Statement for the Record
of
Seán P. McGurk
Acting Director, National Cybersecurity and Communications Integration Center
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs Committee
Washington, DC

November 17, 2010

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee: I am Seán McGurk, the Acting Director of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) within the Office of Cybersecurity and Communications at the National Protection and Programs Directorate, and I have served for the last two years as Director of the Control Systems Security Program within the National Cyber Security Division. It is a pleasure to appear before you today to discuss the Department's cybersecurity mission and how we are coordinating with the nation's critical infrastructure asset owners and operators to reduce the cyber risk to industrial control systems.

Overview of DHS Cybersecurity Responsibilities

DHS is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. DHS serves as the principal federal agency to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, state and local governments, and the private sector to protect domestic critical infrastructure and key resources.

DHS takes threats to our private sector critical cyber infrastructure as seriously as we take threats to our conventional, physical infrastructure because our society and our economy depend on these networks and systems to operate effectively. A successful, large-scale cyber attack could have cascading effects across many sectors and around the world, which is among the reasons why President Obama identified our digital infrastructure as a national strategic asset.

In line with the President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, DHS has developed a long-range vision of cybersecurity for the nation's homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: (1) help create a safe, secure and resilient cyber environment; and (2) promote cybersecurity knowledge and innovation.

We are moving forward on this mission and working collaboratively with our public and private sector partners to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. At the Office of Cybersecurity and Communications (CS&C), we are working to enable and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats:

1. First, we continue to enhance the EINSTEIN system's capabilities as a critical tool in protecting our federal executive branch civilian departments and agencies.

2. Second, we are finalizing the National Cyber Incident Response Plan (NCIRP) in collaboration with the private sector and other key stakeholders. The NCIRP provides a framework for effective incident response capabilities and coordination to ensure that all cybersecurity partners—including federal agencies, state and local governments, the private sector and international partners—are prepared to participate in a coordinated and managed response to a cyber incident.

3. Third, and the focus of my testimony today, is our efforts to increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

As you know, the term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition (SCADA), process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as electricity, drinking water, and manufacturing. Control systems security is particularly important because of the inherent interconnectedness of the critical infrastructures and key resources (CIKR) sectors (i.e., water and wastewater treatment depends on the energy and chemical sectors, energy fuels transportation, and

other sectors, etc.). We also rely on control systems to operate our federal, state, local, and tribal governments; therefore, assessing risk and effectively securing industrial control systems are vital to maintaining our nation's strategic interests, public safety, and economic well-being.

Cybersecurity – Critical Infrastructure Protection

Our nation depends on the continuous and reliable performance of a vast and interconnected critical infrastructure to sustain our way of life. Although each of the critical infrastructure industries, from energy though water treatment, is vastly different, they all have one thing in common: they are dependent on control systems to monitor, control, and safeguard their processes.

A successful cyber attack on a control system could potentially result in physical damage, loss of life, and cascading effects that could disrupt services. As such, DHS recognizes that the protection and security of control systems is essential to the nation's overarching security and economy.

In May 2004, the Department established the Control Systems Security Program (CSSP) to guide a cohesive effort between government and industry to reduce the cyber risk to industrial control systems. As part of this effort, the CSSP works to protect critical infrastructure by providing expertise, tools, and leadership to the owners and operators of control systems. The CSSP also leads development and implementation of the Department's *Strategy to Secure Control Systems* (Strategy).

Strategy to Secure Control Systems

The strategy helps to guide efforts—both public and private—to improve control systems security in the nation's critical infrastructure. The primary goal of the strategy is to build a long-term common vision for effective risk management of Industrial Control Systems (ICS) security through successful coordination of efforts among public and private stakeholders. The strategy identifies CSSP as the lead in evaluating cyber risk and serving as the focal point for coordinating cybersecurity activities, including risk management and incident response, for critical infrastructure asset owners and operators.

Risk Management

The CSSP conducts operational cyber risk management activities and strategic readiness initiatives to manage cyber risk. The Industrial Control Systems Computer Emergency Response Team (ICS-CERT) is the operational arm of CSSP, acting as the focal point for analyzing and coordinating response to incidents and threats impacting industrial control systems. The ICS-CERT works in coordination with the United States Computer Emergency Readiness Team (US-CERT) and is a component of the NCCIC. With regard to strategic readiness, CSSP has a number of program areas focused on cyber preparedness and risk management, including conducting training classes, providing input to standards development, producing informational cybersecurity products and tools, conducting onsite cybersecurity assessments, and overseeing the Industrial Control Systems Joint Working Group.

In partnership with the Department of Energy, which is the Sector Specific Agency responsible for the Energy Sector under the National Infrastructure Protection Plan, the Industrial Control Systems Joint Working Group provides a vehicle for stakeholders to communicate and partner across all critical infrastructure sectors to better secure industrial control systems. The Working Group is a representative group comprised of owners and operators, international stakeholders, government, academia, system integrators, and the vendor community. The purpose of the Working Group is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, deployment and secure operations of industrial control systems.

As you are aware, cybersecurity training is essential to increasing awareness of threats and the ability to combat them. To that end, CSSP conducts multi-tiered training through web-based and instructor-led classes across the country. In addition, a week-long training course is conducted at CSSP's state-of-the-art advanced training facility at the Idaho National Laboratory to provide hands-on instruction and demonstration. This training course includes a "red team/blue team" exercise in which the blue team attempts to defend a functional mockup control system, while the red team attempts to penetrate the network and disrupt operations. The positive response to this week-long course has been overwhelming, and the classes are filled within a few days of announcement. To date, more than 16,000 professionals have participated in some form of CSSP training through classroom venues and web-based instruction.

CSSP also provides leadership and guidance on efforts related to the development of cybersecurity standards for industrial control systems. CSSP uses these industry standards in a variety of products and tools to achieve its mission.

First, CSSP uses and promotes the requirements of multiple federal, commercial and international standards in its Cyber Security Evaluation Tool (CSET) which has been requested by and distributed to hundreds of asset owners. Tool users are evaluated against these standards based on answers to a series of standard-specific questions. CSET is also used by CSSP assessment teams to train and bolster an asset owner's control system and cybersecurity posture in onsite assessments. In fiscal year 2010, the program conducted more than 50 onsite assessments in 15 different states and two U.S. territories, including several remote locations where the control systems represent potential single points of failure for the community. The program is planning for 75 onsite assessments in fiscal year 2011.

Second, the program developed the *Catalog of Control Systems Security: Recommendations for Standards Developers*, which brings together pertinent elements from the most comprehensive and current standards related to control systems. This tool is designed as a "superset" of control systems cybersecurity requirements and is available in the CSET and on the website for standards developers and asset owners.

Lastly, the CSSP provides resources, including time and expertise, to standards development organizations including National Institute of Standards and Technology (NIST), the International Society of Automation, and the American Public Transportation

Association. Experts provide content, participate in topic discussions, and review text being considered by the standards body.

As a member of the Smart Grid Interoperability Panel, CSSP participated in the NIST Cybersecurity Working Group, which extensively used the CSSP-developed *Catalog of Control Systems Security: Recommendations for Standards Developers* to create a framework for assessing and mitigating risk to Smart Grid technologies in NIST Report 7628, *Guidelines for Smart Grid Cyber Security*.

In addition to performing assessments and participating in standards development, the CSSP has also created a series of recommended practices and informational products to assist owners and operators in improving the security of their control systems. These information resources are publicly available online[1] and are also promoted through the Working Group and other sector forums.

Incident Response

While these strategic readiness activities help to reduce overall risk to control systems, the industry needed an operational response group to turn to when actual cyber incidents occurred. In 2009, the CSSP established the Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) to coordinate response to and analyze control systems-related incidents, conduct analyses of vulnerabilities and malicious software, and disseminate cybersecurity alerts and advisories to all sectors. The ICS-CERT provides a focused operational capability to provide owners and operators of control systems situational awareness and technical assistance in the event of an incident. The ICS-

[1] http://www.us-cert.gov/control_systems/

CERT, in coordination with US-CERT, also provides onsite incident response to organizations that require assistance in responding to a control systems attack. For larger scale cyber attacks and generally, ICS-CERT coordinates with the other NCCIC components including US-CERT, the National Communications Center, and DHS Intelligence and Analysis to ensure appropriate levels of awareness and technical support.

Upon notification of an incident, the ICS-CERT performs a preliminary diagnosis to determine the extent of the compromise. At the impacted organization's request, ICS-CERT can deploy a fly-away team to meet on-site with the company or organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow-on analysis. ICS-CERT provides mitigation strategies and assists asset owners and operators in restoring service, as well as recommendations for improving overall network and control systems security. In fiscal year 2010, ICS-CERT conducted 13 incident response activities to organizations in need. During these assist visits, infected systems were identified and sanitized, and steady state operations were restored. In all cases, ICS-CERT assisted the organizations in developing focused mitigation plans, and provided access to tools for follow-on defensive measures. The increasing call for support and value-add that the organization has demonstrated has led to the need to augment ICS-CERT's force, which we plan to do in fiscal year 2011.

Coordination and Integration

The ICS-CERT coordinates control systems-related security incidents and information sharing with federal, state, and local agencies and organizations, as well as private sector

constituents including vendors, owners and operators, and international and private sector computer emergency response teams.

In addition, the ICS-CERT leverages relationships with many working groups – including the Industrial Control Systems Joint Working Group and the Federal Control Systems Security Working Group – to increase and improve information sharing with critical infrastructure asset owners and operators and vendor community. It is through these relationships that private sector partners and vendors have called on the ICS-CERT during control systems emergencies and events.

In 2007, the CSSP studied several scenarios to evaluate the impacts of a successful cyber attack on critical control systems infrastructure in several critical infrastructure sectors, including energy and transportation. The studies used hypothetical, but credible, cyber attack scenarios that employed common hacking methods and knowledge of control systems. Consequences of the attacks ranged from multiple-day shutdowns of facilities without death or injury, to extensive system damages, casualties, and billions in economic loss. The scenario development took advantage of open source literature, in-house and industry cyber experts, CSSP research and documentation, and engineering analysis to assess the feasibility of a cyber attack and derive the outcomes with assessed damage. Additional scenario development and analysis was conducted for cyber attacks on a nuclear power generation plant, an electricity-generating station, and a large industrial facility. This analysis also yielded estimated consequences resulting in significant economic impact, major disruption to services, injuries and potential loss of life.

Stuxnet

While scenario analysis plays an important part of understanding and reducing risk to critical infrastructure, a real-world threat emerged earlier this year that significantly changed the landscape of targeted cyber attacks. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware. What makes Stuxnet unique is that it uses a variety of previously seen individual cyber attack techniques, tactics, and procedures, automates them, and hides its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring. The concern for the future of Stuxnet is that the underlying code could be adapted to target a broader range of control systems in any number of critical infrastructure sectors.

The ICS-CERT immediately began to analyze the code and coordinate actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers.

Our analysis quickly uncovered that this sophisticated malware has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. The malware is highly complex and contains over 4,000 functions, comparable to the amount of code in some commercial software applications.

Leveraging the unique capabilities and partnership with the Idaho National Laboratory, ICS-CERT was able to conduct sophisticated analysis on Stuxnet. ICS-CERT has documented that the malware was written to look specifically for computers running the Siemens WinCC Human Machine Interface (HMI). It then copies components into the associated Structured Query Language (SQL) database and checks to see if the HMI is connected to certain Siemens Simatic Programmable Logic Controller (PLC) models. If it finds the specific model of PLC, Stuxnet then checks for specific program elements in the PLCs and, if found, attempts to install rogue ladder logic into the PLC program.

ICS-CERT analysis indicates that the logic is only changed when these specific conditions are met. This selective infection criterion, along with the analysis of the logic injected by Stuxnet, indicates that a specific process was likely targeted. However, while we do not know which process was the intended target—it is important to note that the combination of Windows operating software and Siemens hardware can be used in control systems across critical infrastructure sectors—from automobile assembly lines to mixing baby formula to processing chemicals.

Furthermore, ICS-CERT concluded that Stuxnet was professionally created using carefully planned development concepts. The malware implements state-of-the-art techniques and capabilities for infecting a system, preventing detection (to maintain its presence), exfiltrating data, and inhibiting analysis once the code is detected. In other words, this code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product, and indicate to the operator and your anti-virus software that everything is functioning as expected.

To combat this threat, the ICS-CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July. To date, the ICS-CERT has briefed dozens of government and industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit.

Looking ahead, the Department is concerned that attackers could use the publicly available information about the code to develop variants targeted at broader installations of programmable equipment in control systems. The ICS-CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, on-site incident response activities, and information sharing and partnerships. The salient lesson of Stuxnet, and other emerging threats, is that the CSSP mission and coordination between DHS and the control systems community are vital to our efforts to protect the nation's critical infrastructure.

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, let me end by thanking you for the strong support you have provided the Department. Thank you for again for this opportunity to testify. I would be happy to answer your questions.