Statement for the Record
of
Seán P. McGurk
Director, Control Systems Security Program
National Cyber Security Division
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Washington, D.C.

July 21, 2009

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I am Seán McGurk, the Director of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) at the National Protection and Programs Directorate. I am pleased to appear before you today to discuss the importance of securing the control systems that operate our critical infrastructure.

A control system is a general term that 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 in our electric power grid is particularly important because of the significant interdependencies inherent with the use of energy in all other sectors. Additionally, we rely on the electric grid to operate the Federal, state, and local, tribal governments; therefore, assessing risk and effectively securing industrial control systems are vital actions to maintaining our Nation's strategic interests, public safety, and economic prosperity.

In 2003, the National Strategy to Secure Cyberspace designated DHS as the lead agency for cybersecurity. Since then, Homeland Security Presidential Directives (HSPD) 7 and 23 have established national policies and further outlined the Department's responsibility to collaborate with public and private sector entities to evaluate emerging technologies.

Additionally, various Government Accountability Office (GAO) reports (e.g., GAO report: *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*) have further shaped Federal activities to improve the security of critical infrastructure and key resources (CIKR) by identifying the risks that could impact the networks that operate our critical infrastructure. In May 2004, DHS created the Control Systems Security Program (CSSP) to further this mission and lead a cohesive effort focused on reducing the cyber risks to the control systems that operate the CIKR.

To establish a framework to secure the CIKR, DHS issued the National Infrastructure Protection Plan (NIPP). This plan identifies the CSSP as responsible for leading activities to reduce the likelihood of success and severity of impact of cyber attacks against our Nation's control systems. The CSSP recognizes that understanding the threats, vulnerabilities, and subsequent mitigation strategies is essential in securing industrial control systems.

The CSSP funding for fiscal year 2009 is $22 million, an increase from the previous year's budget of $12 million that enabled us to expand and enhance the Advanced Vulnerability Discovery facility. This facility provides advanced modeling and simulation capabilities that will aid in identifying the interdependencies of the infrastructures. Additionally, the Federal workforce increased from one position to an authorization for nine Federal employees. For FY 2010, the President's budget request included an increase of $5.56 million for the CSSP. With these enhancements, DHS will be able to evaluate new technologies and begin assessing risk across additional CIKR sectors. CSSP continues to build a culture of reliability and security by partnering with government agencies, industry, and the international community to reduce the cyber risks to U.S.-based control systems and evaluate emerging technologies such as the Advanced Metering Infrastructure and the Smart Grid for the energy sector.

In order to understand the risks, it is important to understand the threats, including actors and motivations, not only to control systems, but to digital computing in general.

- Common hackers comprise the most prevalent group of cyber attackers. They attempt to break-in or hack into computer systems or exploit flaws in software to circumvent systems security. Often the motivation is data exfiltration for financial

gain. Other hackers install backdoors such as Trojans or other software such as rootkits that enable them to remotely access the system or device at a later date to perform a variety of nefarious actions.

- The insider is a dangerous threat to control systems because the individual has internal knowledge to processes and components. Insiders can defeat security measures put in place even when entities follow best practices and procedures.
- Cyber-terrorists or hacktivists are those who seek to disrupt Internet activity in the name of a shared ideology or personal, political, or social cause. These actors collaborate via cyberspace and work as an organized group against their targets to further their political or social agenda. Web defacements, denial of service attacks, and redirects are the most common acts carried out against a target or targets.

These security challenges offer opportunities for malicious actors to attempt to penetrate our critical infrastructure using the vulnerabilities in advanced technologies such as the Smart Grid.

The CSSP evaluates risk and serves as the focal point for coordinating numerous resources to assist all critical infrastructure entities, including the members of the electric power grid. The CSSP conducts operational cyber risk management activities and leads strategic initiatives to develop the mitigation plans to manage cyber risk to an acceptable level. These activities include: control systems sector analysis of vulnerabilities and interdependencies; scenario development; vendor product assessments; incident response activities; and the development of assessment tools, information products, and training.

In 2006, CSSP conducted an analysis based on the premise of using the electric grid to attack a nuclear facility (originally this was the "PANDORA" analysis that later became "AURORA"). This analysis was performed at the Control Systems Analysis Center (CSAC) operated by the Department of Energy's Idaho National Laboratory. The CSAC's analysis demonstrated how a perpetrator could use the electric utility system to produce significant nuclear plant apparatus and systems. It is important to note that this vulnerability was not related to a specific or imminent threat, and that the vulnerable control system and the

equipment which could be damaged by an attack are often owned by two different entities. The analysis highlights the importance of assessing risk, interdependencies, and the need to secure industrial control systems in order to maintain our Nation's strategic interests, public safety, and economic prosperity.

While these efforts result in cybersecurity strategies that help to increase the overall security of the electric grid, they do not protect the grid from attacks. DHS works closely with the Department of Energy in providing mitigation measures that reduce the risk of cyber attacks, such as those exploiting the AURORA vulnerability. DHS works directly with the sector specific agencies such as the Departments of Defense and Energy, The Federal Energy Regulatory Commission (FERC) and the Nuclear Regulatory Commission (NRC), as well as with our private sector partners such as the North American Electric Reliability Corporation (NERC) to help them secure their infrastructure assets through voluntary programs.

The Secretary of Homeland Security takes the issue of securing our Nation's critical infrastructure very seriously and continues to emphasize an all-hazards approach to a safe and secure homeland. The CSSP focuses on a broad range of strategic cybersecurity initiatives related to securing the systems that operate the Nation's critical infrastructure, regardless of the cause.

Since 2004 the Department has conducted 148 assessments of electric sector facilities through the Office of Infrastructure Protection. These include cybersecurity assessments conducted by CSSP, which utilize several tools that we developed, such as the Control Systems Cyber Security Self Assessment Tool (CS2SAT) and the Cyber Security Vulnerability Analysis (CSVA). DHS and the other sector-specific agencies perform these vulnerability assessments as directed in HSPD 7, which states that in accordance with guidance provided by the Secretary of Homeland Security, sector-specific agencies shall:

> (a) collaborate with all relevant Federal Departments and Agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;
>
> (b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

In addition to performing vulnerability analyses and assessments, the CSSP also created a series of recommended practices and informational products to assist owner-operators in improving the security of their control systems. These information resources are publicly available online at http://www.us-cert.gov/control_systems/ and also are promoted through the monthly meetings held by the Cross-Sector Cyber Security Working Group, the Industrial Control Systems Joint Working Group's (ICSJWG) quarterly meetings, and other sector forums.

While products and tools allow asset owners and operators to understand the cyber risk to their control systems, it is essential that all stakeholders have knowledge of the fundamental principles of control systems security. To that end, we developed an advanced training center at the Idaho National Laboratory which includes functional models of critical infrastructure equipment. This center provides award-winning, hands-on training that ranges from introductory web-based courses to advanced, hands-on "Red Team/Blue Team" exercises and instructor-led classes. This effort has trained more than 14,000 professionals through both classroom and web-based instruction.

To further our mission and lead a cohesive effort between government and industry, the Program created two overarching initiatives: the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the ICSJWG.

The ICS-CERT, in coordination with the Department's United States Computer Emergency Readiness Team (US-CERT), responds to and analyzes control systems-related incidents, conducts analyses of vulnerabilities and malicious software (malware), and disseminates cybersecurity guidance to all sectors through informational products and alerts. The ICS-CERT provides a more efficient coordination of control system-related security incidents and information sharing with Federal, state, and local agencies and organizations, the Intelligence Community, and private sector constituents including vendors, owner-operators, and international and private sector computer emergency response teams (CERTs).

Recently, the ICS-CERT responded to an incident at a public water utility, conducting onsite analysis of an event and providing recommendations to increase the security posture of the facility. Additionally, we conducted detailed digital media analysis of the system hard drive in order to determine the root cause of the incident. I am available to provide details of the incident in a classified brief at a later date.

The CSSP and ICS-CERT regularly identify vulnerabilities and work with the vendors, owners, and operators of control systems to develop mitigation strategies tailored to their use and application in each of the critical sectors. We recognize there can be a gap between identification of a vulnerability and development of a vendor patch or full solution. To address this, the CSSP developed a Vulnerability Management Process operated by the ICS-CERT, in conjunction with trusted partners, to identify interim mitigation and consequence management approaches. We also engage with our Federal partners, such as the Departments of Defense and Energy as well as the Intelligence Community, to address equities and mitigate risks as we move from vulnerability identification, to risk assessment, to mitigation development and promulgation. These efforts help us evaluate new and emerging technologies such as Smart Grid, and the cyber risks that they introduce to control systems.

The ICSJWG follows a structured approach in accordance with the NIPP partnership framework and the Critical Infrastructure Partnership Advisory Council to continue the successful efforts of the Process Control System Forum to accelerate the design, development, and deployment of more secure industrial control systems. The ICSJWG is comprised of industry representatives from both private sector and government coordinating councils and provides a vehicle for communicating and partnering across all CIKR sectors among Federal, state, and local agencies, and private asset owner-operators of industrial control systems. The ICSJWG and ICS-CERT collaborate with one another to leverage partnerships for information sharing and awareness of current threats and vulnerabilities. CSSP is also collaborating with the DHS Science & Technology Directorate (S&T) to ensure that their planned research and development in this area is well-informed and complements CSSP's related work with industry and owners/operators.

Implementation of the Smart Grid will include the deployment of many new technologies, such as advanced sensors to improve situational awareness, advanced metering, automatic meter reading, and integration of distributed generation resources. These new technologies will require the addition of multiple communication mechanisms and infrastructures that must be coordinated with the developing technologies and existing systems. Smart Grid deployment is likely to increase the complexity of the existing power grid system. Increased complexity and expanded communication paths could lead to an increase in vulnerability to cyber attack unless there is a coordinated effort to enforce security standards for design, implementation, and operation. As the lead agency for cybersecurity and preparedness, DHS is evaluating the risks and developing guidance to increase the security of control systems with the implementation of new technologies.

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I have outlined the role the Department's Control Systems Security Program will play in addressing the risks that Smart Grid technologies will introduce to control systems. With your assistance, we will help the Department continue to protect America. Thank you again for this opportunity to testify. I will be happy to answer your questions.