Homeland Security

ICS-CERT MONITOR

Contents

National Cybersecurity and Communications Integration Center

ICS-CERT

This is a publication of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT is a component of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT coordinates control systems-related security incidents and information sharing with federal agencies; state, local, tribal, and territorial governments; and control systems owners, operators, and vendors to reduce the risk of cyber attack against the Nation's critical infrastructure.

This issue and past issues of the ICS-CERT Monitor can be found at the following URL: https://ics-cert.us-cert.gov/monitors

Contact Information

For questions related to this report or to contact ICS-CERT:

NCCIC/ICS-CERT Operations Center
Toll Free: 1-877-776-7585
International: 1-208-526-0900
Email: ics-cert@hq.dhs.gov
Web site: http://ics-cert.us-cert.gov

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

GovDelivery

ICS-CERT launched a new digital subscription system with GovDelivery to help you stay informed. By signing up for GovDelivery, you can receive new ICS-CERT product release notices directly to your inbox. Learn more, and sign up for GovDelivery at the following URL: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

Downloading PGP/GPG Keys

https://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT_PGP_Pub_Key.asc

ICS-CERT Services

ICS-CERT Vulnerability Coordination

In this issue of the Monitor, we highlight ICS-CERT Vulnerability Coordination

The primary objective of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Vulnerability Coordination Team's work is the timely mitigation of vulnerabilities to reduce the likelihood of a successful cyber attack against the Nation's critical infrastructure (CI). In this effort, the Vulnerability Coordination team engages with Federal, state, local, and tribal governments and with industrial control systems (ICS) owners, operators, and vendors in the private sector. Vulnerability coordination requires technical expertise and close trusted partnerships with each of these key stakeholders in the ICS community.

ICS-CERT's vulnerability handling process involves five basic steps: 1) Detection and Collection; 2) Analysis; 3) Mitigation Coordination; 4) Application of Mitigation; and 5) Disclosure.

In the detection and collection step, the vulnerability team collects vulnerability reports through vulnerability analysis and monitoring of public sources or they receive vulnerability information directly from researchers. Upon learning of a vulnerability, the team eliminates duplicates and false alarms and catalogs each vulnerability.

Vulnerability Coordination Process:

1. Detection and Collection
2. Analysis
3. Mitigation Coordination
4. Application of Mitigation
5. Disclosure

In the analysis step, the team works with vendor analysts to examine the vulnerability and identify all its potential threats.

In the mitigation coordination step, the team works with the vendor for mitigation and patch issuance. The vulnerability team allows sufficient time for the vendor to effectively resolve and perform patch regression testing against any given vulnerability.

In the application of mitigation step the team coordinates with vendors to allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to ICS-CERT's public disclosure of the vulnerability.

In the disclosure step, after coordinating with vendors and gathering technical and threat information, the team publishes an alert or advisory to notify end users about the vulnerabilities. ICS-CERT strives to disclose accurate, neutral, objective information. ICS-CERT references other available information on vulnerabilities and corrects misinformation when necessary.

For more information, please go to the following URLs: https://ics-cert.us-cert.gov/ and https://ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy.

Situational Awareness

Cybersecurity Crawl, Walk, Run

In every profession, there is a progression of skill levels. Let's call them "crawl," "walk," and "run." It should be the goal of every professional to reach the run level within their selected field. In this respect, the world of cybersecurity is no different. An example of the run skill level in the world of cybersecurity is the ability to conduct a penetration test, or "pen" test, on your own network. A pen test is an attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.

You are at the walk level if you are using a security information and event management (SIEM) system. A SIEM system collects logs and other security-related documents and forwards them to a centralized management console. The evaluation of these records allows the administrator to identify anomalous events and take corrective action.

You are in the crawl stage of cybersecurity if you have implemented the basic elements of security: you have separated and hardened your networks; you have patched and updated all of your systems; you have implemented a change management system; you have implemented a demilitarized zone (DMZ) that filters both incoming and outgoing traffic; and you have disabled all unused ports.

There is one more stage that one might best describe as lying on your back with your feet in the air, looking at your toes, and wondering, "What are those things for?" If you are not sure you fit into this category, here are some questions to ask. Have I ever clicked on a link in an unsolicited email? Have I ever used a free USB drive from a business convention? Do I have any passwords written down? If you answered yes to any of these questions, please keep reading.

Information technology (IT) and operational technology (OT) platforms are only as secure as the users who operate them. The technical aspects described above can only aid in securing your networks. The true first-line defense in cybersecurity is proper training. Proper training and constant awareness can help to keep users from becoming victims of social engineering schemes. The fact that government agencies and security companies have developed multiple detailed programs focused exclusively on spear-phishing attacks is proof that, regardless of the magnitude of the technical security solutions an organization employs, the actions of even just one unaware user can be potentially disruptive.

ICS-CERT would like to introduce you to the enterprise solution that will solve all your cybersecurity problems; however, such a solution does not exist. The best we can do is encourage you to develop a strong training plan and encourage all your users to stay vigilant. If you don't delete the unsolicited emails, or take the t-shirt instead of the USB drive at the next convention, or memorize your password, then be prepared to exercise your recovery plan.

ICS-CERT News

DHS Moving US-CERT Portal to HSIN, Rebranding as NCCIC Portal

The U.S. Department of Homeland Security (DHS) is currently in the process of consolidating all secure portal capabilities into the Homeland Security Information Network (HSIN). This move will migrate all US-CERT Portal (NC4 Mission Center) content to HSIN (including the ICS-CERT compartment). In addition to this move, DHS will rebrand the US-CERT Portal as the National Cybersecurity and Communications Integration Center (NCCIC) Portal to reflect the fact that the portal is a resource for all NCCIC organizations and stakeholders.

This migration will provide significant functionality, features, and enhanced security, and it will enable greater customization and configuration for the communities (formerly compartments). HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information with streamlined collaboration and real-time communications throughout all homeland security mission areas. For more information on the HSIN Program, please visit the HSIN page on the DHS web site.

ICSJWG Fall 2016 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) hosted its 2016 Fall Meeting in Fort Lauderdale, Florida, from September 13-15, at the Embassy Suites Fort Lauderdale 17th Street hotel. This meeting brought together over 280 stakeholders from the ICS community, with over half of the group attending for the first time.

Keynote Speakers included:

- Billy Rios, Founder of WhiteScope
- Joel Langill, ICS Cybersecurity Subject Matter Expert at AECOM Management Services Group
- John Felker, Director, NCCIC, DHS
- Marty Edwards, Director, ICS-CERT, DHS

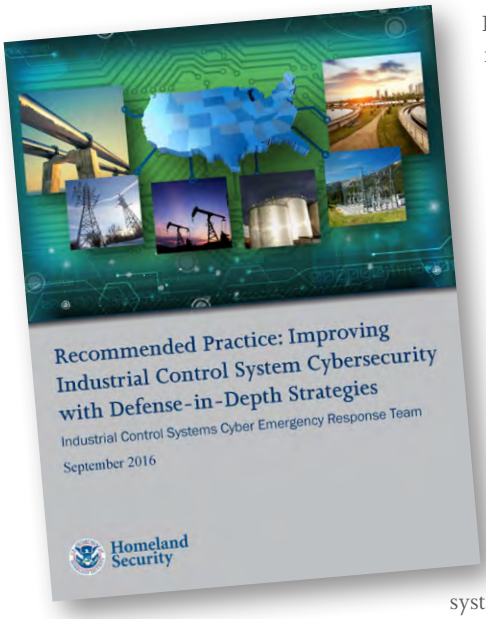
Meeting Highlights:

- Hands-On Technical Workshop and Training focused on Network Monitoring of ICS and Google Hacking/Shodan
- "Ask Me Anything" session with Marty Edwards
- Plenary panel sessions focused on Vulnerability Coordination and Research
- Back by Popular Demand: "Viewing Your Network through the Eyes of an Attacker."

ICS-CERT Hosts Regional Training in Lisbon, Portugal

The ICS-CERT Training team hosted a four-day ICS cybersecurity training session in Lisbon, Portugal the week of September 12th. The DHS Office of Cybersecurity and Communications' Office of International Affairs arranged the session in cooperation with the US Embassy in Portugal and with sponsorship from the US European Command. This was the first European session conducted for the 101/201/202 series of courses. There were over 80 attendees, representing 23 countries, who participated in technical discussions on the cyber protection of industrial control systems.

ICS-CERT Releases Defense-in-Depth and Annual Vulnerability Coordination Reports

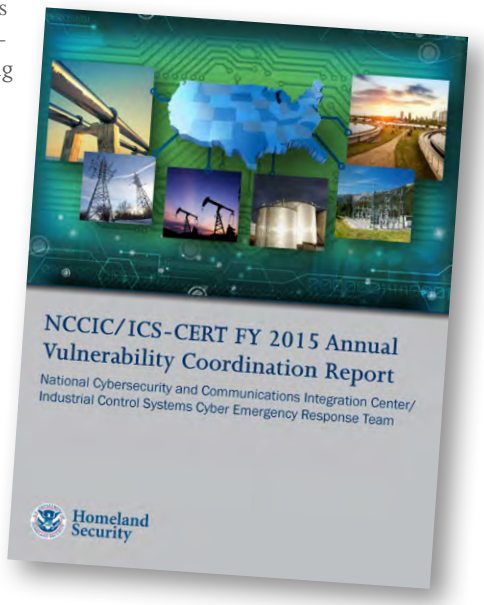


In September, ICS-CERT released a new version of two reports: "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" and "NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report." The new version of the Defense-in-Depth document modernizes and improves the flagship document issued in 2009, reflecting the evolution of control systems management, security practices, and change management within the ICS community, as well as addressing emerging threats to critical infrastructure. It is a living document that provides an aggregated compendium of the current state of ICS security practices.

This document provides guidance for developing mitigation strategies for specific cyber threats and direction on how to create a Defense-in-Depth security program for control systems. Defense-in-Depth is a holistic approach that uses specific countermeasures, implemented in layers, to create an aggregated, risk-based security posture and helps to defend against cybersecurity threats and vulnerabilities. Defense-in-Depth provides a flexible and useable framework for improving cybersecurity protection when applied to control systems. You can find the newly updated Defense-in-Depth report at the following URL: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

The intent and scope of the ICS-CERT Annual Vulnerability Report is to provide a summary of the DHS's NCCIC/ICS-CERT vulnerability coordination efforts performed in FY 2015.

This report provides trend analysis for all vulnerabilities reported to ICS-CERT in FY 2015. Most notably, researchers found that 52 percent came from improper input validation and permissions, privileges, and access controls. While this high percentage may indicate a pressing cybersecurity gap, it is also possible that it merely reflects the type of vulnerabilities targeted by researchers reporting to ICS-CERT. The majority of reported vulnerabilities for FY 2015 came from the Energy, Critical Manufacturing, and Water and Wastewater Sectors.



You can find the Annual Vulnerability Coordination report at the following URL: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf.

What is a CSET Assessment?

ICS-CERT developed the Cyber Security Evaluation Tool (CSET®) to guide users through a step-by-step process to assess their control systems and information technology network security practices against recognized industry standards. The CSET output is a prioritized list of recommendations for improving the cybersecurity posture of an organization's enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices.

Each recommendation links to a set of actions that enhance cybersecurity controls. ICS-CERT designed CSET for easy installation and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), the Transportation Security Administration (TSA), the U.S. Department of Defense (DoD), and others. When the tool user selects one or more of these standards, CSET opens up a set of questions for the asset owner to answer. The tool then compares the answers to these questions against a selected security assurance level and generates an individualized report that shows areas for potential cybersecurity improvement. CSET provides an excellent means to perform a self-assessment of the security posture of your control system environment by doing the following:

- Contributing to your organization's risk management and decision-making process,
- Raising awareness and facilitating discussion on cybersecurity within your organization,
- Highlighting vulnerabilities in your organization's systems and providing recommendations on ways to address the vulnerability,
- Identifying areas of strength and best practices being followed by your organization,
- Providing a method to systematically compare and monitor improvement in your cyber systems, and
- Providing a common industry-wide tool for assessing cyber systems.

For more information, see ICS-CERT's Assessment FAQs and the CSET fact sheet.

What is the PCII Program?

The Protected Critical Infrastructure Information (PCII) Program, part of DHS's National Protection and Programs Directorate (NPPD), is an information-protection program to enhance information sharing between the private sector and the government. This program protects qualifying information voluntarily submitted to the government and validated as PCII from public disclosure under the Freedom of Information Act (FOIA) and similar state and local disclosure laws and from use in civil litigation. DHS and other federal, state, and local analysts use PCII in pursuit of a more secure homeland, focusing primarily on:

- Analyzing and securing critical infrastructure and protected systems,
- Identifying vulnerabilities and developing risk assessments, and
- Enhancing recovery preparedness measures.

PCII can be shared directly through the PCII Program or through DHS field representatives and other federal agencies designated to receive PCII by the PCII Program Manager.

For more information, see the PCII web page and the PCII FAQs.

ICS-CERT Assessment Activity for September/October 2016

ICS-CERT conducts onsite cybersecurity assessments of industrial control systems (ICSs) to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In September/October 2016, ICS-CERT conducted 10 onsite assessments across 2 sectors (Table 1). Of these 10 assessments, 3 were Cyber Security Evaluation Tool (CSET®) assessments, 4 were Design Architecture Review (DAR) assessments, and 3 were Network Architecture Verification and Validation (NAVV) assessments (Table 2). For detailed information on ICS-CERT's CSET, DAR, and NAVV assessments, go to https://ics-cert.us-cert.gov/assessments.

Table 1: Assessments by sector, September/October 2016.

Assessments by Sector	September 2016	October 2016	September/ October Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	1		1
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	6	3	9
Monthly Totals	7	3	10 Total Assessments

Table 2. Assessments by type, September/October 2016.

Assessments by Type	September 2016	October 2016	September/ October Totals
CSET	2	1	3
DAR	3	1	4
NAVV	2	1	3
Monthly Totals	7	3	10 Total Assessments

Recent Product Releases

Alerts

ICS-ALERT-16-286-01 Sierra Wireless Mitigations Against Mirai Malware, October 12, 2016

ICS-ALERT-16-263-01 BINOM3 Electric Power Quality Meter Vulnerabilities, September 19, 2016

ICS-ALERT-16-256-01 FENIKS PRO Elnet Energy Meter Vulnerabilities, September 12, 2016

ICS-ALERT-16-256-02 Schneider Electric ION Power Meter CSRF Vulnerability, September 12, 2016

Advisories

View Advisories Feed

ICSA-16-301-01 Honeywell Experion PKS Improper Input Validation Vulnerability, October 27, 2016

ICSA-16-299-01 Siemens SICAM RTU Devices Denial-of-Service Vulnerability, October 25, 2016

ICSA-16-294-01 Moxa EDR-810 Industrial Secure Router Privilege Escalation Vulnerability, October 20, 2016

ICSA-16-292-01 Schneider Electric PowerLogic PM8ECC Hard-coded Password Vulnerability, October 18, 2016

ICSA-16-287-01 OSIsoft PI Web API 2015 R2 Service Account Permissions Vulnerability, October 13, 2016

ICSA-16-287-02 Siemens Automation License Manager Vulnerabilities, October 13, 2016

ICSA-16-287-03 Siemens SIMATIC STEP 7 (TIA Portal) Information Disclosure Vulnerabilities, October 13, 2016

ICSA-16-287-04 Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities, October 13, 2016

ICSA-16-287-05 Moxa ioLogik E1200 Series Vulnerabilities, October 13, 2016

ICSA-16-287-06 Fatek Automation Designer Memory Corruption Vulnerabilities, October 13, 2016

ICSA-16-287-07 Kabona AB WDC Vulnerabilities, October 13, 2016

ICSA-16-252-01 GE Bently Nevada 3500/22M Improper Authorization Vulnerability, October 6, 2016

ICSMA-16-279-01 Animas OneTouch Ping Insulin Pump Vulnerabilities, October 5, 2016

Follow ICS-CERT on Twitter: @icscert

ICSA-16-278-01 INDAS Web SCADA Path Traversal Vulnerability, October 4, 2016

ICSA-16-278-02 Beckhoff Embedded PC Images and TwinCAT Components Vulnerabilities, October 4, 2016

ICSA-16-273-01 American Auto-Matrix Front-End Solutions Vulnerabilities, September 29, 2016

ICSA-16-271-01 Siemens SCALANCE M-800/S615 Web Vulnerability, September 27, 2016

ICSA-16-264-01 Moxa Active OPC Server Unquoted Service Path Escalation Vulnerability, September 20, 2016

ICSA-16-259-01 Yokogawa STARDOM Authentication Bypass Vulnerability, September 15, 2016

ICSA-16-259-02 ABB DataManagerPro Credential Management Vulnerability, September 15, 2016

ICSA-16-259-03 Trane Tracer SC Sensitive Information Exposure Vulnerability, September 15, 2016

ICSA-16-224-02 Rockwell Automation RSLogix 500 AND RSLogix Micro File Parser Buffer Overflow Vulnerability, September 15, 2016

ICSA-16-250-01 Siemens SIPROTEC 4 and SIPROTEC Compact Vulnerabilities, September 6, 2016

Other

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 13, 2016

NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report, September 28, 2016

Open Source Situational Awareness Highlights

The ICS "Subversive Six"- Unseen Risk Points in Your Industrial Networks

10-19-2016

http://www.belden.com/blog/industrialsecurity/the-ics-subversive-six-unseen-risk-points-in-your-industrial-networks.cfm

NIST Released Special Publication: SP 800-150

10-5-2016

http://csrc.nist.gov/news_events/#oct5

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Demonstration of hacking a protective relay and taking control of a motor – the grid is at risk

9-15-2016

http://www.controlglobal.com/blogs/unfettered/demonstration-of-hacking-a-protective-relay-and-taking-control-of-a-motor-the-grid-is-at-risk/

Coordinated Vulnerability Disclosure

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS-CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@hq.dhs.gov or toll free at 1-877-776-7585.

Researchers Assisting ICS-CERT with Products Published September/ October 2016

ICS-CERT appreciates having worked with the following researchers:

- Adam Crain of Automatak LLC, ICSA-16-299-01 Siemens SICAM RTU Devices Denial-of-Service Vulnerability, October 25, 2016
- Independent researcher Maxim Rupp, ICSA-16-294-01 Moxa EDR-810 Industrial Secure Router Privilege Escalation Vulnerability, October 20, 2016
- Independent researcher He Congwen, ICSA-16-292-01 Schneider Electric PowerLogic PM8ECC Hard-coded Password Vulnerability, October 18, 2016
- Alexandru Ariciu of Applied Risk, ICSA-16-287-05 Moxa ioLogik E1200 Series Vulnerabilities, October 13, 2016
- Ariele Caltabiano (kimiya) working with Trend Micro's Zero Day Initiative (ZDI), ICSA-16-287-06 Fatek Automation Designer Memory Corruption Vulnerabilities, October 13, 2016
- Martin Jartelius and John Stock of Outpost 24, ICSA-16-287-07 Kabona AB WDC Vulnerabilities, October 13, 2016
- Rapid7, ICSMA-16-279-01 Animas OneTouch Ping Insulin Pump Vulnerabilities, October 5, 2016
- Independent researcher Ehab Hussein of IOActive, ICSA-16-278-01 INDAS Web SCADA Path Traversal Vulnerability, October 4, 2016
- Gregor Bonney from FH Aachen University of Applied Sciences, ICSA-16-278-02 Beckhoff Embedded PC Images and TwinCAT Components Vulnerabilities, October 4, 2016
- Independent researcher Maxim Rupp, ICSA-16-273-01 American Auto-Matrix Front-End Solutions Vulnerabilities, September 29, 2016
- Independent researcher Zhou Yu, ICSA-16-264-01 Moxa Active OPC Server Unquoted Service Path Escalation Vulnerability, September 20, 2016
- Karn Ganeshen, ICS-ALERT-16-263-01 BINOM3 Electric Power Quality Meter Vulnerabilities, September 19, 2016
- Trend Micro's Zero Day Initiative (ZDI), ICSA-16-259-02 ABB DataManagerPro Credential Management Vulnerability, September 15, 2016
- Independent researcher Maxim Rupp, ICSA-16-259-03 Trane Tracer SC Sensitive Information Exposure Vulnerability, September 15, 2016
- Ariele Caltabiano (kimiya) working with Trend Micro's Zero Day Initiative, ICSA-16-224-02 Rockwell Automation RSLogix 500 AND RSLogix Micro File Parser Buffer Overflow Vulnerability, September 15, 2016

Upcoming Events

December 2016

Industrial Control Systems Cybersecurity (301) Training (5 days)

December 12-16

Idaho Falls, Idaho

Closed

January 2017

Industrial Control Systems Cybersecurity (301) Training (5 days)

January 9 - 13

Idaho Falls, Idaho

Closed

For a current schedule of events that the ICS-CERT is supporting and may be of interest to control system individuals involved in security, go to https://ics-cert.us-cert.gov/calendar.

PCII Protection – Your Information Will Be Protected

Industry partners may request protection under the Critical Infrastructure Information Act of 2002 when submitting information to ICS-CERT. If the proper process is followed and ICS-CERT validates that information, it becomes PCII. ICS-CERT's policy is to keep confidential any reported information specific to your organization or activity. Protected Critical Infrastructure Information (PCII) protections mean that homeland security partners can be confident that sharing their information with the government will not expose sensitive or proprietary data. PCII can only be accessed in accordance with strict safeguarding and handling requirements. Only trained and certified federal, state, and local government employees or contractors may access PCII. (http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program).

Reporting Incidents

Please let us know if you have experienced a cyber intrusion or anomalous activity on your network. Reporting to ICS-CERT is completely voluntary; however, your information is extremely useful for understanding the current threat landscape, including the techniques adversaries are using, types of malware, possible intent of campaigns, and sectors targeted. Prompt and detailed reporting can lead to early detection and prevent incidents from occurring against the nation's critical infrastructure.

We Want to Hear from You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: ics-cert@hq.dhs.gov.

ICS-CERT publishes the ICS-CERT Monitor bimonthly, six times a year.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT web page at: http://ics-cert.us-cert.gov.

Please direct all questions or comments about the content or suggestions for future content to ICS CERT at: ics-cert@hq.dhs.gov.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.