CSSP Year in Review

Control Systems Security Program and
Industrial Control Systems Cyber Emergency Response Team

FY 2011

Homeland Security

What's Inside

Welcome	1
Introduction	2
Accomplishments	3
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	4
National Cybersecurity and Communications Integration Center (NCCIC)	5
Industrial Control Systems Consequence Effects and Analysis (ICS-CEA)	5
ICS-CERT key accomplishments for include:	6
Cybersecurity Assessments	7
Cybersecurity Training and Vendor Assessments	8
Roadmaps and Standards Development	9
Industrial Control Systems Joint Working Group	10
Path Forward	11
Assistance from CSSP	12

Homeland Security

Welcome

At no point in the history of our modern industrial world has cybersecurity been more important. In the seven years since the Department of Homeland Security's Control Systems Security Program (CSSP) was created, the risk and impact of cyber vulnerabilities affecting the nation's critical infrastructures and key resources (CIKR) has steadily increased.

Today, events ranging from subtle disruptions to more serious consequences have become a persistent and daily occurrence. Yet, even in the midst of this constant risk, control systems owners, operators, and manufacturers are working diligently to apply anti-malware, intrusion detection, and user authentication measures to their systems based in part on the research validated and shared through the CSSP.

In this Year in Review, you will read about our successes in the control systems community. Over the last year, we have seen a lot of positive things happening. The program continues to grow the Industrial Control Systems Joint Working Group (ICSJWG), and as a result, the volume and quality of research being created by the independent control systems security community is increasing. In turn, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is working diligently to keep the information flowing to the asset owners, vendors, and operators of CIKR.

Also, as awareness of cyber vulnerabilities in the CIKR community grows, the ICS-CERT has been deploying more on-site incident fly-away teams to help critical infrastructure organizations deal with analysis and recovery efforts from cyber incidents.

We still face challenges though. CSSP continues to fine tune the process to share actionable and timely information with those owners, operators, and vendors who have a "need to know" and be alerted to the threats facing the community.

We value the partnerships we have formed with you, and look forward to another year working to protect the vast and interconnected infrastructures that keep our country, and, indeed, the world running safely and securely.

Regards,

Marty Edwards
Director
Control Systems Security Program
Industrial Control Systems Cyber Emergency Response Team
Department of Homeland Security
ICSJWG GCC Chair

Introduction

Our nation depends on the continuous and effective performance of a vast, interconnected critical infrastructure. The majority of this infrastructure is owned by the private sector and is composed of the 18 CIKR sectors identified in the National Infrastructure Protection Plan (NIPP).

Although each CIKR sector is unique, they all depend on control systems that monitor, control, and safeguard vital processes. DHS recognizes that the protection and security of control systems is essential to the nation's security and economy. Many of the industrial control systems (ICS) used today were designed for operability and reliability and were not intended to be connected to external networks or business systems.

In today's open communications environment, ICS are highly network-based and use common standards for communication protocols. CIKR asset owners and operators have gained immediate benefits by increasing the connectivity of their ICS, particularly when collecting information for business and economic operations. However, this connectivity exposes network assets to cyber infiltration and subsequent manipulation of sensitive operations.

Therefore, the CSSP strives to strengthen the nation's control system security posture by coordinating across government, private sector, and international organizations in reducing the risk to CIKR.

This Year in Review will highlight the many accomplishments of both the CSSP and its operational component, the ICS-CERT.

Accomplishments

In FY 2011, CSSP continued to move forward and grow as a program. By providing increased support to the vendors, owners, and operators of critical infrastructure, the program continued to work toward a safer and more secure tomorrow by accomplishing several key tasks:

- ICS-CERT fly-away teams were deployed to seven organizations over the fiscal year (FY).
- Approximately 600 participants attended the Fall 2010 and Spring 2011 ICSJWG Conferences with over 200 scheduled to attend the Fall 2011 ICSJWG.
- The ICSJWG Cross-Sector Roadmap Document was finalized.
- Cyber Security Evaluation Tool (CSET) Version 4.0 was released in August 2011 with over 1,150 CSETs being distributed in FY 2011.
- The CSET tool is now downloadable from the CSSP website.
- In FY 2011, over 75 CSET onsite assessments were completed.
- Over 40 training courses have been conducted domestically and internationally for public and private partners with over 1,300 attendees.
- CSSP provided more than a 100 situational awareness briefings and presentations at stakeholder meetings and conferences.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

The ICS-CERT provides cyber incident response, analysis, and information sharing to address the cybersecurity threats and vulnerabilities unique to industrial control systems (ICS). For example, this capability provides onsite and remote incident response services for a variety of cyber threats ranging from general malicious code infections to advanced persistent threat (APT) intrusions.

The response team also produces alerts and advisories to warn of vulnerabilities and to recommend mitigations and best practices for securing ICS and the workplace. ICS-CERT does this in partnership with private sector organizations and Information Sharing and Analysis Centers in order to coordinate and leverage cybersecurity efforts across all 18 critical infrastructure sectors.

A technical analysis and malware lab enables the ICS-CERT to provide analysis of vulnerabilities and malware threats to control system environments. The team is able to verify vulnerabilities for researchers and vendors, perform impact analysis, and provide patch validation and testing prior to deployment to the asset-owner community.

Another service the program offers asset owners is no-cost onsite assistance and offsite analysis to support discovery, forensics analysis, and recovery efforts associated with a cybersecurity event (incident) focused on control environments within critical infrastructure. Onsite assistance consists of a fly-away team being made available to deploy onsite to review affected entities' network architectures, collect applicable forensic data, assist with immediate mitigation efforts when appropriate, and work with the stakeholder to identify future defense strategies. Offsite services include providing analytical findings, including determination of origin and breadth and depth of compromise from data captured during the onsite deployment to the customer.

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 center responsible for the production of a common operating picture for cybersecurity and communications across federal, state, and local governments, intelligence and law enforcement communities, and the private sector. Other key organizations include the United States Computer Emergency Readiness Team (US-CERT), National Coordinating Communications for Telecommunications, and the DHS Office of Intelligence and Analysis.

The ICS-CERT is a component of the National Cybersecurity and Communications Integration Center (NCCIC). As a component of the NCCIC, ICS-CERT enhances DHS cyber incident response and vulnerability disclosure coordination efforts to ensure that control systems security issues are addressed by monitoring, evaluating and responding to issues affecting critical infrastructure and key resources.

Industrial Control Systems Consequence Effects and Analysis (ICS-CEA)

The ICS-CEA framework is a critical infrastructure modeling and simulation capability that provides a means for users to model, analyze and share information related to potential consequences of naturally occurring or man-made threats upon our nation's critical infrastructure. The ICS-CEA system provides the NCCIC a capability for daily use of modeling, simulation, analysis, and information sharing related to potential cross-sector "consequence" effects to industrial control systems and their related CIKR sectors.

In FY 2011, ICS-CEA has been utilized for responding to multiple requests by the NCCIC regarding the identification of potentially affected CIKR because of natural disasters and potential man-made threats. These events have included support for analysis of potential impacts because of spring flooding in the midwest, multiple tropical storms, and hurricanes including Hurricane Irene, summer wildfires throughout the US, large scale power outages in the southwest, and the Virginia earthquake near the Capitol region.

ICS-CERT key accomplishments for FY 2011 include:

ICS-CERT deployed onsite incident response fly-away teams to seven critical infrastructure organizations to assist with analysis and recovery efforts of a cyber incident.

As part of the information sharing mission, ICS-CERT published over 100 security alerts and advisories to the ICS community warning of various threats and vulnerabilities impacting control systems.

Vulnerability analysis and coordination rose a staggering 600% in FY 2011, with researchers utilizing ICS-CERT as a conduit to vendors in the ICS space.

Reported cyber incidents were also up over 200% from FY 2010 with more asset owners and operators contacting ICS-CERT for support during a cyber event.

Cybersecurity Assessments

CSSP offers the CSET, a DHS product that assists organizations in protecting their key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks against recognized industry and government standards, guidelines, and practices. It includes both high-level and detailed questions related to all industrial control and IT systems, regardless of sector. CSET generates both interactive (on-screen) and printed reports that provide a summary of security level gaps or areas that do not meet the recommendations of the selected standards. These reports can be used to help an organization plan and prioritize mitigation strategies. Organizations who wish to conduct a self assessment can download CSET from the CSSP website. Over 1,150 copies of the tool were distributed in FY 2011.

In addition to the CSET, CSSP also offers onsite training and guidance to asset owners in using CSET during onsite assessments. These assessments are conducted at no cost to the asset owners. This "over-the-shoulder" training and guidance is provided to assist asset owners in using the tool to better understand their control systems cybersecurity posture.

In FY 2011, CSSP conducted over 75 assessments across the sectors. For information on the CSET or to download the tool, visit the website at:

http://www.us-cert.gov/control_systems/satool.html

Cybersecurity Training

CSSP offers several training programs including Introductory, Intermediate, and Advanced Control Systems Security classes. These classes are offered at no cost to ICS professionals and managers across all sectors of CIKR. In FY 2011, over 40 training sessions were provided consisting of over 20 Introductory, 8 Intermediate, and 10 Advanced ICS classes.

In April of 2011, CSSP released a new Management Level Training Course that provides managers with a high-level overview of control systems security.

Vendor Assessments

The Vendor Assessments effort focuses on vulnerabilities in specific vendor equipment/software where CSSP analyzes the potential impacts of emerging exploits in various ICS environments. CSSP completed assessments of several systems in FY 2011 and provided findings and recommendations to system vendors for consideration and action. The ICS-CERT leveraged these discoveries to issue alerts and guiding principles to the ICS stakeholder community to identify, mitigate, and reduce the security risks.

Roadmaps and Standards Development

The Control Systems Security Program established the Roadmap to Secure ICS Working Group, which in FY 2011 finalized the Cross-Sector ICS Cybersecurity Roadmap. This Roadmap addresses a broad range of cybersecurity strategies applicable to those industrial sectors that may not have had the opportunity to complete their own assessments. The program also supports development and implementation of an ICS roadmap within the Chemical Sector and has assisted the Energy Sector in updating their 2006 ICS Cybersecurity Roadmap to include validation of near-term goals and objectives.

CSSP is supporting roadmap development efforts in the Dams, Nuclear, Water, and Transportation sectors through various private and public partnerships.

The program continues to demonstrate leadership by helping standards organizations develop new cybersecurity standards and advance existing efforts. The program also serves as a key member of the following:

- Smart Grid Interoperability Panel (SGIP) supporting National Institute of Standards and Technology (NIST) in the development of smart grid interoperability standards.
- SGIP Cybersecurity Working Group in the development of a framework of cybersecurity guidelines and standards for smart grid interoperability.
- ISA-99.
- APTA Cyber Security Recommended Practices.

Industrial Control Systems Joint Working Group

Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," directed DHS to produce and execute a comprehensive, integrated national plan for CIKR protection. In response, the DHS National Cyber Security Division (NCSD), CSSP developed the Strategy for Securing Control Systems.

This strategy led to the creation of the Industrial Control Systems Joint Working Group (ICSJWG), which is designed to help support, guide, and coordinate the efforts of public, private, and international entities to reduce cybersecurity risks to control systems while managing risk in critical infrastructure. In an effort to bring these entities together, ICSJWG hosts two conferences every year.

The ICSJWG 2010 Fall Conference was held in October in Seattle, Washington, where Stuxnet presentations and related threat and vulnerability discussions encompassed most of the conference sessions.

The CSSP hosted the Spring ICSJWG Conference in Dallas, Texas, in May 2011. Over 250 participants networked with others in the industry and learned about the latest control systems security issues being addressed by both private sector and government.

Throughout the year, the ICSJWG subgroups continue to meet and address the cybersecurity challenges associated with ICS. The ICSJWG accomplished several key items this year, which include:

- The ICS Roadmap Development subgroup finalized a common cross-sector ICS roadmap.
- The GCC/SCC council created a Standards & Metrics subgroup to actualize standards within the control systems space and measure performance with outcome or process based metrics.

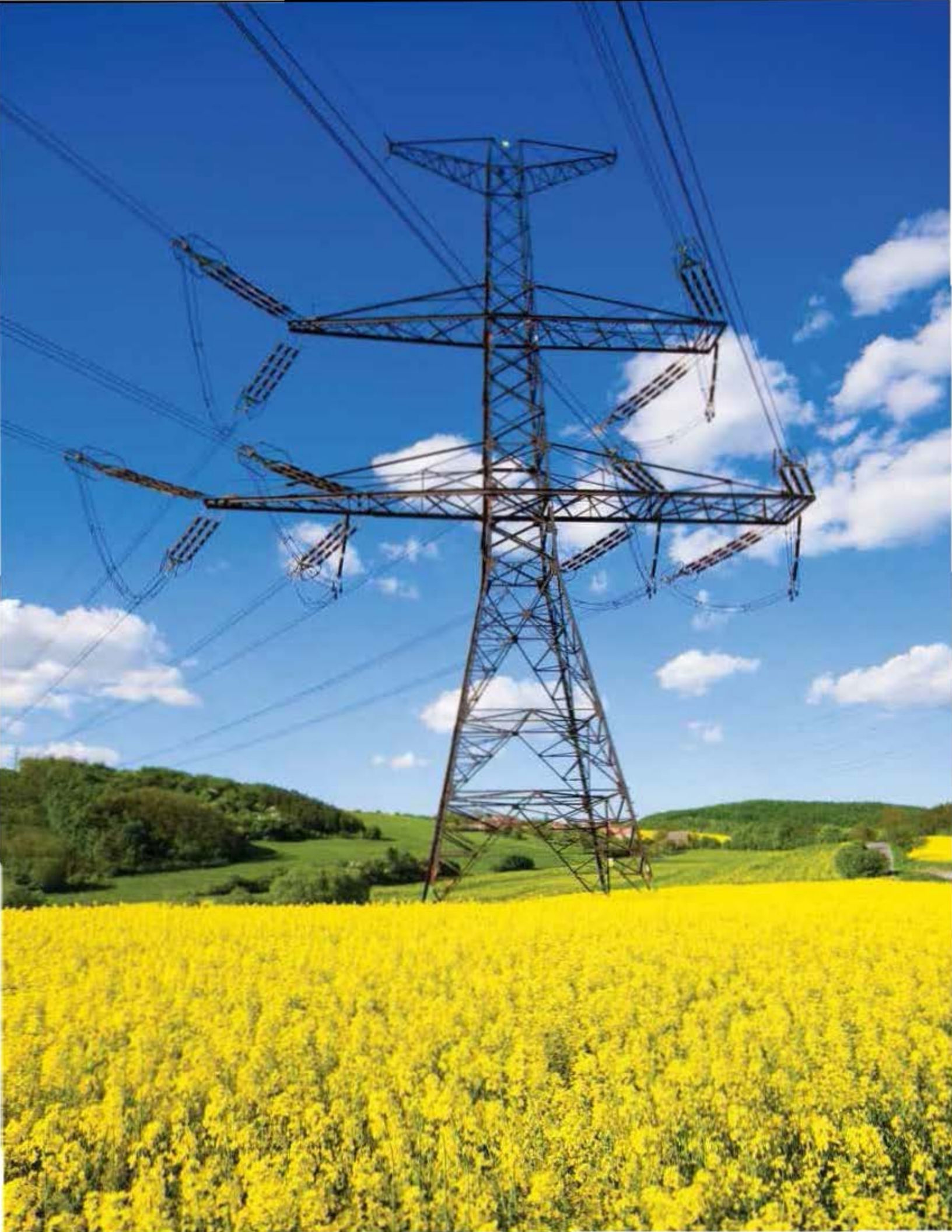
Path Forward

The evolution of industrial control systems, as well as threats to those systems, requires CSSP and ICS-CERT to continue evolving to meet the needs of owners, vendors, and operators. It is our goal to assist in providing the stakeholder community with the tools and services required to securely operate those systems that the nation's critical infrastructures rely apon daily.

Goals in the upcoming year include strengthening the incident response capability and providing continued onsite incident response teams to assist CIKR owners and operators with investigation and remediation of damages following a cyber incident on industrial control systems. Supporting this, improvements will also be made to malware analysis capabilities.

In addition to providing onsite assessments, CSSP will continue to focus on support for standards development organizations and release upgrades to the CSET tool. This tool is for use across the control systems community, including public and private sector partners, to increase situational awareness for cybersecurity status and improve the health of CIKR stakeholders' control systems.

CSSP plans to revise the Strategy to Secure Control Systems. The program will promote and maintain the CSSP website as a central repository for control systems cybersecurity information, vulnerability reporting, and cross-sector information sharing for public and private sector partners. CSSP also will continue industrial systems security support to the NCCIC and is dedicated to maintaining our position as a world class leader in control systems security.



Assistance from CSSP is only a phone call away

The CSSP and the ICS-CERT encourage you to report suspicious cyber activity and vulnerabilities affecting critical infrastructure control systems.

To report control systems cyber incidents and vulnerabilities contact the ICS-CERT:

ics-cert@dhs.gov
877-776-7585

www.us-cert.gov/control_systems/ics-cert

For more information on the Control Systems Secuirty Program visit:

http://www.us-cert.gov/control_systems/

Homeland Security

10-50925