NCCIC

ICS-CERT MONITOR

Contents

ICS-CERT News

Situational Awareness

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 any questions related to this report, please contact NCCIC Customer Service at:

U.S. Toll Free: (888) 282-0870

Email: nccicustomerservice@hq.dhs.gov

Report an ICS incident to ICS-CERT

Report an ICS software vulnerability

Get information about reporting

Granicus

ICS-CERT launched a new digital subscription system with Granicus to help you stay informed. By signing up for Granicus, 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 News

NCCIC Realignment

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and cyber risk management center that is a national nexus of cyber and communications cyber risk management integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among public and private sector partners to build awareness of cyber and communications vulnerabilities, threats, incidents, impacts, and mitigations. The NCCIC mission is to reduce the likelihood and severity of incidents and vulnerabilities that may significantly compromise the security and resilience of the Nation's critical infrastructure (CI) information technology and communications networks in both the public and private sector.

Recently, the NCCIC went through an organizational realignment to consolidate and enhance the effectiveness of its mission-essential functions, which includes changes to the structures of the ICS-CERT, NCC, and US-CERT divisions. This realignment has no impact to the technical expertise and services our stakeholders rely on us to provide, but there will be changes to divisional products, such as the ICS-CERT Year in Review and ICS-CERT Monitor. Instead, the NCCIC will be broadening those products to encompass all programs in the new NCCIC Year in Review and the NCCIC Monitor, which will still contain information that will be beneficial to CI owners and operators. This approach will benefit our stakeholders so that they have a stronger understanding of the NCCIC organization, as well as the breadth of its services and products that they can leverage for their individual cybersecurity needs.

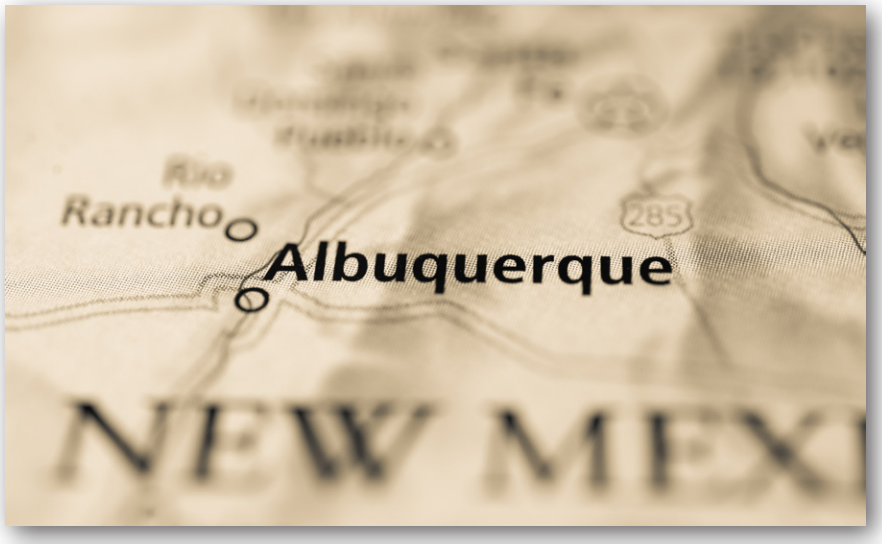
The NCCIC Year in Review and NCCIC Monitor will be available via the ICS-CERT website. The NCCIC partners with Granicus (GovDelivery) to provide a digital subscription system to help users stay informed. By signing up for Granicus, users can receive the NCCIC Year in Review, NCCIC Monitor, ICS-CERT Alerts, ICS-CERT Advisories and ICS-CERT Announcements product release notices directly to their email Inbox. Granicus subscriptions are available to anyone, worldwide. Learn more, and sign up for Granicus at: Granicus New Subscription. The Granicus sign-up page allows users to set up their account with their email address or favorite social media account (Facebook, Google, or Yahoo).

ICSJWG 2018 Spring Meeting Announcement

The 2018 Spring Industrial Control Systems Joint Working Group (ICSJWG) Meeting will occur April 10–12, 2018, in Albuquerque, New Mexico. The ICSJWG team looks forward to a broad and diverse group of stakeholders to be in attendance for further engagement on issues central to the evolving industrial control systems (ICS) cybersecurity field, as the program builds off of the success of the 2017 Fall Meeting held in Pittsburgh, Pennsylvania. Keynote speeches, varied presentations, intimate breakout sessions and panels, a hands-on workshop, fluid interactions with vendor booths, concrete networking opportunities, and more will enrich the Spring Meeting, which will ensure that attendees are able to confidently walk away with actionable information for their everyday role in ICS cybersecurity.

Further information for the upcoming Meeting is available, and will continue to develop, on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. In the meantime, if you have any questions, feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

On the web site, you will soon find detailed logistical, background, and preparatory information on various components of the Meeting, including the Call for Abstracts. We encourage interested speakers to ultimately submit abstracts for consideration, which will be due by February 23, 2018, and reviewed by ICSJWG Program Management and the ICSJWG Steering Team. Please review the Call for Abstracts, upon its forthcoming release, for full details on abstract submission.



ICSJWG Webinar Preview: "Life after Ukraine"

Following the well-received success of the October 2017 ICSJWG Webinar, "Creating Predictable Fail Safe Conditions for Healthcare Facility-Related Control Systems and Medical Devices by Use of System Segmentation," presented by Michael Schroeder, Director of Programs at 3 Territory Solutions, LLC, the ICSJWG team is excited to announce the next Webinar in its ongoing series: "Life After Ukraine: Industrial Control System Cybersecurity Industry Trends and Strategies."

Brian Proctor (GICSP, CISSP, CRISC) of SecurityMatters will present this much-anticipated session, on January 24, 2018, commencing at 2:00 pm (EST).

Slated to draw a significant number of attendees, "Life After Ukraine" will discuss the plans and actions that industrial asset owners, globally, are putting in place and implementing following various cyber-attacks that Ukraine has incurred, including maturing operational technology (OT) security beyond mere compliance or industry baselines.

If you are interested in participating in future webinars, please contact ICSJWG.Communications@hq.dhs.gov. The next Webinar is tentatively planned for March 2018. Generally, if you have a topic you would like to share with the ICSJWG community, please consider presenting an ICSJWG-hosted Webinar. For more information, please reach out to the same email address above.

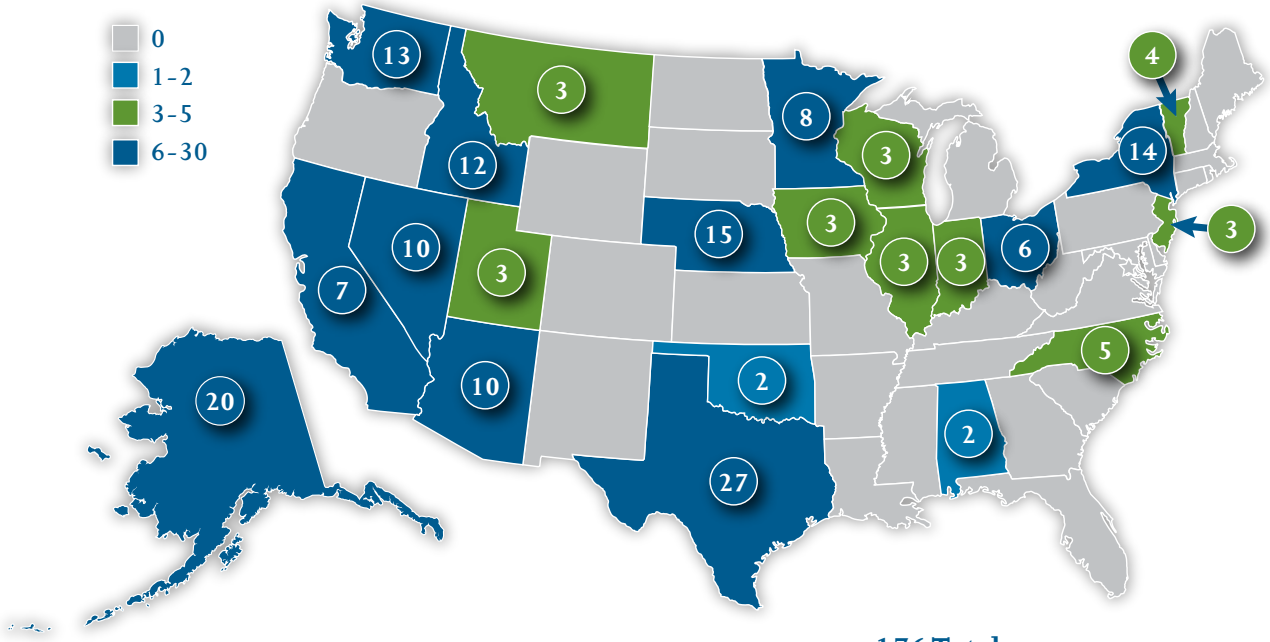
Fiscal Year 2017 ICS Assessment Summary

In Fiscal Year 2017, ICS-CERT conducted 176 assessments, a 35 percent increase from Fiscal Year 2016, including

- 39 high-level security posture evaluations utilizing the Cyber Security Evaluation Tool (CSET®),
- 74 ICS architecture design reviews, and
- 63 network traffic analyses.

ICS-CERT conducted assessments across eight of the 16 CI sectors. These included Energy, Water and Wastewater Systems, Dams, Commercial Facilities, Government Facilities, Critical Manufacturing, Transportation Systems, and Food and Agriculture. The Energy and Water and Wastewater Systems sectors together represented 69 percent of all assessments. ICS-CERT performs these voluntary assessments at the request of the asset owner. As a result, year-to-year fluctuations in assessments for a given CI sector are generally demand driven (based on customer requests).

FY 2017 Assessments by State



176 Total Assessments for FY 2017

Fiscal Year 2017 ICS Assessment Summary *(continued)*

Overarching Discoveries

The ICS-CERT assessment teams identified 753 discoveries through its 137 architecture design reviews and network traffic analyses. The assessment methodology categorizes weakness based on the National Institute of Standards and Technology's (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," control family sub-categories. While the assessment teams identified weakness across all control families, six categories represented roughly 33 percent of the total vulnerabilities discovered across assessed CI sectors.

FY 2014-2017 Top Six Weakness Categories in Order of Prevalence

FY 2014	FY 2015	FY 2016	FY 2017
1. Boundary Protection	1. Boundary Protection	1. Boundary Protection	1. Boundary Protection
2. Access Control Policy and Procedures	2. Least Functionality	2. Least Functionality	2. Identification and Authentication (Organizational Users)
3. Least Privilege	3. Authenticator Management	3. Identification and Authentication (Organizational Users)	3. Allocation of Resources
4. Remote Access	4. Identification and Authentication (Organizational Users)	4. Physical Access Control	4. Physical Access Control
5. Physical Access Control	5. Allocation of Resources	5. Audit Review, Analysis, and Reporting	5. Account Management
6. Information System Monitoring	6. Least Privilege	6. Authenticator Management	6. Least Functionality

Table 1: FY2014–FY2017 Top Six Weaknesses.

FY 2017 Most Prevalent Weaknesses

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Allocation of Resources	3	• No backup or alternate personnel to fill position if primary is unable to work • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to: ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

Table 2: Risks Associated with FY2017 Most Prevelent Weaknesses.

The ICS-CERT assessment team focuses on cybersecurity defenses that can prevent malicious attacks. Discoveries within assessment reports focus on the greatest potential for impact and the largest gain when mitigated. The best defense in control system security is having a solid network architecture that isolates sensitive control systems from inherently risky enterprise networks. Thus, it was no surprise that the primary discovery in Fiscal Year 2017, as in previous years, were flaws in network architecture boundaries.

A growing concern identified in many assessments this year is the use of shared and group accounts. These make it difficult to identify the actual user and they allow malicious parties to use them with anonymity. Accounts used by a shared group of users typically have poor passwords that malicious actors can easily guess and that users do not change frequently or when a member of the group leaves.

Another growing trend observed in many assessments concerns the resources allocated to provide cybersecurity to control systems. Many sites assessed this year were short staffed, and many had positions with no backup personnel. Although some sites had started planning for attrition of staff, many did not have a plan to address loss of key personnel. One site had seven key personnel, four of whomh would be eligible for retirement next year.

Maintaining visibility in the top discoveries this year were problems related to physical access. While this is not something the ICS-CERT focuses on during assessments, the team often sees this issue during assessments. ICS components and infrastructure should only be accessible to authorized personnel as necessary to maintain the system. The team observed cases where infrastructure (i.e., routers and switches) was in company space but accessible to staff with no need to have physical access. Other cases included ICS components in public areas without any physical restrictions (i.e., locked doors or enclosures) to prevent access from a passerby. Some sites did not have locked doors to the operations plant, which would allow anyone to walk in and potentially have access to control system components.

Overall, the ICS-CERT assessment team is still seeing many of the same vulnerabilities as in previous years, with the largest areas of concern still being the protection of the sensitive control system environment. Concerns of the attrition of skilled staff and the use of shared accounts are a growing trend. While the main issues observed this year seem largely the same, the assessment team has noted increasing attention from asset owners to control system security.

For additional recommended practices and guidance for developing mitigation strategies for specific cyber threats, please reference ICS-CERT's "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies."

Fiscal Year 2017 Workforce Development and Training Statistics

On-line Training Courses

Number of professionals who completed online training courses: 19,956

Instructor Led 301 (Red/Blue) Training Courses

Number of courses: 12

Total number of attendees: 492

Instructor Led Regional Training Courses

Number of regional events: 4

Number of 101 class attendees: 274

Number of 201 class attendees: 322

Number of 202 class attendees: 307

Total number of attendees: 903

Fiscal Year 2017 Vulnerability Summary

The NCCIC Industrial Control Systems Vulnerability Management and Coordination team has had a year of continued growth and change. Outside of the typical control system vulnerabilities disclosed, the vulnerability team has seen an increase of non-traditional "at risk" devices that play a key part of the Nation's CI. We have seen a significant increase in work done in the Healthcare and Public Health sector. After multiple botnet incidents resulting from insecure Internet of Things (IoT) technology, we saw an increase in disclosure of these types of devices. We have also recently been coordinating disclosures resulting from the Key Reinstallation Attack (KRACK). The vulnerabilities from these devices reflect how risks to any network must be continuously monitored and managed as they become more diverse.

As cybersecurity has continued to mature within the Healthcare and Public Health Sector, we have seen an increase of vulnerabilities published, by 400 percent over the previous year. In addition to researchers, we are seeing the medical device manufacturers taking an active role in responsibly disclosing vulnerabilities and providing mitigation strategies in a timely manner. These continued efforts by manufacturers will create better quality product with more resilience and security. If this behavior continues, it will lead to a more resilient medical sector overall.

With the plethora of IoT devices flooding the markets and networks, it is not a surprise that we have seen additional disclosures and advisories involving these devices. This came sharply into focus with the spread of the Brickerbot, Mirai, and Hajime. These threats exploited default or hard-coded passwords in order bring IoT devices into malicious states. These threats are not typical of an OT network, but the vulnerabilities are common among aging ICS infrastructure. These at-risk devices can become pivot points for threat actors and have the potential to impact operational environments.

The disclosure of the KRACK vulnerability introduced a new risk of man-in-the-middle attacks in the OT environment. While many vendors want to discount the risk as a third-party issue, the fact remains that the finding still exists in the many customer's operational environments. For networks that leverage Wi-Fi capabilities, it is typically challenging to completely control wireless emanations in the way traditional wired networks are managed. Asset owners should make sure to do their due diligence to implement the mitigations strategies associated with the affected products. This vulnerability is another example of IT risk crossing over to the OT network.

The risks to the OT network are ever expanding, and asset owners should continue to be aggressive in their efforts to secure their OT environments. Threat actorss continue to seek ways to bridge boundaries between the IT/IoT/OT environments. The responsibility cannot lie solely on the asset owner to secure their environments. Asset owners should be turning to their vendors with requirements and expectations of products that are not only secure but have the functionality to be secured. The responsibility will always be on asset owners to build secure environments, but the vendor has responsibility to communicate risk to their customers in a timely and transparent manner.

ICS-CERT Assessment Activity for November/December 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 November/December 2017, ICS-CERT conducted 22 onsite assessments across three sectors (Table 1). Of these 22 assessments, five were CSET assessments, nine were Design Architecture Review (DAR) assessments, and eight were Network Architecture Verification and Validation (NAVV) assessments (Table 2).

Table 1: Assessments by sector, November/December 2017.

Assessments by Sector	November 2017	December 2017	November/ December Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing			
Dams			
Defense Industrial Base			
Emergency Services			
Energy	7	6	13
Financial Services			
Food and Agriculture			
Government Facilities		3	3
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems	3	3	6
Water and Wastewater Systems			
Monthly Totals	10	12	22 Total Assessments

Table 2. Assessments by type, November/December 2017.

Assessments by Type	November 2017	December 2017	November/ December Totals
CSET ™	2	3	5
DAR	4	5	9
NAVV	4	4	8
Monthly Totals	10	12	22 Total Assessments

Recent Product Releases

Alerts

ICS-ALERT-17-341-01 WAGO PFC200, December 7, 2017

Advisories

ICSA-17-355-01 Moxa NPort W2150A and W2250A, December 21, 2017

ICSA-17-355-02 Schneider Electric Pelco VideoXpert Enterprise, December 21, 2017

ICSA-17-353-01 ABB Ellipse, December 19, 2017

ICSA-17-353-02 PEPPERL+FUCHS/ecom instruments WLAN Capable Devices using the WPA2 Protocol, December 19, 2017

ICSA-17-353-03 Ecava IntegraXor, December 19, 2017

ICSA-17-353-04 Siemens LOGO! Soft Comfort, December 19, 2017

ICSA-17-353-05 WECON Technology Co., Ltd. LeviStudio HMI, December 19, 2017

ICSA-17-339-01A Siemens Industrial Products (Update A), December 19, 2017

ICSA-17-318-01B Siemens SCALANCE, SIMATIC, RUGGEDCOM, and SINAMICS Products (Update B), December 19, 2017

ICSA-17-341-01 Xiongmai Technology IP Cameras and DVRs, December 7, 2017

ICSA-17-341-02 Rockwell Automation FactoryTalk Alarms and Events, December 7, 2017

ICSA-17-341-03 PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH, December 7, 2017

ICSA-17-334-01 Siemens SWT3000, November 30, 2017

ICSA-17-334-02 Geovap Reliance SCADA, November 30, 2017

ICSA-17-332-01 Siemens SCALANCE W1750D, M800, and S615, November 28, 2017

ICSMA-17-332-01 Ethicon Endo-Surgery Generator G11 Vulnerability, November 28, 2017

ICSA-17-325-01 PHOENIX CONTACT WLAN Capable Devices using the WPA2 Protocol, November 21, 2017

ICSA-17-320-01 Moxa NPort 5110, 5130, and 5150, November 16, 2017

ICSA-17-320-02 Siemens SICAM, November 16, 2017

ICSA-17-318-02 ABB TropOS, November 14, 2017

ICSMA-17-318-01 Philips IntelliSpace Cardiovascular System and Xcelera System Vulnerability, November 14, 2017

ICSA-17-313-01 AutomationDirect CLICK, C-More, C-More Micro, GS Drives, and SL-Soft SOLO, November 9, 2017

ICSA-17-313-02 Schneider Electric InduSoft Web Studio and InTouch Machine Edition, November 9, 2017

ICSA-17-306-01 Siemens SIMATIC PCS 7, November 2, 2017

ICSA-17-306-02 Advantech WebAccess, November 2, 2017

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 ncciccustomerservice@hq.dhs.gov or toll free at 1-888-282-0870.

Researchers Assisting ICS-CERT with Products Published November/December 2017

ICS-CERT appreciates having worked with the following researchers:

- Federico Maggi, ICSA-17-355-01 Moxa NPort W2150A and W2250A, December 21, 2017
- Steven Seeley of Source Incite, and Michael DePlante and Brad Taylor working with Zero Day Initiative, ICSA-17-353-03 Ecava IntegraXor, December 19, 2017
- Michael DePlante, working with Trend Micro's Zero Day Initiative, ICSA-17-353-05 WECON Technology Co., Ltd. LeviStudio HMI, December 19, 2017
- Independent researcher Clinton Mielke, ICSA-17-341-01 Xiongmai Technology IP Cameras and DVRs, December 7, 2017
- Maxim Rupp, ICSA-17-341-03 PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH, December 7, 2017
- Can Demirel of Biznet Bilisim, ICSA-17-334-02 Geovap Reliance SCADA, November 30, 2017
- Florian Adamsky, ICSA-17-320-01 Moxa NPort 5110, 5130, and 5150, November 16, 2017
- Mark Cross of RIoT Solutions, ICSA-17-313-01 AutomationDirect CLICK, C-More, C-More Micro, GS Drives, and SL-Soft SOLO, November 9, 2017
- Steven Seeley, working with Zero Day Initiative, ICSA-17-306-02 Advantech WebAccess, November 2, 2017

Upcoming Events

March 2018

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

March 19–23, 2018

Idaho Falls, Idaho

Course information and registration

April 2018

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

April 16–20, 2018

Idaho Falls, Idaho

Course description. Registration will be available approximately 90 days prior to the start date.

April/May 2018

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

April 30–May 4, 2018

Idaho Falls, Idaho

Course description. Registration will be available approximately 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: ncciccustomerservice@hq.dhs.gov.

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 ncciccustomerservice@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.