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 here: 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 here: 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

Incident Response Activity

Notable Incident

As part of normal operations, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) found a number of internet-facing devices on Shodan. Many of the Shodan entries show an IP address owned by an Internet Service Provider (ISP).

ISPs do not provide customer information to ICS-CERT. We coordinated a message to the ISPs through the National Coordinating Center for Communications (NCC), which, along with ICS-CERT and the United States Computer Emergency Readiness Team (US-CERT), is a component of the National Cybersecurity Communications and Integration Center (NCCIC). The message asked the ISPs to contact the endpoint customer with the findings and to reach out to ICS-CERT for further assistance, if needed.

As part of normal operations, ICS-CERT found a number of Internet facing devices on Shodan.

One ISP sent registered messages to endpoint customers with the specific findings from the Shodan search and information to contact ICS-CERT. A vendor/integrator supporting a water facility, who received the message from the ISP, called ICS-CERT. We notified them of our findings and are currently working on a mitigation plan to heighten their security posture.

Viewing Your Network through the Eyes of an Attacker

From the Spring 2016 Industrial Control Systems Joint Working Group (ICSJWG) presentation by ICS-CERT's Terrance McKay and Richard Wyman

For over seven years, ICS-CERT has worked with its industry partners to improve the cybersecurity posture of their industrial control systems (ICSs) through onsite assessments. The assessment offerings include the Cyber Security Evaluation Tool (CSET®), the Design Architecture Review (DAR), and the Network Analysis Verification and Validation (NAVV). Each type of assessment serves a different purpose. The CSET focuses on the administrative aspects of the systems life cycle (procure, install, maintain, and dispose) by asking a series of yes and no questions. The DAR is more free-flowing in that it is a facilitated discussion of the industry partner's network architecture. The NAVV is an analysis of the data traffic captured at key boundary points in the network. Collectively, these three assessments have given ICS-CERT a broad overview of the state of the cybersecurity of control systems that monitor and control the nation's infrastructure.

One of the key observations made by ICS-CERT's assessment team is that the cybersecurity maturity level of the organization is often related to:

- how well the organization knows what information is publicly available on its control system,
- how this information is controlled,
- how its system is designed, and
- how data flow from one node to another, especially as it crosses the ICS/IT perimeter.

To simplify it, the cybersecurity maturity level of the organization is dependent on how well it knows and understands its control system and network.

Why is this important? When malicious actors target a cyber system, they do extensive reconnaissance of the system using techniques like footprinting, which is a methodical process for profiling the system and scanning to learn everything they can about it. This is an essential step before launching an attack.

When an organization can view its system through the eyes of attackers, concrete steps can be taken to put controls into place reducing the risk of malicious actors from targeting its system.

Some of the tools and techniques the assessment team uses to help asset owners better understand their systems include open source research, Shodan searches, and passive scans of ICS networks. Using these tools and techniques will allow you to know what an attacker likely knows about your network. The better you know your own network, the better you're able to defend it.

Understanding the Protected Critical Infrastructure Information Process

In the previous issue of the Monitor, we discussed the Protected Critical Infrastructure Information (PCII) Program (https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Mar-Apr2016_S508C.pdf). In this Monitor, we discuss how an asset owner or operator receives PCII protection.

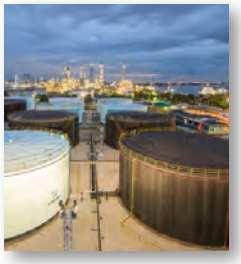
The PCII express statement is the vehicle used to codify the PCII agreement with ICS-CERT. In the document, it states the information being submitted is not available in the public domain and the information is not being submitted in lieu of any regulatory requirement.

Once signed and returned, the protections mentioned in the previous PCII article are in place. If needed, an asset owner may have the form reviewed and signed by their own legal counsel or by an authorized party. An integrator may submit the express statement on behalf of an asset owner they are supporting. The incident handler will set the contact up with a US-CERT Portal account to be able to share information and documentation outside normal email channels for additional security and privacy. When the express statement is complete, it can be sent to the incident handler via the portal.

As stated in the PCII Express Statement, information cannot be submitted in lieu of a regulatory requirement. If the sector in which an asset owner operates requires reporting, that should be completed by the asset owner. To strengthen the trust relationship with the asset owner and operators, ICS-CERT cannot be subpoenaed for the data submitted under PCII, nor will we share details with a regulator. ICS-CERT cannot provide a robust mitigation without a full context of information and understanding of the situation.

Asset owners and operators are welcome to contact ICS-CERT at any time for questions or clarification about the process.





Industrial Control Systems Joint Working Group

Spring 2016 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) 2016 Spring Meeting was held at Chaparral Suites—Scottsdale in Scottsdale, Arizona, on May 3–5. This was the largest ICSJWG Meeting to date, bringing together over 300 stakeholders from the ICS community. Over the course of three days, attendees had the opportunity to network and interact through demonstrations, presentations, panels, and lightning round talks.

Highlights of the 2016 Spring Meeting:

- Keynote presentations from:
  - Gregory Touhill, Deputy Assistant Secretary for Cybersecurity and Communications;
  - Frank Grimmelmann, President and CEO of Arizona Cyber Threat Response Alliance (ACTRA);
  - Mark Fabro, President and Chief Scientist of Lofty Perch; and
  - Marty Edwards, Director of ICS-CERT.
- A Hands-On Forensics Technical Workshop that allowed attendees to learn recommended best practices for performing hard drive and memory captures on a live system.
- ICSJWG's second Vendor Expo.
- "Ask Me Anything" session with Marty Edwards.

Fall 2016 Meeting Preview

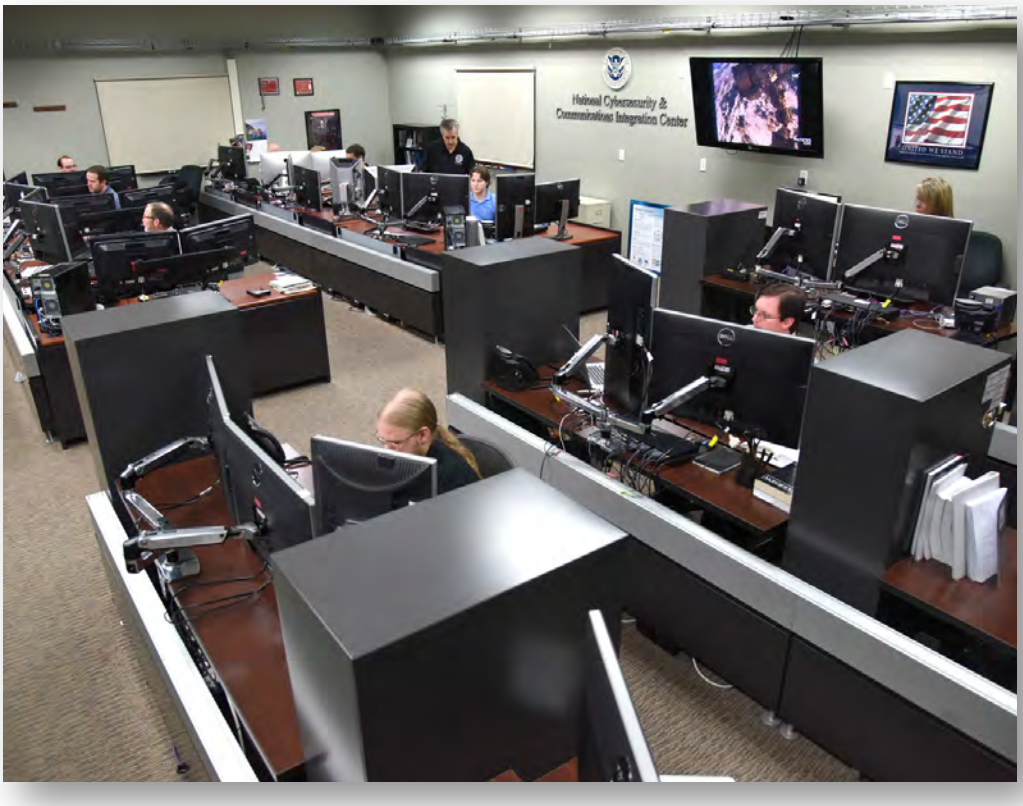
We are excited to announce that the ICSJWG 2016 Fall Meeting will take place September 13-15, 2016, at Embassy Suites Ft. Lauderdale—17th Street in Ft. Lauderdale, Florida. Registration is now open and the ICSJWG is accepting abstracts until July 8th.

- Confirmed Keynote Speakers:
  - Billy Rios, Founder of WhiteScope
  - John Felker, Director of Operations, NCCIC
- Meeting Highlights:
  - Hands-On Technical Workshop and Training focused on Network Monitoring of ICS and Google Hacking/Shodan
  - "Ask Me Anything" session with NCCIC/ICS-CERT representatives
  - ICS Vulnerability Research Panel
  - Back by Popular Demand: "Viewing Your Network Through the Eyes of an Attacker"

Additional information regarding the venue, call-for-abstracts, and registration are available on the ICSJWG website: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

The AAL at the ICSJWG Spring 2016 Meeting

ICS-CERT's Advanced Analytical Laboratory (AAL) attended the ICSJWG Spring 2016 conference in Scottsdale, Arizona, to present on the evolving trends of malware design and the changing tactics of attackers. The AAL created this presentation as an expansion on the September/October 2015 Monitor article titled "Trends in Malware," in which they discussed some of the threats faced by both commercial industry and individual users (https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep-Oct2015.pdf).



Over the last decade, malware design has become more developed and streamlined, malware authors have begun selling their wares to third parties, and the number of threat actors has increased dramatically because of a lowered skillset requirement when orchestrating an attack. With the steady growth in ransomware as an example, the profitability of extortion by means of malware has solidified to a 1,425-percent return on investment for criminals (https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf). The targeting of essential operations requires the victim to quickly find a solution and avoid downtime or loss of critical operational capabilities (http://sanfrancisco.cbslocal.com/2016/02/18/california-hospital-ransomware-attack-hackers/). This, along with the inability to continue delivery of services and the damage done to the victim's reputation, dramatically increases the likelihood of the victim acceding to the attacker's demands.

While the end user of a system often detects ransomware, other infections take great care to avoid detection. Tracking down compromises presents a challenge and may require the combination of data from many sources across the network, such as event logs and network packet captures.

Once asset owners identify a compromise, they face a challenging path to remediation, especially in critical networks supporting ICS or when the attack has gone unnoticed for a long period of time. The fastest or easiest solution to getting the suspect system off the network may only delay an attack or alert the attackers that the asset owner has tracked them. Worse, some remediation actions may destroy evidence that a responder might need to mitigate the threat.

During the ICSJWG Spring 2016 meeting, the AAL also held a hands-on, technical workshop for attendees to become familiar with utilities used to capture hard drive and memory images for later analysis. These images can allow an analyst to identify artifacts created by threat actors on a compromised system, as well as decipher what techniques or utilities the threat actors used during the attack and what information they took. This analysis provides the information necessary for the identification of malware and remediation after identifying an attack, and potentially aiding in the prevention of future compromises. The AAL's publicly available fact sheet titled "So You Think You've Been Compromised" describes the different steps of the image capturing process (https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_AreYouCompromised_S508C.pdf).

During the conference, members from AAL heard many questions and concerns from people throughout the ICS space, with topics ranging from data integrity and challenges with whitelisting to the detection of unknown malicious activity on the network. These problems do not have quick fixes and often challenge both administrators and end users with the difficult task of weighing usability against security.

As malware continues to evolve and as attackers adapt to a more technologically adept and security-minded generation of computing, the AAL will continue its work to increase awareness of the new and constantly evolving threats to the ICS sectors.

ICS-CERT Assessment Activity for May/June 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 May/June 2016, ICS-CERT conducted 21 onsite assessments across five sectors (Table 1). Of these 21 assessments, eight were Cyber Security Evaluation Tool (CSET®) assessments, six were Design Architecture Review (DAR) assessments, and seven 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, May/June 2016.

Assessments by Sector	May 2016	June 2016	May/June Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy			
Financial Services			
Food and Agriculture		3	3
Government Facilities		1	1
Healthcare and Public Health			
Information Technology		1	1
Nuclear Reactors, Materials, and Waste			
Transportation Systems	5		5
Water and Wastewater Systems	7	4	11
Monthly Totals	12	9	21 Total Assessments

Table 2. Assessments by type, March/April 2016.

Assessments by Type	May 2016	June 2016	May/June Totals
CSET	7	1	8
DAR	2	4	6
NAVV	3	4	7
Monthly Totals	12	9	21 Total Assessments

Assessment Trends

The top six weaknesses the ICS-CERT assessment team found in 2015 fell under the categories of (1) boundary protection, (2) least functionality, (3) authenticator management, (4) identification and authentication, (5) least privilege, and (6) allocation of resources. By comparison, the three main weaknesses the team has seen in recent months include two of these categories, boundary protection and identification and authentication, but also includes the category of configuration settings.

Boundary protection. Most of the networks assessed by ICS-CERT are physically flat, with no internal boundaries or segmentation. ICS-CERT recommends both internal and external network boundaries, using Layer 2 and 3 devices to control network traffic and provide a logical place to monitor network traffic. Control systems should not run on the same network as business systems.

Configuration settings. One of the most common issues found by the assessment team is misconfiguration or inconsistent configuration. Another common issue is the failure to harden servers by removing unnecessary services and locking down ports and settings to the least functionality needed to run the necessary functions.

Identification and authentication. Many control systems use common or group accounts. This prevents the ability to identify which users are on a system and who is doing what. The assessment team recommends that individual accounts be used for all system access. If this isn't possible, compensating controls should be implemented to provide accountability for actions. Another issue in this category is the failure to use multifactor authentication in remote connections. Remote connections are one of the greatest risks to control systems, and ICS-CERT recommends that extra precaution be taken to identify and authenticate remote access users. Multifactor authentication could be implemented with something as simple as an RSA token with a time-based key or a call back method to verify the user.

In recent months, the assessment team has also seen an increased use of newer technologies such as Virtual Routing and Forwarding (VRF) and Layer 7 Firewalls that automatically segment networks based on deep packet analysis of traffic. With newer technologies being used in the control system environment, some deep seated ideas in securing control systems are shifting. The assessment team is reviewing these new technology implementations to determine what security risks they present.

Recent Product Releases

Alerts

ICS-ALERT-16-182-01 Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities, June 30, 2016

Advisories

View Advisories Feed

ICSA-16-182-01 Eaton ELCSoft Programming Software Memory Vulnerabilities, June 30, 2016

ICSA-16-182-02 Siemens SICAM PAS Vulnerabilities, June 30, 2016

ICSA-16-175-01 Rockwell Automation Allen-Bradley Stratix 5400 and 5410 Packet Corruption Vulnerability, June 23, 2016

ICSA-16-175-02 Unitronics VisiLogic OPLC IDE vlp File Parsing Stack Buffer Overflow Vulnerability, June 23, 2016

ICSA-16-175-03 Meinberg NTP Time Server Vulnerabilities, June 23, 2016

ICSA-16-173-01 Advantech WebAccess ActiveX Vulnerabilities, June 21, 2016

ICSA-16-173-02 Schneider Electric PowerLogic PM8ECC Cross-site Scripting Vulnerability, June 21, 2016

ICSA-16-168-01 Moxa PT-7728 Series Switch Improper Authorization Vulnerability, June 16, 2016

ICSA-16-166-01 OSIsoft PI SQL Data Access Server Input Validation Vulnerability, June 14, 2016

ICSA-16-166-02 OSIsoft PI AF Server Input Validation Vulnerability, June 14, 2016

ICSA-16-161-01 Siemens SIMATIC S7-300 Denial-of-Service Vulnerability, June 9, 2016

ICSA-16-161-02 Siemens SIMATIC WinCC Flexible Weakly Protected Credentials Vulnerability, June 9, 2016

ICSA-16-159-01 Trihedral VTScada Vulnerabilities, June 7, 2016

ICSA-16-126-01 KMC Controls Conquest BACnet Router Vulnerabilities, June 7, 2016

ICSA-16-154-01 GE MultiLink Series Hard-coded Credential Vulnerability, June 2, 2016

ICSA-16-152-01 Moxa UC 7408-LX-Plus Firmware Overwrite Vulnerability, May 31, 2016

ICSA-16-152-02 ABB PCM600 Vulnerabilities, May 31, 2016

ICSA-16-147-01A Environmental Systems Corporation Data Controllers Vulnerabilities (Update A), May 26, 2016

ICSA-16-147-02 Sixnet BT Series Hard-coded Credentials Vulnerability, May 26, 2016

ICSA-16-147-03 Black Box AlertWerks ServSensor Credential Management Vulnerability, May 26, 2016

ICSA-16-145-01 Moxa MiiNePort Vulnerabilities, May 24, 2016

ICSA-16-140-01 Resource Data Management Intuitive 650 TDB Controller Vulnerabilities, May 19, 2016

ICSA-16-140-02 Siemens SIPROTEC Information Disclosure Vulnerabilities, May 19, 2016

ICSA-16-138-01 IRZ RUH2 3G Firmware Overwrite Vulnerability, May 17, 2016

ICSA-16-042-01 Moxa EDR-G903 Secure Router Vulnerabilities, May 17, 2016

ICSA-16-133-01A Meteocontrol WEB'log Vulnerabilities (Update A), May 17, 2016

ICSA-16-131-01 Panasonic FPWIN Pro Vulnerabilities, May 10, 2016

Follow ICS-CERT on Twitter: @icscert

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 May/June 2016

ICS-CERT appreciates having worked with the following researchers:

- Ariele Calgaviano working with Zero Day Initiative, ICSA-16-182-01 Eaton ELCSoft Programming Software Memory Vulnerabilities, June 30, 2016
- Ilya Karpov and Dmitry Sklyarov of Positive Technologies, ICSA-16-182-02 Siemens SICAM PAS Vulnerabilities, June 30, 2016
- Steven Seeley of Source Incite, ICSA-16-175-02 Unitronics VisiLogic OPLC IDE vlp File Parsing Stack Buffer Overflow Vulnerability, June 23, 2016
- Independent researcher Ryan Wincey, ICSA-16-175-03 Meinberg NTP Time Server Vulnerabilities, June 23, 2016
- Zhou Yu of Acorn Network Security, ICSA-16-173-01 Advantech WebAccess ActiveX Vulnerabilities, June 21, 2016
- Independent researcher Can Demirel, ICSA-16-168-01 Moxa PT-7728 Series Switch Improper Authorization Vulnerability, June 16, 2016
- Independent researcher Maxim Rupp, ICSA-16-126-01 KMC Controls Conquest BACnet Router Vulnerabilities, June 7, 2016
- Independent researcher Maxim Rupp, ICSA-16-147-01A Environmental Systems Corporation Data Controllers Vulnerabilities (Update A), May 26, 2016
- Independent researcher Neil Smith, ICSA-16-147-02 Sixnet BT Series Hard-coded Credentials Vulnerability, May 26, 2016
- Independent researcher Lee Ryman, ICSA-16-147-03 Black Box AlertWerks ServSensor Credential Management Vulnerability, May 26, 2016
- Independent researcher Karn Ganeshen, ICSA-16-145-01 Moxa MiiNePort Vulnerabilities, May 24, 2016
- Independent researcher Maxim Rupp, ICSA-16-140-01 Resource Data Management Intuitive 650 TDB Controller Vulnerabilities, May 19, 2016
- Independent researcher Maxim Rupp, ICSA-16-042-01 Moxa EDR-G903 Secure Router Vulnerabilities, May 17, 2016
- Independent researcher Karn Ganeshen ICSA-16-133-01A Meteocontrol WEB'log Vulnerabilities (Update A), May 17, 2016

Upcoming Events

September 2016

ICSJWG 2016 Fall Meeting

September 13-15

Ft. Lauderdale, Florida

Course description and registration

October 2016

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

Date TBD

Idaho Falls, Idaho

Course description and registration link will be posted when available

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.