



NCCIC

ICS-CERT MONITOR



Contents

ICS-CERT Services
Situational Awareness
HSIN Tip
ICS-CERT News
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 Services

ICS-CERT ICSJWG Meetings

In this issue of the Monitor, we highlight ICS-CERT ICSJWG Meetings

The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) established the Industrial Control Systems Joint Working Group (ICSJWG) in 2009 to facilitate information sharing and collaboration among industrial control system (ICS) stakeholders from the 16 critical infrastructure (CI) sectors and the Federal government, with the purpose of reducing the cybersecurity risk to the nation's ICS. The ICSJWG provides a vehicle for the ICS community to network, collaborate, and share information freely.

The focal point of the ICSJWG is the biannual face-to-face meetings. These meetings provide the opportunity for anyone in the ICS community, newcomers and industry veterans alike, to network and share information formally or informally through presentations, panels, training sessions, demonstrations, and ad hoc discussions among peers. The face-to-face meetings are unique in that they target the ICS community and include all sectors, with subject matter experts from private industry, trade associations, information sharing groups, academia, and governmental agencies. The focus on networking and collaboration is what sets the ICSJWG meetings apart from a mere conference with presentations. ICSJWG members consistently give the face-to-face meetings high ratings for their relevancy and value to their professional lives. ICSJWG meetings are direct reflection of the ICS community, and the ICSJWG Program Management Office (PMO) strives to continuously improve the meetings based on stakeholder feedback.

In addition to the biannual meetings, the ICSJWG sponsors ad hoc webinars to address issues that are of concern to ICS stakeholders. The ICSJWG also publishes the ICSJWG Quarterly Newsletter and various other informational products. The newsletter includes relevant information from ICS-CERT along with articles and whitepapers submitted by the community. ICSJWG publishes information products as needed to raise awareness regarding a particular issue or to address a specific need.

For more on the ICSJWG's meetings, newsletters, and information products, go to the [ICSJWG page](#) on ICS-CERT's website.



Data Classification for Recovery Planning

Is your data air, water, or food?

To survive, a person needs air, water, and food. In Maslow's hierarchy of needs these are all first tier basic needs. The average person can survive for about three minutes without air, about three days without water, and about three weeks without food. All three categories are easily defined and prioritized.

In the information technology (IT)/operational technology (OT) world in which we live and operate, data is one of our first tier basic needs. Data needs to be identified, defined, and prioritized. Why? Because not all data is equal.

The argument that all of your data is important is an easy one to win. You can present a use case for every field in every table in every database in the network; however, the issue is not whether you need the data, but when you need it.

The most critical information should have the shortest backup cycle. This allows reinstallation of the most current information. For the recovery plan to be successful, it must account for every type of data.

An organization must consider the type of information needed to operate when evaluating the disruptions it could face. After identifying the different levels of data needed, an organization should prioritize according to the level of impact a disruption may have on various systems. An organization's tolerance for system downtime is inversely



proportional to the cost of recovery. The lower the tolerance for system downtime, the higher the cost to maintain a "hot" backup system. The organization should determine which systems must become functional again within minutes or hours and which can be down for days or weeks without serious impact.

These decisions must have executive-level support. The organization must directly tie IT asset priorities to business requirements. For an organization to perform an effective impact analysis, the IT professionals must be able to explain the impacts in business terms. Once the executives understand the consequences of system disruptions, they can support and fund recovery planning.

Let's consider the example of a financial institute, or a bank. In a normal day, a bank makes loans, receives loan payments, and processes members' deposits and withdrawals, among other operations. If the bank became a victim of ransom-

ware, a high priority would be to restore employee access, followed closely by customer access. Any archived data that isn't regularly accessed can be set as a low recovery priority.

Data classification is an essential part of disaster-recovery planning. How long can your business survive without each classification of data? Is it air, water, or food?

Cybersecurity Defense

The human element is always the weakest link of any cybersecurity defense system. Humans are the eyes and ears into what is actually happening and what computers cannot detect. They are also most likely to be involved in a system compromise. Every organization's cybersecurity defense plan should include security awareness training.

Today, employees face sophisticated spear phishing and ransomware attacks. They need regular training to maintain awareness of the importance of information security and their role in defending the company's network and business.

First, organizations should create and maintain policies and procedures regarding cyber security and computer usage to help staff members understand what is expected of them. These policies should cover all areas of the business, including corporate and ICS networks. For example, a bring your own device (BYOD) policy can expand a network's attack surface. Companies should have an official policy either forbidding BYOD or outlining the requirements for the use of personal devices. Companies should also define password policies for users and provide well-defined network-based security procedures for ICS. Procedures should



also provide users with information on what to do if they think an attack has compromised their machine.

Security awareness training should include the following:

- monthly phishing tests,
- brown bag lunch discussions on cyber security,
- posters reminding users of their security responsibilities, and
- cheat sheets or cards so users know what to do if something doesn't look right.

Organizations can build security awareness programs in house or with commercially available programs, but however it is done, security awareness training is an important part of defending your network. And the users are always the first line of defense.

Tips for using The Homeland Security Information Network



The Homeland Security Information Network (HSIN) provides many online training options for new and experienced users.

When you log on to HSIN, from the HSIN Central landing page, choose either the Training link on the blue menu bar or the “Take a HSIN Class” link in the Quicklinks menu on the right side of the page.

The HSIN Training page includes a list of “User Training” items. The HSIN Basics training is a very useful overview of HSIN that DHS recommends for all HSIN users. HSIN

Basics provides HSIN users with a general understanding of HSIN:

- What is HSIN?
- How is HSIN used?
- What are Mission Advocates?
- What are HSIN features?
- What are HSIN Document Management Best Practices?

The HSIN Training page also includes a series of links to training on “HSIN Features”:

- HSIN Connect,
- HSIN Box,
- HSIN Notify,
- HSIN Chat, and
- User Directory.

HSIN online training is self-paced; users can start/stop as time permits.

Take the opportunity to get the most out of your HSIN experience. Log in or request a HSIN account [here](#).



ICSJWG Meetings

ICSJWG Fall 2017 Meeting Preview

ICS-CERT is excited to announce that the 2017 Fall Industrial Control Systems Joint Working Group (ICSJWG) Meeting will take place 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 critical infrastructure. 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 days of presentations and discussions in the form of keynote speakers (including NCCIC Director of Operations 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 Q&A

Assessments Q&A

Who should be at the assessment?

Please invite any personnel including control systems operators/engineers, IT, policy/management personnel, and subject matter experts who are familiar with your site's control system architecture, topologies, and protocols to attend the assessment.

How long do you need to complete the assessment?

A CSET/DAR/NAVV assessment will take approximately 3–4 days to complete.

What kind of meeting space should I secure for the assessment?

Please ensure that a meeting room is reserved with a projector. We recommend a round table or U-shaped table setup in the room in order to better facilitate questions and discussion.

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

PCII Q&A

What are the penalties for intentionally mishandling PCII?

Recognizing that receipt of CII submissions from the private sector is contingent upon keeping submissions safe from unauthorized access, distribution, and misuse, the CII Act and the Final Rule apply criminal and civil penalties for intentionally mishandling PCII. All Federal, state and local government employees with access to PCII, including the program manager, all program staff, officers and deputy officers, and all designees of the program manager share responsibility for ensuring that PCII is properly safeguarded in accordance with stringent procedures. Federal, state and local government employees who do not follow these safeguarding procedures may be subject to disciplinary action including criminal and civil penalties and loss of employment. State laws governing theft, conspiracy, and trade secrets may apply to government employees and contractors who intentionally mishandle PCII. The CII Act does not limit any enforcement mechanism.

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

ICS-CERT Assessment Activity for May/June 2017

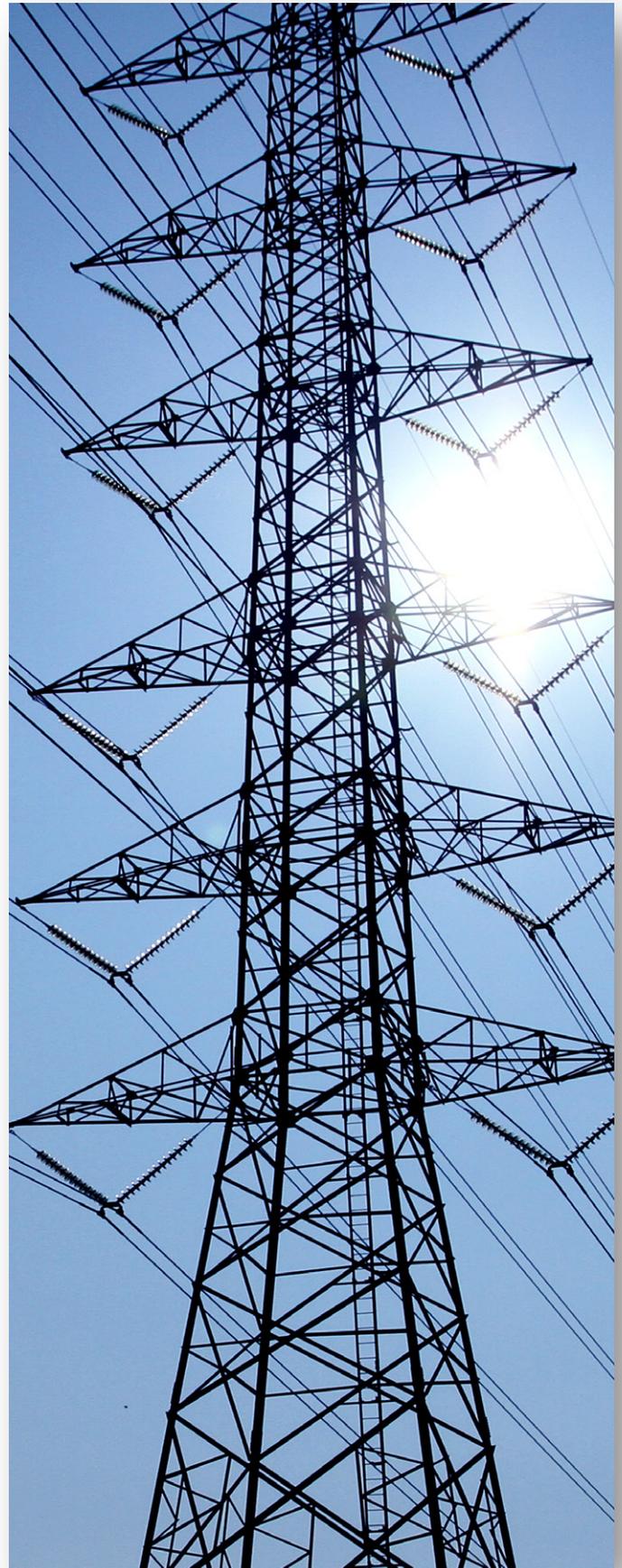
ICS-CERT conducts onsite cybersecurity assessments of industrial control systems (ICSs) to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In May/June 2017, ICS-CERT conducted 34 onsite assessments across 5 sectors (Table 1). Of these 34 assessments, 11 were Cyber Security Evaluation Tool (CSET®) assessments, 13 were Design Architecture Review (DAR) assessments, and 10 were Network Architecture Verification and Validation (NAVV), (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 2017.

Assessments by Sector	May 2017	June 2017	May/June Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing	2		2
Dams		6	6
Defense Industrial Base			
Emergency Services	3		3
Energy		8	8
Financial Services			
Food and Agriculture			
Government Facilities			
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems	9	6	15
Monthly Totals	14	20	34 Total Assessments

Table 2: Assessments by type, May/June 2017.

Assessments by Type	May 2017	June 2017	May/June Totals
CSET™	6	5	11
DAR	5	8	13
NAVV	3	7	10
Monthly Totals	14	20	34 Total Assessments



Recent Product Releases

Alerts

[ICSA-ALERT-17-281-01](#) Petya Malware Variant, June 30, 2017

[ICSA-ALERT-17-135-01I](#) Indicators Associated With WannaCry Ransomware (Update I), June 13, 2017

Advisories

[ICSA-17-180-01](#) Siemens SIMATIC Industrial PCs, SINUMERIK Panel Control Unit, and SIMOTION P320, June 29, 2017

[ICSA-17-180-02](#) Schneider Electric U.motion Builder, June 29, 2017

[ICSA-17-180-03](#) Siemens Viewport for Web Office Portal, June 29, 2017

[ICSA-17-178-01](#) Newport XPS-Cx, XPS-Qx, June 27, 2017

[ICSA-17-173-01](#) Siemens SIMATIC CP 44x-1 Redundant Network Access Modules, June 22, 2017

[ICSA-17-173-02](#) Siemens XHQ, June 22, 2017

[ICSA-17-171-01](#) Ecava IntegraXor, June 20, 2017

[ICSA-17-129-01B](#) Siemens devices using the PROFINET Discovery and Configuration Protocol (Update B), June 20, 2017

[ICSA-17-129-02A](#) Siemens devices using the PROFINET Discovery and Configuration Protocol (Update A), June 15, 2017

[ICSA-17-166-01](#) Cambium Networks ePMP, June 14, 2017

[ICSA-17-164-01](#) Trihedral VTScada, June 13, 2017

[ICSA-17-164-02](#) OSIsoft PI Server 2017, June 13, 2017

[ICSA-17-164-03](#) OSIsoft PI Web API 2017, June 13, 2017

[ICSA-17-157-01](#) Rockwell Automation PanelView Plus 6 700-1500, June 6, 2017

[ICSA-17-157-02](#) Digital Canal Structural Wind Analysis, June 6, 2017

[ICSA-17-152-01](#) Phoenix Broadband Technologies LLC PowerAgent SC3 Site Controller, June 1, 2017

[ICSA-17-143-01](#) Moxa OnCell, May 23, 2017

[ICSA-17-115-04](#) Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400, May 23, 2017

[ICSM-17-082-02](#) B. Braun Medical SpaceCom Open Redirect Vulnerability, May 23, 2017

[ICSA-17-138-01](#) Miele Professional PG 85 Series, May 18, 2017

[ICSA-17-138-02](#) Schneider Electric Wonderware InduSoft Web Studio, May 18, 2017

[ICSA-17-117-01A](#) GE Multilin SR, UR, and URplus Protective Relays (Update A), May 18, 2017

[ICSA-17-136-01](#) Detcon SiteWatch Gateway, May 16, 2017

[ICSA-17-136-02](#) Schneider Electric SoMachine HVAC, May 16, 2017

[ICSA-17-136-03](#) Hanwha Techwin SRN-4000, May 16, 2017

[ICSA-17-136-04](#) Schneider Electric VAMPSET, May 16, 2017

[ICSA-17-131-01](#) Phoenix Contact GmbH mGuard, May 11, 2017

[ICSA-17-131-02](#) Satel Iberia SenNet Data Logger and Electricity Meters, May 11, 2017

[ICSA-17-129-03](#) Siemens SIMATIC WinCC and SIMATIC WinCC Runtime Professional, May 9, 2017

[ICSA-17-094-04](#) Rockwell Automation Stratix 5900, May 9, 2017

[ICSA-17-124-01](#) Hikvision Cameras, May 4, 2017

[ICSA-17-124-02](#) Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras, May 4, 2017

[ICSA-17-124-03](#) Advantech WebAccess, May 4, 2017

[ICSA-17-094-05](#) Rockwell Automation ControlLogix 5580 and CompactLogix 5380, May 4, 2017

[ICSA-17-122-01](#) Schneider Electric Wonderware Historian Client, May 2, 2017

[ICSA-17-122-02](#) CyberVision Kaa IoT Platform, May 2, 2017

[ICSA-17-122-03](#) Advantech B+B SmartWorx MESR901, May 2, 2017



Open Source Situational Awareness Highlights

The State of SCADA HMI Vulnerabilities

<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities>

NIST Releases Draft SP 1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations for comment

<http://csrc.nist.gov/publications/PubsDrafts.html#SP-1800-8>

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 2017

ICS-CERT appreciates having worked with the following researchers:

- Maksim Malyutin from Embedi, ICSA-17-180-01 Siemens SIMATIC Industrial PCs, SINUMERIK Panel Control Unit, and SIMOTION P320, June 29, 2017
- rgod working with Trend Micro's Zero Day Initiative, ICSA-17-180-02 Schneider Electric U.motion Builder, June 29, 2017
- Hannes Trunde from Kapsch BusinessCom AG, ICSA-17-180-03 Siemens Viewport for Web Office Portal, June 29, 2017
- Maxim Rupp, ICSA-17-178-01 Newport XPS-Cx, XPS-Qx, June 27, 2017
- Tenable Network Security, ICSA-17-171-01 Ecava IntegraXor, June 20, 2017
- Karn Ganeshen, ICSA-17-166-01 Cambium Networks ePMP, June 14, 2017
- Karn Ganeshen, ICSA-17-164-01 Trihedral VTScada, June 13, 2017
- Karn Ganeshen, ICSA-17-157-02 Digital Canal Structural Wind Analysis, June 6, 2017
- Iñaki Rodríguez, ICSA-17-152-01 Phoenix Broadband Technologies LLC PowerAgent SC3 Site Controller, June 1, 2017
- Maxim Rupp, ICSA-17-143-01 Moxa OnCell, May 23, 2017



- Rockwell Automation, David Formby and Raheem Beyah of Georgia Tech and Fortiphed Logic, Inc., ICSA-17-115-04 Rockwell Automation Allen-Bradley MicroLogix 1100 and 1400, May 23, 2017
- Marc Ruef and Rocco Gagliardi of scip AG, ICSMA-17-082-02 B. Braun Medical SpaceCom Open Redirect Vulnerability, May 23, 2017
- Karn Ganeshen, ICSA-17-138-02 Schneider Electric Wonderware Industrial Soft Web Studio, May 18, 2017
- Maxim Rupp, ICSA-17-136-01 Detcon SiteWatch Gateway, May 16, 2017
- Zhou YU, ICSA-17-136-02 Schneider Electric SoMachine HVAC, May 16, 2017
- Can Demirel and Faruk Unal of Biznet Bilisim, ICSA-17-136-03 Hanwha Techwin SRN-4000, May 16, 2017
- Kushal Arvind Shah from Fortinet's Fortiguard Labs, ICSA-17-136-04 Schneider Electric VAMPSET, May 16, 2017
- Karn Ganeshen, ICSA-17-131-02 Satel Iberia SenNet Data Logger and Electricity Meters, May 11, 2017
- IPcamtalk user "Montecrypto", ICSA-17-124-01 Hikvision Cameras, May 4, 2017
- Zhou Yu working with Trend Micro's Zero Day Initiative, ICSA-17-124-03 Advantech WebAccess, May 4, 2017
- Andrey Zhukov from USSC, ICSA-17-122-01 Schneider Electric Wonderware Historian Client, May 2, 2017
- Jacob Baines from Tenable Network Security, ICSA-17-122-02 CyberVision Kaa IoT Platform, May 2, 2017
- Maxim Rupp, ICSA-17-122-03 Advantech B+B SmartWorx MESR901, May 2, 2017



Follow ICS-CERT on Twitter: [@icscert](https://twitter.com/icscert)

Upcoming Events

September 2017

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

September 18–22

Idaho Falls, Idaho

Canceled

October 2017

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

October 16–20 (Tentative)

Idaho Falls, Idaho

[Course description](#); Registration will be posted
July 24-28.

NOTE: There will be no training July. The August session is not open to the public for registration.

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>.