

Upcoming Events

- April 4-8:
Industrial Control
Systems Cybersecurity
(301) Training
Idaho Falls, ID
- May 3-5: ICSJWG 2016
Spring Meeting
Scottsdale, AZ
- May 9-13:
Industrial Control
Systems Cybersecurity
(301) Training
Idaho Falls, ID
- June 6-9:
Regional Training
Boston, MA

ICS- CERT Resources

[Training Resources](#)
[Incident Reporting](#)
[Assessments](#)
[CSET – New 7.1!](#)
[Alerts & Advisories](#)
[HISN](#)
[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.

Upcoming Spring Meeting

The date for the upcoming ICSJWG 2016 Spring Meeting is fast approaching! The Spring Meeting is being held at the Chaparral Suites (soon to be Embassy Suites – Scottsdale), in Scottsdale, AZ on May 3-5, 2016. This meeting will bring together public and private sector ICS cybersecurity experts from critical industries for three full days of presentations, demonstrations, and panels. The Spring Meeting will also include a Hands-On Forensics Technical Workshop, a Vendor Expo, and dedicated time for networking opportunities with industry peers. The following is a list of keynote speakers who have been confirmed for the Meeting:

- Gregory Touhill, Deputy Assistant Secretary for Cybersecurity and Communications, DHS
- Marty Edwards, Director of ICS-CERT, DHS
- Frank Grimmelmann, President & CEO of Arizona Cyber Threat Response Alliance
- Mark Fabro, President & Chief Security Scientist of Lofty Perch
- A Representative from the Arizona Federal Bureau of Investigation

So, take the time and register today at no cost for the upcoming ICSJWG 2016 Spring Meeting by using the following [link](#). Also for meeting attendees, the Chaparral Suites is offering rooms on a limited basis at the government per diem rate as well as numerous amenities. For reservations, use the following [booking link](#) to navigate to the ICSJWG group page at the Chaparral Suites or call 1-800-528-1456 and mention the Meeting. We look forward to seeing you in Scottsdale!

CSET 7.1 Released by ICS-CERT

ICS-CERT released the latest version of its Cyber Security Evaluation Tool (CSET), CSET 7.1, in February 2016. CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's cybersecurity posture. CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to analyze their ICS and IT network security practices using many recognized government and industry standards and recommendations. This update includes changes to NIST SP800-161, NERC CIP Compliance Risk Based Priority List, an enhanced dashboard, requirements organized according to standard, custom parameter values, and a doubled number of networks components.

ICS-CERT Announces Ukraine Action Campaign

The U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been actively working with the government of Ukraine and other U.S. Federal Government entities to understand the December 23, 2015 attacks against Ukrainian power infrastructure. ICS-CERT and the FBI will conduct unclassified in-person briefings, as well as online webinars, for asset owners and their supporting personnel, as well as Federal,

State, Local, Tribal and Territorial Government representatives to increase awareness of the threat and provide additional information. The briefing sessions will provide details about the events surrounding the attack, techniques used by the threat actors, and strategies for mitigating risks and improving the cyber defensive posture of an organization. Interested individuals may register for a session by visiting: <https://secure.inl.gov/ics-cert-briefing/?campaignName=Ukraine%20Cyber%20Attack>.

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.*

Meet the Intrusion Detection Systems: A Growing Family that is Protecting Critical Infrastructure

By: Anis Bishara, Application Engineer (U.S.), Gil Kroyzer, Founder & CEO Author, ICS2

Today's cybercriminals are more organized and more sophisticated than ever before. With every passing day, we are learning of new variants of cyber-attacks that are capable of bypassing traditional security defenses. According to published information, over 50% of such attacks target the Energy Sector, with the number and severity of attacks growing as they are financed by hostile countries, crime organizations or commercial entities. [For full article, click here.](#)

What's the Difference between Reliability and Resilience?

By: Aaron Clark-Ginsberg, Stanford University

The ability to keep the lights on in the event of a cyber-incident is a major concern for the electric sector. Power grid resilience and power grid reliability are both frequently, and often interchangeably, referenced in conversations about keeping the lights on. This begs the question: what is the difference between reliability and resilience? This brief describes the difference between reliability and resilience in relation to cyber-incidents and the power grid. [Full article available here.](#)

ICS/SCADA Cyber Security Requirements: A Practical Approach

By: Harsha Banavara, Schneider Electric USA Inc.

According to Gartner Research, by 2020 about 25 Billion "things" will be connected to the internet (Internet of Things - IoT). This is a five-time increase from the 4.9 Billion "things" that were connected in 2015 [1]. With (Industrial Internet of Things) IIoT, the problems have just worsened as the threat surface area has increased exponentially. We in the ICS world have only been focused on performance and ease of use and knowingly or unknowingly compromising security. [Click here for full article.](#)

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