Department of
Homeland Security

# CSSP

## Control Systems Security Program

Our nation depends on the continuous and effective performance of a vast and interconnected critical infrastructure to sustain our modern way of life. This infrastructure, the majority of which is owned by the private sector, is comprised of critical infrastructures and key resources (CI/KR), as identified in the National Infrastructure Protection Plan (NIPP). These CI/KRs include: Energy, Chemical, Banking and Finance, Drinking Water and Water Treatment Systems, Dams, Postal and Shipping, Agriculture and Food, Defense Industrial Base, Public Heath and Healthcare, National Monuments and Icons, Transportation Systems, Commercial Facilities, and Commercial Nuclear Reactors, Materials and Waste.

Although each of these critical infrastructure industries is vastly different, they all have one thing in common. They are all dependent on control systems—computer based systems used within our nation's critical infrastructures—to monitor, control, and safeguard their vital processes.

Control systems, which may also be known as Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), are essential to industry and government alike because they support the operation of the nation's critical infrastructure.

### Protecting the Systems that Control Our Infrastructure

Control systems are transitioning from proprietary closed-systems to common and widely used technologies and are increasingly connected to open networks, such as corporate intranets and the Internet. This transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks.

A successful cyber attack on a control system could potentially result in physical damage, loss of service, loss of life, severe economic impact, and cascading effects that could disrupt other services. Therefore, the Department of Homeland Security (DHS) has been tasked under the Homeland Security Act of 2002 to coordinate the overall national effort to enhance the protection of our critical infrastructures.

### Control Systems Security Program

To reduce control system risks within and across all critical infrastructure sectors, the Department's National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP) to coordinate efforts among federal, state, local, and tribal governments, as well as control systems owners, operators and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

### CSSP Goal

The goal of the CSSP is to guide a cohesive effort between government and industry to reduce the risk to critical infrastructure control systems. To lead this effort, the CSSP executes a strategy composed of two interrelated objectives, on both national and international fronts, and works with other government entities and the control systems community to improve the security posture of our nation's control systems.

Department of Homeland Security

# CSSP
## Control Systems Security Program

### Objective 1: Provide Guidance

The CSSP provides guidance to the control systems community through a variety of mechanisms and activities.

- Enhancing the United States Computer Emergency Readiness Team (US-CERT) capability to coordinate control system incident management and provide timely situational awareness information for control systems.
- Maintaining a technical support center to conduct assessments of commercially available control systems and components.
- Enhancing industry practices for securing control systems against cyber attacks by providing assessment tools, implementation guidelines, and recommended practices.
- Performing outreach activities and improving awareness in the control system community through training and education.
- Providing informational products to assist vendors and owners/operators in designing, procuring, installing, and operating controls systems to mitigate risks.
- Providing strategic recommendations to the research and development community for development and testing of next-generation secure control systems.
- Assisting national and international standards organizations in developing control systems cyber security standards.

### Objective 2: Develop Partnerships

The CSSP works closely with public and private entities to establish effective partnerships with national laboratories, government entities and industry, as well as technical professionals across the control systems community to improve the security posture of our nation's control systems.

- Working with Government stakeholders through the Federal Control Systems Security Working Group to coordinate the Government effort.
- Facilitating monthly vendor's conference calls to address cyber security issues common to the control systems vendor community.
- Managing the Process Control Systems Forum (PCSF) to facilitate the collaboration of stakeholders to accelerate the design, development, and deployment of more secure control systems. Participants include national and international stakeholders from government, academia, owner/operators, systems integrators, and vendors.
- Working in partnership with the Institute for Information Infrastructure Protection (I3P) to identify high-value applied research to enhance control systems security. I3P is a consortium that includes academic institutions, federally-funded labs and non-profit organizations.
- Working with international partners to facilitate information sharing and rapid adoption of international recommended practices.

### Reporting Control Systems Cyber Incidents and Vulnerabilities

Threats to control systems can come from numerous sources, including disgruntled employees and malicious intruders. Reporting control systems incidents and vulnerabilities greatly assists the DHS in maintaining situational awareness and managing cyber events affecting the nation's critical control systems.

Control systems incidents and vulnerabilities should be reported via the US-CERT:

Web: http://www.US-CERT.gov/control_systems
Phone: (703) 235-5110 or (888) 282-0870

### Obtaining Additional Information

To learn more about the CSSP, visit:
http://www.US-CERT.gov/control_systems

To obtain additional information or request involvement or assistance, contact:
cssp@dhs.gov