STATEMENT OF CHARLES EDWARDS

DEPUTY INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

FACILITATING CYBER THREAT INFORMATION SHARING AND PARTNERING WITH THE PRIVATE SECTOR TO PROTECT CRITICAL INFRASTRUCTURE: AN ASSESSMENT OF DHS CAPABILITIES

MAY 16, 2013

Good Morning Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee:

Thank you for the opportunity to discuss DHS' efforts to secure the Nation's industrial control systems. The majority of information that I will provide today is contained in our February 2013 report, *DHS Can Make Improvements to Secure Industrial Control Systems (OIG-13-39).*

Industrial control systems (ICS) are systems that include supervisory control and data acquisition, process control, and distributed control that manage and monitor the Nation's critical infrastructure and key resources (CIKR).[1] ICS are an integral part of our Nation, and help facilitate operations in vital sectors. Beginning in 1990, companies began connecting their operational ICS with enterprise systems that are connected to the Internet. This allowed access to new and more efficient methods of communication, as well as more robust data, and gain quicker time to market and interoperability. However, security for ICS was inherently weak because it allowed remote control of processes and exposed ICS to cyber security risks that could be exploited over the Internet. As a result, ICS are increasingly under attack by a variety of malicious sources. These attacks range from hackers looking for attention and notoriety to sophisticated nation-states intent on damaging equipment and facilities, disgruntled employees, competitors, and even personnel who inadvertently bring malware into the workplace by inserting an infected flash drive into a computer. A recent survey revealed that a majority of the companies in the energy sector had experienced cyber attacks, and about 55 percent of these attacks targeted ICS. These attacks involved large-scale denial-of-service and network infiltrations. Successful attacks on ICS can give malicious users direct control of operational systems, creating the potential for large-scale power outages or man-made environmental disasters and cause physical damage, loss of life, and other cascading effects that could disrupt services.

Some recent cyber attacks have included the following:

- In February 2011, the media reported that hackers had stolen proprietary information worth millions of dollars from the networks of six energy companies in the United States and Europe.

- In December 2011, a sophisticated threat actor targeted the oil and natural gas subsector. Affected asset owners across the sector voluntarily worked with DHS during the investigation.

- Throughout 2011, there were reports of spear-phishing via email in the Energy sector; no negative impacts occurred to the companies' control processes and operations.

- In March 2012, an alert was issued regarding phone-based social engineering attempts at two or more power distribution companies. The callers attempted to direct the company

[1] There are 18 CIKR sectors: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Information Technology, National Monuments and Icons, Nuclear Reactors, Material and Waste, Postal and Shipping, Transportation Systems, and Water.

personnel to take action to correct a problem that would have allowed the attacker to gain access to their ICS.

- In April 2012, media reported that a Canadian ICS manufacturing company inadvertently planted a backdoor login account in its own operating systems, which contain switches and servers used in mission-critical communications networks that operate power grids and railway and traffic control systems. This account could have allowed attackers to access the devices via the Internet.

The Industrial Control Systems – Cyber Emergency Response Team's (ICS-CERT) operational capabilities focus on the private sector CIKR ICS and networks, which is essential to the Department's mission to protect the Nation's critical infrastructure, particularly against emerging cyber threats. Additionally, ICS-CERT uses the Request Tracker Ticketing System to capture analytical and status information regarding vulnerabilities and incidents. The ticketing system maintains the incident response team's remote technical assistance and onsite assessment status and reports. Tickets are color-coded based on age. The ticketing system notifies the assigned personnel when the status of a ticket is changed or further action is needed. Additionally, 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 of ICS.

ICS-CERT exchanges information with stakeholders via the Homeland Security Information Network (HSIN) – Critical Sector. The Office of the Chief Information Officer (OCIO) develops and maintains HSIN and serves as data governance steward for HSIN policy documents, including the HSIN Model Charter and HSIN Terms of Service. Although OCIO is the data steward, the office is not responsible for maintaining the content that users and communities of interest post to any element of HSIN.[2] Each community of interest sponsor is responsible for maintaining and sharing the content within the community of interest and through the community of interest shared space.[3] The administration and governance of the communities of interest, including creation of individual sites within the community, is at the discretion of their sponsors. OCIO works in cooperation with each community of interest to enforce the rules in the charter and terms of services. OCIO conducts regular reviews of communities of interest to validate and justify its purpose, objectives, and operational need. National Protection and Programs Directorate (NPPD) sponsors and manages the critical sector communities of interest.

DHS' Progress in Improving the Security of Industrial Control Systems

We reported that Department needed to improve the security of ICS and information sharing to enhance program effectiveness. DHS has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats,

[2] HSIN communities of interest are separate environments wherein users involved in the same subject matter area or industry may post and view potentially relevant news and information and use collaborative tools.

[3] The HSIN shared space allows authorized stakeholders and content contributors to publish finished products and relevant documents that (1) have appropriate markings providing sharing permissions at the document level, and (2) are targeted to an authorized audience based on their credentials and related community of interest and system wide rules for sharing.

and disseminate mitigation strategies. For example, DHS has taken the following actions to improve ICS security and foster better partnerships between the Federal and private sectors:

- Establishing ICS-CERT Incident Response Team, also known as the fly away teams, to support the public and private sectors through onsite and remote incident response services on a variety of cyber threats, ranging from general malicious code infections to advanced persistent threat intrusions. Additionally, in March 2012, NPPD released the Cyber Security Evaluation Tool Version 4.1. The updated tool assists users in identifying devices connected to their networks, as well as external connections, by creating a diagram of their systems.

- Operating a malware lab that provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. The team verifies vulnerabilities for researchers and vendors, performs impact analysis, and provides patch validation and testing prior to deployment to the asset-owner community.

- Improving the quality of its alerts and bulletins by including actionable information regarding vulnerabilities and recommended mitigations and best practices for securing ICS.

- Providing products to the ICS community on a daily, weekly, monthly, quarterly, and as-needed basis, through email, website, and portal postings. These products help ICS-CERT to improve the situational awareness of ICS and provide status updates of its working groups, articles of interest, and upcoming events and training.

- Implementing a virtual private network solution to allow NPPD program officials to access program applications and systems (e.g., the ICS-CERT ticketing system) located at the Idaho National Laboratory (INL).[4]

- Assisting in developing various roadmaps for the cross-sector, dams, nuclear, water, and transportation. The roadmaps provide vision and framework for mitigating cybersecurity risk to the wide variety of systems critical to each sector's operations.

Finally, the Department has strengthened its outreach efforts with the ICS community, including vendors, owners/operators, academia, and other Federal agencies. These efforts include participating in the periodic meetings with the Cross-Sector Cyber Security Working Group; Government Coordinating Council and Sector Coordinating Council; and various sector specific groups.

Major Challenges

Despite these actions, NPPD still faces challenges in reducing the cybersecurity risks for the Nation's ICS. Further, NPPD can improve its efforts to protect and secure control systems that are essential to the Nation's security and economy. Specifically, ICS-CERT needs to consolidate

[4] A virtual private network is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. Users can access resources on remote networks, such as files, printers, databases, or internal websites.

its information sharing and communication efforts with Sector Specific Agencies and the private sector to ensure that these stakeholders are provided with potential ICS threats and vulnerabilities to mitigate security threats timely. In addition, DHS needs to improve communications with Sector Specific Agencies and the private sector by providing advanced notification of ICS-CERT's remote technical and onsite incident assessments.

Consolidation of Multiple Information Sharing Communities of Interest

Many of the private sector partners we interviewed (e.g., owners/operators, regulators, and working groups) use the HSIN, ICS-CERT, and United States Computer Emergency Readiness Team (US-CERT) portals to retrieve advisories, vulnerability information, and best practices. There are 55 communities of interest on the HSIN-Critical Sectors intended to facilitate communication and collaboration among all CIKR sectors and the Federal Government. However, DHS does not have a consolidated summary overview page on HSIN-Critical Sectors that highlights new information and activities to ensure that ICS cybersecurity information is shared effectively. As a result, the content for each of the CIKR sectors and must be searched individually for pertinent and updated information. For example, the Dams, Emergency Management, and Electricity and Oil and Natural Gas subsector communities of interest, which are used by companies that belong to multiple sectors, have to be searched individually and may contain non-cybersecurity information, such as physical security, emergency response, and planning. These searches can be time-consuming for the stakeholders.

Additionally, each community of interest is arranged differently, making it more cumbersome for the users to retrieve useful information. For example, some HSIN users told us that the various communities of interest contain duplicate information. As a result, some Sector Specific Agencies want to build additional portals for their stakeholders to streamline the information DHS provides.

ICS-CERT officials acknowledged that existing communities of interest could confuse owners/operators. To eliminate duplicate information from the communities of interest, ICS-CERT created a subcommittee to address stakeholder concerns regarding the communities of interest. ICS-CERT officials said that ICS-CERT only contributed content to the communities of interest and does not have the responsibility for site set up. However, NPPD plans to hold discussions with OCIO to determine whether these communities of interest could be consolidated to better serve stakeholder needs.

We recommended that the Under Secretary, NPPD collaborate with OCIO to streamline the HSIN portal to ensure that ICS cyber information is shared effectively.

Advance Notification of Remote Technical and Onsite Assessments

All the Sector Specific Agencies senior officials that we interviewed expressed a need to be notified in advance when ICS-CERT is performing onsite or remote technical assistance assessments with private companies within their sectors. For example, these officials suggested that ICS-CERT publish a "heads-up" or "quick anonymous" informational alert regarding an ongoing investigative/pending event, sectors and devices affected, and whether a potential fix

exists. The Sector Specific Agency officials told us that such notifications would be helpful and would allow them to react more appropriately if other companies call them with questions. For example, according to Nuclear Sector Specific Agency officials, the Department's Domestic Nuclear Detection Office sends an email alert to state authorities and its offices regarding upcoming site visits.

DHS does not communicate timely the results of its remote technical and onsite assessments to the public. We interviewed officials from three Sector Specific Agencies, six government and private sector councils, and 23 private companies from the dams, energy, and nuclear sectors to evaluate whether ICS-CERT shared sufficient information and communicated effectively. Overall, these officials acknowledged that DHS had improved the quality of alerts and bulletins that addressed various cyber topics. However, they expressed concerns regarding the timeliness of ICS-CERT's information sharing and communications. As a result, the stakeholders are concerned that a great deal of time might elapse until stakeholders were made aware of the same or similar incident that could affect their systems.

Additionally, both Sector Specific Agencies and private sector officials said that an advance notification would be helpful to increase dialogue with ICS-CERT on an event or threat that has not been made public. The private sector officials suggested that advance notification can allow them to assist ICS-CERT in developing solutions and mitigating strategies as well as determining whether an incident is isolated or systemic.

ICS-CERT management acknowledged the Sector Specific Agencies', councils', and private sector's concerns regarding the sharing of active incidents and threats, such as identified cyber intrusions and spear-phishing emails. Additionally, ICS-CERT management told us that the private sector perceives that ICS-CERT has more useful information available than it is willing to share. However, ICS-CERT management said that proprietary information and ongoing law enforcement investigations limit the amount of information ICS-CERT can disseminate. For example, there were instances in which the Federal Bureau of Investigation was engaged in an ongoing investigation and had withheld sensitive law enforcement information. Additionally, the protected critical infrastructure information between DHS and the private sector owner prohibits ICS-CERT from sharing vulnerability and malware assessment information.

We recommended that the Under Secretary, NPPD promote collaboration with Sector Specific Agencies and private sector owners/operators by communicating preliminary technical and onsite assessment results to address and mitigate potential security threats on ICS.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the Subcommittee.