them with immunity when sharing cybersecurity information with DHS. At the same time, the proposal mandates robust privacy oversight to

ensure that the voluntarily shared information does not impinge on individual privacy and civil liberties.

3) Critical Infrastructure Cybersecurity Risk Mitigation. The Nation's critical infrastructure, such as the electricity grid and financial sector, is vital to supporting the basics of life in America. Market forces are pushing infrastructure operators to put their infrastructure online, which enables them to remotely manage the infrastructure and increases their efficiency. However, when our infrastructure is online, it is also vulnerable to malicious cyber activities that could cripple essential services. Our proposal emphasizes transparency to help market forces ensure that critical-infrastructure operators are accountable for their cybersecurity.

   The Administration proposal requires DHS, in consultation with the appropriate agencies, to work with industry to identify the Nation's core critical infrastructure and to prioritize the most important cyber risks to that infrastructure. Representatives of critical infrastructure entities and standards setting organizations would then work together to propose standardized risk mitigation frameworks which focus not on compliance but instead on increasing actual security in a cost-effective manner. Then, each critical-infrastructure operator would propose a plan that identifies the steps it will take to address the identified risks as guided by the applicable framework. Each critical infrastructure entity's plan will be assessed by a third-party, commercial evaluator. Companies that are already required to report to the Security and Exchange Commission (SEC) would also have to certify to the SEC that they had developed and were implementing a risk mitigation plan. A high-level summary of the plan and the evaluation results would be publically accessible, in order to facilitate transparency and to ensure that the plan is adequate. In the event that the process fails to produce strong frameworks, DHS, working with the National Institute of Standards and Technology, could modify or produce a new framework. DHS can also work with firms to help them shore up plans that are deemed insufficient by commercial evaluators.

Protecting Federal Government Computers and Networks

Over the past five years, the Federal Government has greatly increased the effort and resources we devote to securing our computer systems. While we have made major improvements,[1] updated legislation is necessary to reach the Administration goals for Federal cybersecurity, so the Administration's legislative proposal includes:

1) Management. The Administration proposal would update the Federal Information Security Management Act (FISMA) and formalize DHS' current role in managing cybersecurity for the Federal Government's civilian computers and networks, in order to provide departments and agencies with a shared source of expertise. The legislation would also promote the ongoing transformation of FISMA toward increased automation and performance based security measures.

[1] *See* GAO, .*Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, March 5 2010.

2) Personnel. The recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, so we need to be sure that the government can recruit and retain these talented individuals. Our legislative proposal will give DHS more flexibility in hiring these individuals. It will also permit the government and private industry to temporarily exchange experts from the other, so that both can learn from each others' expertise.

3) National Cybersecurity Protection Program. The Administration proposal directs DHS to establish a program to actively protect federal systems and to continue the DHS efforts that are underway in this area. This program will include activities such as deploying intrusion detection and prevention capabilities, conducting risk assessments, and providing incident response and other technical assistance. DHS conducts many of these activities today under existing authority. For example, DHS is deploying what is referred to as the National Cybersecurity Protection System – of which the EINSTEIN intrusion detection and prevention capabilities are a key component. The EINSTEIN system helps block malicious actors from accessing federal executive branch civilian agencies, while DHS works closely with those agencies to bolster their own defensive capabilities. Despite progress in this area, deploying EINSTEIN to new agencies has sometimes been slowed due to the need for lengthy reviews and interagency agreements. To address this issue, the proposal will clarify DHS' authorities to protect federal systems. At the same time, strong privacy and civil liberties protections have been incorporated into the provision to protect the rights of federal employees and other users of federal systems.

4) Data Centers. The Federal Government has embraced cloud computing, where computer services and applications are run remotely over the Internet. Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law.

Protecting Individuals' Privacy and Civil Liberties

The Administration's proposal ensures the protection of individuals' privacy and civil liberties through a framework designed expressly to address the challenges of cybersecurity.

- It requires DHS to implement its cybersecurity program in accordance with privacy and civil liberties procedures. These must be developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All federal agencies who would obtain information under this proposal will follow privacy and civil liberties procedures, developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
- All monitoring, collection, use, retention, and sharing of information is limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement purposes only with the approval of the Attorney General.

- When a private-sector business, state, or local government wants to obtain immunity in connection with sharing of information with DHS, it must first make reasonable efforts to remove identifying information unrelated to cybersecurity threats.
- The proposal also mandates the development of layered oversight programs and congressional reporting.
- Immunity for the private sector business, state, or local government is conditioned on its compliance with the requirements of the proposal.

Taken together, these requirements create a new framework of privacy and civil liberties protection designed expressly to address the challenges of cybersecurity.

Conclusion

Our Nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. The Administration has responded to Congress' call for input on the cybersecurity legislation that our Nation needs, and we look forward to engaging with Congress as they move forward on this issue.

Greg Schaffer
Acting Deputy Undersecretary
National Protection and Programs Directorate
Department of Homeland Security

Greg Schaffer was named Acting Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) on June 5, 2011. Prior to that appointment, Mr. Schaffer served as Assistant Secretary for Cybersecurity and Communications (CS&C), a position he had held since June 1, 2009, when he was appointed by U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano. As Assistant Secretary, Mr. Schaffer worked within NPPD to lead the coordinated efforts of CS&C and its components, including the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System. He engaged the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm the Nation’s strategic cyber and communications infrastructure. Before joining the Department, Mr. Schaffer served as senior vice president and chief risk officer for Alltel Communications LLC, where he had responsibility for logical security, physical security, internal and external investigations, fraud, law enforcement relations, privacy and regulatory compliance. From 2004-2007, Mr. Schaffer held a variety of senior positions at Alltel—including chief risk officer, chief security officer and chief information security officer. For four years before joining Alltel, Schaffer was a director in PricewaterhouseCoopers, LLP, Cybercrime Prevention and Response Practice, where he developed and implemented computer forensic examinations in connection with major internal investigations at Fortune 500 companies. From 1997-1999, Mr. Schaffer served as a computer crime prosecutor in the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. Prior to joining the Justice Department, Mr. Schaffer was a partner with the law firm of Manatt, Phelps & Phillips, specializing in civil litigation related to computer technology issues. Mr. Schaffer holds a J.D. from the University of Southern California Law Center and a B.A. degree from the George Washington University.

James A. Baker
Associate Deputy Attorney General
Department of Justice

James A. Baker is an Associate Deputy Attorney General at the U.S. Department of Justice where he is responsible for a range of national security, cyber security, and other matters. Mr. Baker previously served as Counsel for Intelligence Policy at the Department from 2001-2007 where, among other things, he was in charge of representing the United States before the Foreign Intelligence Surveillance Court. In addition, he served as a federal prosecutor with the Department’s Criminal Division. From 2008-2009, Mr. Baker was Assistant General Counsel for National Security at Verizon Business. He has also taught national security law at Harvard Law School, and was a Fellow at the Institute of Politics at Harvard’s Kennedy School of Government. He is a graduate of the University of Notre Dame and the University of Michigan Law School.

Robert J. Butler
Deputy Assistant Secretary of Defense for Cyber Policy
Department of Defense

Mr. Robert (Bob) Butler is Deputy Assistant Secretary of Defense for Cyber Policy. He is responsible for providing insightful policy advice and support to the Secretary of Defense and other senior Department of Defense (DOD) leaders by formulating, recommending, integrating, and implementing policies and strategies to improve United States Cyber posture. This encompasses DoD policy relating to requirements, capability development, operations, declaratory policy, employment, and international cooperation or agreements. Mr. Butler served as an Account Executive with Computer Sciences Corporation (CSC), managing Defense Intelligence business with Combatant Commands and Military Services. He managed approximately 200 employees at over ten separate customer locations in the United States, Germany and the United Kingdom. He served as chairman of CSC's cyber technical working group coordinating cyber strategies across commercial, international and federal sector market spaces. Prior to his CSC employment, Mr. Butler served as a member of the career Senior Executive Service, and as the Associate Director, Joint Information Operations Warfare Command (JIOWC), Lackland Air Force Base, Texas. In this position, he advised the JIOWC commander and US Strategic Command leadership on key information operations issues and opportunities for providing superior support to combatant command and Department of Defense plans and operations. Additionally, Mr. Butler guided the development of JIOWC IO strategies and technologies to enhance mission support. Mr. Butler is a retired U. S. Air Force officer. From December 1979 to August 2005, he served in a variety of intelligence and communications-computer systems positions in the continental United States and Europe at the detachment, squadron, group, major command, unified command, Headquarters Air Force and Office of the Secretary of Defense levels.

Ari Schwartz
Senior Internet Policy Advisor
National Institute of Standards and Technology
Department of Commerce

Ari Schwartz serves as the Senior Internet Policy Advisor for the NIST Information Technology Laboratory. He represents NIST on the Department of Commerce Internet Policy Task Force, providing input on areas such as cybersecurity, privacy, and identity management. He also works with NIST Director Patrick Gallagher on IT-related standards issues. Schwartz came to NIST in August, 2010, after serving almost 13 years as Vice President and Chief Operating Officer of the Center for Democracy and Technology. Schwartz's work there focused on increasing individual control over personal and public information. He also worked to improve privacy protections in the digital age and expand access to government information via the Internet. While at CDT, Schwartz regularly testified before Congress and Executive Branch Agencies on these issues. He also led the Anti-Spyware Coalition (ASC), anti-spyware software companies, academics, and public interest groups dedicated to defeating spyware. In 2006, he won the RSA award for Excellence in Public Policy for his work building the ASC and other efforts against spyware. He was also named one of the Top 5 influential IT security thinkers of 2007 by Secure Computing Magazine.