

Upcoming Events

- October 17-21:
Industrial Control
Systems Cybersecurity
(301) Training
Idaho Falls, ID
- November 14-18:
Industrial Control
Systems Cybersecurity
(301) Training
Idaho Falls, ID
- December 12-16:
Industrial Control
Systems Cybersecurity
(301) Training
Idaho Falls, ID

ICS-CERT Resources

[Training Resources](#)
[Incident Reporting](#)
[Assessments](#)
[CSET](#)
[Alerts & Advisories](#)
[HSIN](#)
[Latest Monitor](#)

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on members like you for our Newsletter, Meetings, and Webinars. Content and opinions are those of the authors and do not represent DHS opinions, endorsements, or recommendations.

Fall 2016 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) 2016 Fall Meeting was held in Ft. Lauderdale, FL, on September 13-15, 2016. This Meeting brought together over 280 stakeholders from the ICS community. Over the course of 3 days, attendees had the opportunity to attend numerous seminars and interact with the community through demonstrations, presentations, panels, and lightning round talks.

This meeting featured a keynote presentation from Billy Rios, founder of WhiteScope, discussing the ease of access to voting machines and the impact of cybersecurity on American politics. Joel Langill of AECOM, and John Felker, DHS/NCCIC Director of Operations, and Marty Edwards, NCCIC/ICS-CERT Director also provided keynotes throughout the week. Additionally, this meeting provided a technical workshop and training focused on Network Monitoring of ICS and Google Hacking/Shodan, offering attendees at all technical levels the opportunity to be hands-on with these tools.

Throughout the week, there were presentations from members across the community representing a variety of perspectives. Each day featured interactive panel discussion and the meeting closed with an open Question and Answer session with Director Marty Edwards. We'd like to thank all who attended and presented for their contributions. The Spring 2017 Meeting will be announced soon so please look for an upcoming save-the-date announcement!

CSET® 8.0 Is Now Available

The latest iteration of CSET® is now available on the ICS-CERT website. The new CSET® paradigm supports an even easier walk-through process with each step clearly separated and easily delineated. CSET® 8.0 also has an advanced mode that will allow users to dive even deeper with support for the CCI's (control correlation identifiers), HIPAA, NIST SP800-171, and the Critical Security Controls Version 6.0. For the first time, the new version includes the ability to create unique question sets from existing standards. Users are able to mix and match questions from 30 different standards to generate subsets focused from individual components up to full assessments from multiple standards and organize the questions according to individual need.

ICS-CERT also recently hosted a webinar with a walk-through of CSET®, goals of the tool, and the latest features incorporated into the tool. Using CSET®, users can quickly determine their cybersecurity stance, priorities, and focus their limited cybersecurity time and budget on implementing controls and mitigating vulnerabilities. This webinar was recorded and will be made available to the ICSJWG community via the ICS-CERT website.

Implications of Presidential Policy Directive on Cyber Incident Coordination

On July 26th, President Obama issued Presidential Policy Directive (PPD) 41 concerning cyber incident coordination among federal agencies. This directive identifies the “principles governing the Federal Government’s response to any cyber incident, whether involving government or private sector entities.” PPD-41 further delineates between cyber incidents and significant cyber incidents, with a significant incident being “likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.” For more information regarding this PPD and how it impacts the work of the National Cybersecurity and Communications Integration Center (NCCIC) and ICS-CERT, please see the extended article in the July/August edition of the ICS-CERT Monitor, [available here](#).

Contributed Content Disclaimer: *The advice and instructions provided in the contributed content are provided as is, with no warranties, and should be confirmed and tested prior to implementation.*

New Workshop Looks at What to Do When Building Control Systems Get Hacked

A new workshop, sponsored by the National Institute of Building Sciences, answers the question of what to do when building control systems have been hacked or taken over by ransomware. Intended for building owners, facility managers, engineering, physical security, information assurance and other professionals involved with the design, deployment and operation of building control systems, the “[Your Building Control Systems Have Been Hacked, Now What? Workshop](#),” to be held **Tuesday, October 4, from 8:00 am to 5:00 pm**, in Arlington, Virginia, will provide a combination of classroom learning modules and hands-on laboratory exercises to help attendees learn how to detect, contain, eradicate and recover from a cyber event. [More information available here](#).

Cybersecuring Healthcare Building Control Systems

By: Michael Chipley

Healthcare facilities are some of the most complex structures ever built; yet, they are a system of systems that are notoriously easy to hack. As the use of the Internet of Things (IoT), cloud/mobile computing, medical devices and personal sensors continues to grow exponentially, cybersecuring this multitude of converged healthcare systems presents challenges that will require novel solutions, innovation and organizational culture change. [Full article available here](#).

Protecting Industrial Control Systems: An Integrated Approach

By: RKNEAL

Hackers have infiltrated credit card companies, retailers, health care providers and other consumer industries over the past several years. The hackers are utilizing the very technologies we all use to make life easier – Internet connectivity to bank accounts, health records, etc. – to gain access to our private information and financial accounts. As a result, innovative cyber security providers are constantly improving their defense technologies to keep up with the ever-changing threat landscape. Companies are also increasing their investments in these technologies to protect this critical information. [To continue reading click here](#).

The Perfect Storm Solving critical infrastructure challenges by evolving today's IP networks

By: Tempered Networks

Today, there is no question that our national infrastructure is under attack. Earlier this year, Richard H. Ledgett Jr., deputy director of the National Security Agency, concluded that “today, anyone with a computer and a fairly decent level of knowledge and an Internet connection can pose a very serious threat to an individual, a business, a city and a foreign nation” during a [keynote address](#) during a dinner at the Joint Service Academy Cyber Security Summit at the U.S. Military Academy in West Point, N.Y. [For full article click here.](#)

Deploying ICS Security in a Right Way

By: Daniel Ehrenreich, Consultant and Trainer, SCCE, Israel

I consider it a challenging task to identify and successfully deploy an absolutely innovative and never-seen-before ICS defense solutions. When searching for ICS experts you will meet engineers knowing PLC, RTU and HMI programming, but if you count the experienced ICS-Cyber experts and vendors of solutions you will find just few in each country. Cyber defense experts are either coming from elite army units dealing with cyber risks, top level universities, large financial institutions or government department responsible for data confidentiality. So who can professionally and honestly guide the pharma or food producers, water supply, power plant and refinery operators and other critical infrastructure related to deploying strong cyber security? [Article continues here.](#)

Contact ICS-CERT

Website: <http://ics-cert.us-cert.gov/>

Email: ics-cert@hq.dhs.gov or icsjwg@hq.dhs.gov

Phone: 1-877-776-7585

ICS-CERT publishes alerts and advisories to provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks and current security issues, vulnerabilities, and exploits. These notifications are available on the [ICS-CERT website](#) under [Information Products](#) or via [GovDelivery](#).

If you have a question regarding these products and what they mean for your organization, please contact ICS-CERT at ics-cert@hq.dhs.gov. If you have an ICS incident or software vulnerability to report, please go to [the ICS-CERT Website](#) and scroll to the bottom of the page to the “I Want To” selections. Additional online reporting information is available at <http://www.dhs.gov/report-cyber-risks> and at the bottom of the ICS-CERT Webpage. ICS-CERT will protect and anonymize your information and only share the technically relevant information with partners that have a need to know.