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 Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Washington, DC

March 24, 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, including new and emerging technologies such as Smart Grid. A smart grid is an electric power supplier that applies technologies to deliver energy-efficient, reliable, and cost-saving electricity from suppliers to consumers.

A control system is a general term that encompasses several types of systems, including Supervisory Control and Data Acquisition, process control, and other automated systems that are most often found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes in industries such as electricity, oil and gas, water, and critical manufacturing. Control system security in our electric power grid is particularly important because of the significant interdependencies inherent with the use of energy in all other critical infrastructure sectors. And, of course, we rely on the electric grid for operations of Federal, State and local government. Therefore, assessing risk and effectively securing industrial control systems and their application to technologies such as Smart Grid is vital to maintaining our Nation's strategic interests, public safety, and economic prosperity.

In May 2004, DHS created the Control Systems Security Program to lead a cohesive effort focused on reducing the cyber risks to the control systems within critical infrastructure. In

2006, DHS issued the National Infrastructure Protection Plan (NIPP) that identified the CSSP as responsible for coordinating activities to reduce the likelihood of success and severity of impact of a cyber attack against CIKR through risk mitigation activities. DHS recognizes that control systems exist across sectors and must be secured from cyber attacks whose effects could result in significant consequences. To address this, the CSSP has built a culture of reliability, security, and resilience by partnering with government agencies, industry, and international entities to reduce the cyber risk to all 18 critical infrastructure/key resources (CIKR) sectors. The CSSP leverages the risk management framework and partnership model described in the NIPP, by providing a mechanism for coordination among CIKR stakeholders, government, and industry associations.

The CSSP provides leadership and subject matter experts through partnerships with key stakeholders. We develop guidance in the form of recommended practices, informational products, and assessment tools. We also deliver focused, award-winning training that ranges from introductory web-based courses to advanced, hands-on "Red Team/Blue Team" exercises and instructor-led classes. We are pleased with the positive impact that these efforts are making to assist both public and private sector partners in identifying and mitigating the risks to their control systems by implementing our mitigation strategies and adopting our recommended practices.

To help stakeholders identify vulnerabilities and develop strategies to improve their security posture, we developed the first widely available control system cybersecurity self-assessment tool. It employs a systematic and repeatable approach for owners and operators to assess the security of their industrial control systems network. It also offers recommendations based on industry standards that are customized to the operating characteristics of each control systems facility. This well-received tool is now being used in conjunction with the work of the Department's Protective Security Advisors, under the Office of Infrastructure Protection, to enhance the cybersecurity aspects of their site assistance visits. The CSSP also works closely with the Nation's most critical facilities to perform in-depth site assessments using this and other tools we have developed.

We have also created a series of recommended practices and informational products to assist owner-operators in improving the security of their control systems. These products cover a variety of security topics including defense-in-depth strategies, firewall implementation, patch management, and secure wireless configuration. Other products include the Cyber Security Procurement Language for Control Systems and Catalog of Control Systems Security Recommendations for Standards Developers. These products are publicly available online and are also promoted through the monthly Cross Sector Cyber Security Working Group meetings and other sector forums.

While valuable products and tools such as these allow asset owners to understand the cyber risk to their control systems, it is also imperative that all stakeholders have a full understanding of the underlying fundamentals of control systems security. Consequently, we developed an advanced training center at the Idaho National Laboratory that includes functional models of critical infrastructure equipment. This center provides hands-on training in a realistic, scenario-based environment. Since the Program's inception, we have trained more than 14,000 professionals through both classroom and web-based instruction.

To execute our mission and lead a cohesive effort between government and industry, the Program has created two overarching initiatives: the Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) and the Industrial Control Systems Joint Working Group (ICSJWG).

The ICS-CERT, in coordination with the United States Computer Emergency Readiness Team (US-CERT), responds to and analyzes control systems-related incidents, conducts analysis on vulnerabilities and malicious software, or malware, and disseminates cybersecurity guidance to all sectors through informational products and alerts. The ICS-CERT provides more efficient coordination of control system-related security incidents and information sharing with Federal, State, and local agencies and organizations, the Intelligence Community, private sector constituents including vendors, owner-operators, and international and private sector CERTS.

The ICSJWG follows a structured approach supported by the National Infrastructure Protection Plan 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. In fact, this group is holding its inaugural meeting tomorrow, March 25, and is comprised of industry representatives from both private sector and government coordinating councils. The ICSJWG will provide 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 Program partners with the Department of Energy to provide analysis capabilities of technologies affecting control systems. This relationship provides reciprocal coordination of effort as we evaluate emerging technologies and the cyber issues affecting critical infrastructure. Perhaps most importantly, our Advanced Vulnerability Discovery facility funded by DHS and housed at the Idaho National Laboratory as previously mentioned, offers a world-class test environment where our technical experts continuously evaluate nearly every major control system used in the critical infrastructure.

DHS identifies vulnerabilities and works 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 Program has 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 other Federal partners in this process—such as the Departments of Defense and Energy and the Intelligence Community—to address equities and mitigate risks as we move from vulnerability identification, to risk assessment, to mitigation development and promulgation of these mitigation efforts. These program efforts will help us evaluate new and emerging technologies such as Smart Grid, and the cyber risks that they introduce to control systems.

In Fiscal Year 2009 the overall control systems funding was increased to $18 million to expand the Department's efforts to in addressing control systems vulnerabilities. We were fortunate to receive an additional $4 million in funding, bringing us to a total of $22 million

that enabled us to recapitalize and expand the Advanced Vulnerability Discovery facility. This expansion has better positioned us to enhance our existing Smart Grid collaboration and support activities to the Department of Energy and industry stakeholders.

The 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 communication infrastructures that must be coordinated with new and legacy systems.

The 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, through the Control Systems Security Program, is evaluating the risks and developing guidance to increase the security of control systems affected by Smart Grid technologies and implementations.

DHS recommends that the inclusion of security measures, controls, and countermeasures addressing physical security, personnel security, as well as cybersecurity and the intersection of cyber and physical security both in Smart Grid technologies and project architectures, be a prerequisite for consideration for Recovery Act funding. We are prepared to provide technical assistance and subject matter expertise to support these efforts.

Chairwoman Clarke, Ranking Member Lungren, and distinguished Members, I have outlined the Department's efforts and capabilities, and the role that the 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 for again for this opportunity to testify. I will be happy to answer your questions.