



### Why This Matters

Security for industrial controls systems (ICS) has been inherently weak because the systems were not designed to be accessible from external networks or the Internet. Beginning in 1990, companies began to connect their ICS with enterprise systems that are connected to the Internet. This transition allowed remote control of processes and exposed ICS to cyber security risks that could be exploited over the Internet.

### DHS Response

NPPD concurred with the two recommendations. NPPD will collaborate with the DHS Office of Chief Information Officer (OCIO) to ensure that ICS cyber information is shared effectively in the HSIN portal. Currently, the OCIO is planning to deploy the "HSIN Release 3 Shared Space", which will allow NPPD to share ICS and other information in one space on the portal.

Further, NPPD will continue its strong promotion of increased information sharing and collaboration with both Sector Specific Agencies and with the private sector. This collaboration includes increased awareness and use of the Protected Critical Infrastructure Information program.

#### For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

## DHS Can Make Improvements to Secure Industrial Control Systems

### What We Determined

National Protection and Programs Directorate (NPPD) has strengthened the security of industrial control systems by establishing the Industrial Control Systems Cyber Emergency Response Team to address the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. NPPD also facilitates cybersecurity information sharing between the public and private sectors through various working groups, issuing alerts and bulletins, and conducting cybersecurity training and conferences regarding industrial control systems.

While NPPD has made progress in securing control systems, further improvements can be made in information sharing. For example, NPPD needs to consolidate the multiple information sharing communities of interests used to disseminate control system cybersecurity efficiently and effectively. Additionally, NPPD should provide advance notification of technical and ongoing vulnerability and malware assessments to better coordinate response efforts with the public and private sectors to prevent, detect, and mitigate potential cyber threats.

### What We Recommend

We recommend that the Undersecretary, NPPD:

- 1) Collaborate with OCIO to streamline Homeland Security Information Network (HSIN) portal to ensure that ICS cyber information is shared effectively.
- 2) 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.