



NCCIC

ICS-CERT MONITOR



Contents

ICS-CERT News

Situational Awareness

ICS-CERT Q&A

Onsite Assessment Summary

Recent Product Releases

Open Source Situational
Awareness Highlights

Coordinated Vulnerability Disclosure

Upcoming Events

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: <https://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/USDH-SUSCERT/subscriber/new>.

Downloading PGP/GPG Keys

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

This product is provided "as is" for informational purposes only. DHS does not provide any warranties of any kind regarding any information contained herein. DHS does not endorse any commercial product or service referenced in this publication or otherwise.

ICS-CERT News

ICS-CERT International Training in Lithuania

In July, instructors from the Department of Homeland Security's ICS-CERT Training team traveled to Vilnius, Lithuania, to present an international training session on cybersecurity for industrial control systems (ICS) at the University of Lithuania's Faculty of Mathematics and Informatics.

The Lithuanian Ministry of Defense (MOD) hosted the training in cooperation with the United States European Command (EUCOM).

Over 100 information technology specialists who work in various critical infrastructure (CI) sectors in Lithuania and other NATO countries attended the training. Countries represented include the Czech Republic, Denmark, Estonia, Germany, Latvia, Lithuania, Netherlands, Poland, Slovak Republic, Slovenia, and the United States.

Days one and two of this four-day event provided attendees with an introduction to the basics of ICS security and technical instruction on the protection of ICS using offensive and defensive methods.

On day three, students split into two groups. The first group participated in a hands-on session that helped them understand how and why attacks against process control systems work and provided mitigation strategies to increase the cyber security posture of their control systems networks.

The second group attended two informational briefs provided by the Defense Information Systems Agency (DISA) and EUCOM representatives.

On day four, students in the first group attended the informational briefs while the second group participated in the hands-on session.

The Point of Contact for the training event, a cybersecurity specialist from Lithuania's CSTS MOD (Cyber Security Telecommunications Service, Ministry of Defense), said, "Thank you for your great effort and this wonderful opportunity to educate our specialists. I would say it was a great success."



ICS-CERT at Black Hat/DEF CON 2017

In late July, ICS-CERT team members once again attended the Black Hat and DEFCON conferences in Las Vegas, Nevada. Attendance at these conferences allows ICS-CERT the opportunity to provide ICS demonstrations; follow trends in the research community; learn of and respond to unanticipated vulnerability disclosures; and interface with researchers, manufacturers, and vendors. Each conference commonly hosts technical presentations relevant to ICS-CERT's work in ICS cybersecurity and provides the opportunity for ICS-CERT to gain valuable security information and make professional contacts. Each year, interactions with researchers help ICS-CERT to better understand and address current security trends and concerns. The conferences allow ICS-CERT to interact with IT and ICS vendors to learn more about their products. ICS-CERT team members also present and demonstrate the ICS Village, which provides the attendees with insight into the operation of ICSs and the cybersecurity issues involved. ICS-CERT's



participation in these conferences helps to build relationships with its partners in the ICS community and contributes to its efforts to mitigating risk to the Nation's CI through the sharing of information.

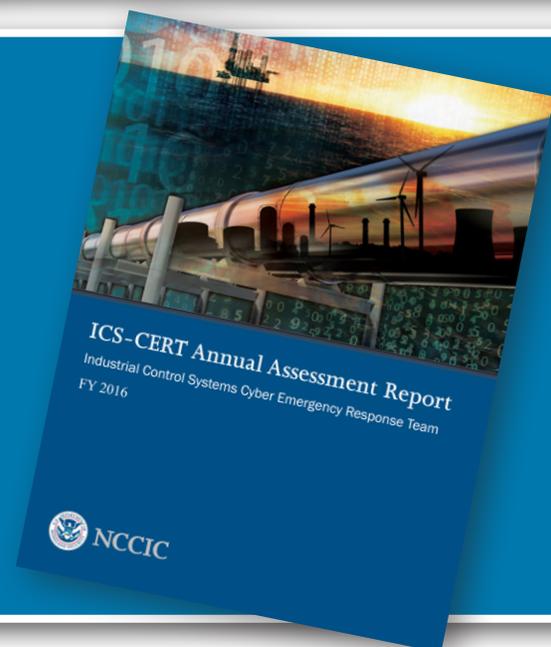
ICSJWG Fall Meeting 2017 Preview



ICS-CERT will hold the 2017 Fall Industrial Control Systems Joint Working Group (ICSJWG) Meeting on September 12–14, 2017, in Pittsburgh, Pennsylvania, at the Omni William Penn Hotel. The meeting will provide an opportunity for stakeholders to interface with peers, network with industry leaders, and stay abreast of the latest initiatives affecting security for ICS and our CI. The Fall 2017 meeting will provide a forum for all control systems stakeholders to gather and exchange ideas about critical issues in ICS cybersecurity. The Meeting will include three full days of presentations and discussions in the form of keynote speakers (including NCCIC Director John Felker and Joel Brenner of MIT/IPRI-CIS) practical demonstrations, presentations, and panels. The Fall meeting will feature the return of the Hands-on Technical workshop, a Vendor Expo, and an "Ask Me Anything" session with ICS-CERT. For event and registration information, visit the [ICSJWG web page](#). We look forward to seeing you in Pittsburgh!

ICS-CERT Releases Third Annual Assessment Report

In July, ICS-CERT released the 2016 Annual Assessment Report. This year marks the third publishing year for this ICS-CERT report, which captures the Assessment team's consolidated discoveries and activities throughout the year. As in previous years, the report provides our stakeholders with important information they can use to help secure their control systems and associated CI. The report summarizes key discoveries, including the most common vulnerabilities across our customer base; provides year-over-year vulnerability comparisons across CI sectors; shows where we focused our activity in FY 2016; describes how customers can request an assessment; and provides our customers with recommendations for enhancing their ICS cybersecurity posture.



Medical Cybersecurity

In calendar year 2016, NCCIC/ICS-CERT publicly released five medical device advisories to the ICS-CERT website. The total number of vulnerabilities identified in the 2016 medical advisories is 1,884. The vast majority of these vulnerabilities, 1,878 to be precise, come from two advisories that report on vulnerabilities identified by automated scanning tools. These scanning tools expedite the vulnerability detection process and make it easier to detect out-of-date, third-party software issues. To prevent this much larger data set from skewing the analysis, ICS-CERT has excluded these anomalous vulnerabilities from the vulnerability metrics analysis. The six remaining vulnerabilities identified in 2016 are Incorrect Permission Assignment for Critical Resource (CWE-732), Channel Accessible by Non-Endpoint (CWE-300), Authentication Bypass by Capture-replay (CWE-294), Use of Insufficiently Random Values (CWE-330), Cleartext Transmission of Sensitive Information (CWE-319), and Stack-based Buffer Overflow (CWE-121). The average CVSS score for these vulnerabilities is 7.1, which is categorized as having a high potential impact.

ICS-CERT works with researchers and vendors to achieve a timely solution to identified cybersecurity vulnerabilities. In 2016, 89 percent of all vulnerabilities that ICS-CERT helped coordinate resulted in the vendors issuing some type of mitigation. For the five medical advisories released in 2016, two advisories referenced vendor issued mitigations, equating to 40 percent. ICS-CERT's cumulative average time to close a vulnerability ticket is 135 days; however, for the medical device tickets in 2016, the average time to close is 210 days. This data suggests that medical device vulnerabilities often have added complexities.

A review of ICS-CERT's medical advisory data for 2016 indicate that medical device vulnerabilities have the potential to have a high impact and may take longer to resolve. In 2017, ICS-CERT has already seen a steady increase of reported medical vulnerabilities. As of August 31, ICS-CERT has published 10 medical device advisories and 4 alerts related to the Healthcare and Public Health sector. ICS-CERT's work on medical vulnerabilities over the past several years indicates that the growing interest in securing medical devices is warranted and the need for it can be expected to continue in the near future.

ICS-CERT Q&A

Assessments Q&A

What is the deliverable?

Upon completion of the assessment process, ICS-CERT will compile an in-depth report for the asset owner, including a prioritized analysis of key discoveries and practical mitigations for enhancing the organization's cybersecurity posture.

Who will receive the final report?

ICS-CERT will send the final report to the POC. The POC may share as they deem appropriate.

How long will the report take to complete?

Approximately 6-8 weeks after the completion of the assessment

For more information, see ICS-CERT's Assessment [FAQs](#) and [Fact Sheets](#).



PCII Q&A

Who can submit information to the PCII program?

Individuals or entities who have information about a CI that is not customarily in the public domain, as defined by the CII Act and the Final Rule, can provide such information to the Protected Critical Infrastructure Information (PCII) Program, so long as the information is submitted in good faith and is not submitted in lieu of compliance with any regulatory requirement. Individuals submitting on behalf of entities must be authorized to do so by the entity. Entities that might submit information include, but are not limited to:

- Private sector companies,
- Working groups comprised of government and private sector representatives, and
- State and local government entities.

What types of information-sharing partnerships and programs can benefit from the PCII program?

The PCII Program provides protections used in various public-private infrastructure information-sharing programs, both within DHS and in other Federal agencies. DHS information-sharing programs include:

- Infrastructure Information Collection Division's Automated Critical Asset Management System (ACAMS), and
- Protective Security Coordination Division's Site Assistance Visits (SAVs) and Buffer Zone Plans (BZPs), Enhanced CI Program's (ECIP) Infrastructure Survey Tool (IST).

For additional questions and answers, see the [PCII FAQs](#).

ICS-CERT Assessment Activity for July/August 2017

ICS-CERT conducts onsite cybersecurity assessments of ICSs to help strengthen the cybersecurity posture of CI owners and operators and of ICS manufacturers. In July/August 2017, ICS-CERT conducted 38 onsite assessments across six sectors (Table 1). Of these 38 assessments, seven were Cyber Security Evaluation Tool (CSET®) assessments, 18 were Design Architecture Review (DAR) assessments, and 13 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, July/August 2017.

Assessments by Sector	July 2017	August 2017	July/August Totals
Chemical			
Commercial Facilities	4	3	7
Communications			
Critical Manufacturing			
Dams	1		1
Defense Industrial Base			
Emergency Services			
Energy	1	9	10
Financial Services			
Food and Agriculture			
Government Facilities	3	5	8
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems		5	5
Water and Wastewater Systems	4	3	7
Monthly Totals	13	25	38 Total Assessments

Table 2. Assessments by type, July/August 2017.

Assessments by Type	July 2017	August 2017	July/August Totals
CSET™	1	6	7
DAR	7	11	18
NAVV	5	8	13
Monthly Totals	13	25	38 Total Assessments



Recent Product Releases

Alerts

[ICS-ALERT-17-216-01](#) Eaton ELCSOFT Vulnerabilities, August 4, 2017

[ICS-ALERT-17-209-01](#) CAN Bus Standard Vulnerability, July 28, 2017

[ICS-ALERT-17-206-01](#) CRASHOVERRIDE Malware, July 25, 2017

Advisories

[ICSA-17-243-01](#) Siemens OPC UA Protocol Stack Discovery Service, August 31, 2017

[ICSA-17-243-02](#) Siemens LOGO!, August 31, 2017

[ICSA-17-243-03](#) Siemens 7KM PAC Switched Ethernet, August 31, 2017

[ICSA-17-243-04](#) OPW Fuel Management Systems SiteSentinel Integra and SiteSentinel iSite, August 31, 2017

[ICSA-17-243-05](#) Moxa SoftCMS Live Viewer

[ICSA-17-150-01](#) Automated Logic Corporation ALC WebCTRL, Liebert SiteScan, Carrier i-VU, August 31, 2017

[ICSMA-17-241-01](#) Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities, August 29, 2017

[ICSA-17-241-01](#) AzeoTech DAQFactory, August 29, 2017

[ICSA-17-241-02](#) Advantech WebAccess, August 29, 2017

[ICSA-17-236-01](#) Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455, August 24, 2017

[ICSA-17-208-04](#) Rockwell Automation Allen-Bradley Stratix and ArmorStratix, August 24, 2017

[ICSA-17-234-01](#) Automated Logic Corporation WebCTRL, i-VU, SiteScan, August 22, 2017

[ICSA-17-234-02](#) SpiderControl SCADA MicroBrowser, August 22, 2017

[ICSA-17-234-03](#) SpiderControl SCADA Web Server, August 22, 2017

[ICSMA-17-229-01](#) Philips' DoseWise Portal Vulnerabilities, August 15, 2017

[ICSA-17-227-01](#) Advantech WebOP, August 15, 2017

[ICSMA-17-227-01](#) BMC Medical and 3B Medical Luna CPAP Machine, August 15, 2017

[ICSA-17-222-01](#) SIMPlight SCADA Software, August 10, 2017

[ICSA-17-222-02](#) Solar Controls Heating Control Downloader (HC-Downloader), August 10, 2017

[ICSA-17-222-03](#) Solar Controls WATTConfig M Software, August 10, 2017

[ICSA-17-222-04](#) Fuji Electric Monitouch V-SFT, August 10, 2017

[ICSA-17-222-05](#) ABB SREA-01 and SREA-50, August 10, 2017

[ICSA-17-220-01](#) OSIsoft PI Integrator, August 8, 2017

[ICSA-17-220-02](#) Moxa SoftNVR-IA Live Viewer, August 8, 2017

[ICSA-17-215-01](#) Schneider Electric Pro-face GP-Pro EX, August 3, 2017

[ICSMA-17-215-01](#) Siemens Molecular Imaging Vulnerabilities, August 3, 2017

[ICSMA-17-215-02](#) Siemens Molecular Imaging Vulnerabilities, August 3, 2017

[ICSA-17-213-01](#) Mitsubishi Electric Europe B.V. E-Designer, August 1, 2017

[ICSA-17-213-02](#) Schneider Electric Trio TView, August 1, 2017

[ICSA-17-208-01](#) Continental AG Infineon S-Gold 2 (PMB 8876), July 27, 2017

[ICSA-17-208-02](#) Mirion Technologies Telemetry Enabled Devices, July 27, 2017

[ICSA-17-208-03](#) PDQ Manufacturing, Inc. LaserWash, Laser Jet and ProTouch, July 27, 2017

[ICSA-17-187-03B](#) Siemens SIPROTEC 4 and SIPROTEC Compact (Update B), July 27, 2017

[ICSA-17-152-02](#) NXP i.MX Product Family, July 25, 2017

[ICSA-17-201-01](#) Schneider Electric PowerSCADA Anywhere and Citect Anywhere, July 20, 2017

[ICSA-17-138-03](#) Rockwell Automation MicroLogix 1100 Controllers, July 18, 2017

[ICSA-17-194-01](#) Siemens SiPass integrated, July 13, 2017

[ICSA-17-194-03](#) Siemens SIMATIC Sm@rtClient Android App, July 13, 2017

[ICSA-17-192-01](#) Siemens SIMATIC Logon, July 11, 2017

[ICSA-17-192-02](#) Fuji Electric V-Server, July 11, 2017

[ICSA-17-192-03](#) ABB VSN300 WiFi Logger Card, July 11, 2017

[ICSA-17-192-04](#) OSIsoft PI Coresight, July 11, 2017

[ICSA-17-192-05](#) OSIsoft PI ProcessBook and PI ActiveView, July 11, 2017

[ICSA-17-192-06](#) Schweitzer Engineering Laboratories, Inc. SEL-3620 and SEL-3622, July 11, 2017

[ICSA-17-187-01](#) Siemens OZW672 and OZW772, July 6, 2017

[ICSA-17-187-02](#) Siemens Reyrolle, July 6, 2017

[ICSA-17-187-04](#) Schneider Electric Wonderware ArchestrA Logger, July 6, 2017

[ICSA-17-187-05](#) Schneider Electric Ampla MES, July 6, 2017

Other Reports

[NCCIC/ICS-CERT FY 2016 Annual Vulnerability Coordination Report](#), August 2017

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 July/August 2017

ICS-CERT appreciates having worked with the following researchers:

- Sergey Temnikov of Kaspersky Lab, ICSA-17-243-01 Siemens OPC UA Protocol Stack Discovery Service, August 31, 2017
- Maxim Rupp, ICSA-17-243-02 Siemens LOGO!, August 31, 2017
- Semen Rozhkov of Kaspersky Lab, ICSA-17-243-04 OPW Fuel Management Systems SiteSentinel Integra and SiteSentinel iSite, August 31, 2017
- Security researcher Ziqiang Gu from Huawei WeiRan Labs, ICSA-17-243-05 Moxa SoftCMS Live Viewer, August 31, 2017
- Evgeny Ermakov from Kaspersky Lab, ICSA-17-150-01 Automated Logic Corporation ALC WebCTRL, Liebert SiteScan, Carrier i-VU, August 31, 2017
- MedSec Holdings Ltd, ICSMA-17-241-01 Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities, August 29, 2017
- Karn Ganeshen, ICSA-17-241-01 AzeoTech DAQFactory, August 29, 2017
- Independent researcher Fritz Sands, independent researcher rgod, Tenable Network Security, and an anonymous researcher, all working with Trend Micro's Zero Day Initiative, and Haojun Hou and DongWang from ADLab of Venustech, ICSA-17-241-02 Advantech WebAccess, August 29, 2017
- Mandar Jadhav from Qualys Security, ICSA-17-236-01 Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455, August 24, 2017
- Gjoko Krstic from Zero Science Lab, ICSA-17-234-01 Automated Logic Corporation WebCTRL, i-VU, SiteScan, August 22, 2017
- Karn Ganeshen, working with Trend Micro's Zero Day Initiative (ZDI), ICSA-17-234-02 SpiderControl SCADA MicroBrowser, August 22, 2017
- Karn Ganeshen, working with Trend Micro's ZDI, ICSA-17-234-03 SpiderControl SCADA Web Server, August 22, 2017
- Ariele Caltabiano (kimiya) working with Trend Micro's ZDI, ICSA-17-227-01 Advantech WebOP, August 15, 2017
- MedSec Holdings Ltd, ICSMA-17-227-01 BMC Medical and 3B Medical Luna CPAP Machine, August 15, 2017
- Karn Ganeshen, ICSA-17-222-01 SIMPLight SCADA Software, August 10, 2017
- Karn Ganeshen, ICSA-17-222-02 Solar Controls Heating Control Downloader (HCDDownloader), August 10, 2017
- Karn Ganeshen, ICSA-17-222-03 Solar Controls WATTConfig M Software, August 10, 2017
- Independent researchers Fritz Sands and kimiya working with Trend Micro's ZDI, ICSA-17-222-04 Fuji Electric Monitouch V-SFT, August 10, 2017
- Bertin Jose and Fernandez Ezequiel, ICSA-17-222-05 ABB SREA-01 and SREA-50, August 10, 2017
- Independent security researcher Karn Ganeshen, ICSA-17-220-02 Moxa SoftNVR-IA Live Viewer, August 8, 2017
- Karn Ganeshen, ICSA-17-215-01 Schneider Electric Pro-face GP-Pro EX, August 3, 2017
- Andrea "rgod" Micalizzi, working with Trend Micro's ZDI, ICSA-17-213-01 Mitsubishi Electric Europe B.V. E-Designer, August 1, 2017
- Karn Ganeshen, ICSA-17-213-02 Schneider Electric Trio TView, August 1, 2017
- Mickey Shkatov, Jesse Mic hael, and Oleksandr Bazhaniuk of the Advanced Threat Research Team at McAfee, ICSA-17-208-01 Continental AG Infineon S-Gold 2 (PMB 8876), July 27, 2017
- Ruben Santamarta of IOActive, ICSA-17-208-02 Mirion Technologies Telemetry Enabled Devices, July 27, 2017
- Billy Rios and Jonathan Butts of WhiteScope and independent security researcher Terry McCorkle, ICSA-17-208-03 PDQ Manufacturing, Inc. LaserWash, Laser Jet and ProTouch, July 27, 2017
- Quarkslab, ICSA-17-152-02 NXP i.MX Product Family, July 25, 2017
- Mark Gondree of Sonoma State University, Francisco Tacliad and Thuy Nguyen of the Naval Postgraduate School, ICSA-17-138-03 Rockwell Automation MicroLogix 1100 Controllers, July 18, 2017
- Karsten Sohr and Timo Glander from the TZI at the University of Bremen, ICSA-17-194-03 Siemens SIMATIC Sm@rtClient Android App, July 13, 2017
- Ariele Caltabiano working with Trend Micro's Zero Day Initiative, ICSA-17-192-02 Fuji Electric V-Server, July 11, 2017
- Maxim Rupp, ICSA-17-192-03 ABB VSN300 WiFi Logger Card, July 11, 2017
- Jason Holcomb with Revolutionary Security, ICSA-17-192-06 Schweitzer Engineering Laboratories, Inc. SEL-3620 and SEL-3622, July 11, 2017

Upcoming Events

September 2017

Industrial Control Systems Cybersecurity Joint Working Group (ICSJWG)
2017 Fall Meeting

September 12–14

Pittsburgh, Pennsylvania

[Additional Information](#)

NOTE: The September Industrial Control Systems Cybersecurity (301) Training has been cancelled for repair and updates to the HVAC systems in the training facility. The October sessions are already closed.

December 2017

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

December 11–15

Idaho Falls, Idaho

[Course description](#); Registration will be available ~90 days prior to the start date.

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. 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.

[Report an incident](#).

We Want to Hear from You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to 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>.