

Upcoming Events

- January 11-15:
Industrial Control Systems Cybersecurity (301) Training
Idaho Falls, ID
- February 8-12:
Industrial Control Systems Cybersecurity (301) Training
Idaho Falls, ID
- February 22-25:
Regional Training (101, 201, 202)
Baton Rouge, LA
- March 7-11:
Industrial Control Systems Cybersecurity (301) Training
Idaho Falls, ID
- May 3-5: ICSJWG 2016 Spring Meeting
Scottsdale, AZ

[Registration information](#)

ICS-CERT Resources

[Training Resources](#)
[Incident Reporting](#)
[Assessments](#)
[CSET – New 7.0!](#)
[Alerts & Advisories](#)
[HISN](#)
[Latest Monitor](#)

Fall and Spring Meeting Update

The 2015 Fall Meeting was held in Savannah, Georgia and featured two and a half days of presentations, including comments from National Cybersecurity and Communications Integration Center (NCCIC) Director John Felker, Tino Mantella (Georgia Technology Association), Marina Krotofil (Independent Researcher), and Robert Lee (SANS). It also featured the first ever Vendor Expo and a demonstration of the ICS Village. We are excited to announce that the Spring meeting will take place in Scottsdale, Arizona on May 3-5, 2016 so please mark your calendars! More details will be released soon but if you have any questions, please contact [ICSJWG Communications](#).

Closing out Fiscal Year 2015 with ICS-CERT

This has been an exciting year for ICS-CERT and the NCCIC as a whole. ICS-CERT continues to grow, handling more incidents, vulnerabilities, and assessments than in year's prior and increasing activities in other areas as well. Additionally, cybersecurity has been recognized as a priority at the highest levels of the U.S. Government. For more information about the year gone by, please see the latest edition of the Monitor or our soon-to-be-published Year in Review for 2015.

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. If you are unable to access the full articles please contact ICSJWG Communications.*

The Value of Bi-directional Countermeasures

By: Joseph J. Januszewski, III, CISSP, North American Electric Reliability Corporation

A recent informal survey conducted by the author using various power sector technical publications and security journals revealed a serious problem that is occurring in border defenses: data exfiltration. This problem is occurring in various sectors. Several DHS ICS-CERT advisories have been written to advise the critical infrastructure community to protect specific resources. A common thread in complaints seen in the cyber community relate to how firewalls can fail an organization. The problem may not be the firewall, necessarily, but the configuration of the security policy. This is not to say that firewall products have not, overall, retained a currency and a relevance in light of a changing threat environment, based upon recent (and some not-so-recent attacks.) These attacks are leading many to declare the network firewall “dead” as a defensive tool. The author posits that in his experience, the under-utilization of creative and stringent policies and inadequate security architectures contribute to the ease with which attackers can successfully breach defenses. [To read the full article, please click here.](#)

Cybersecuring Building Control Systems

By: Michael Chipley, PhD, GICSP, PMP, LEED AP

Building control systems with embedded communications technology—as well as those enabled via an Internet

Protocol (IP) address—provide critical services that allow a building to meet the functional and operational needs of building occupants. Unfortunately, they also can be easy targets for hackers and people with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities; use as an entry point to traditional information technology (IT) systems and data; cause physical destruction of building equipment; and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event. Cyber attacks, such as the Target and Home Depot data hacks, have directed increased attention to the network connectivity of facility/building operations and maintenance vendors, an organization’s business IT systems and facility/building control systems. [Full Article Here](#)

This article was first written for and published in the October 2015 issue of the *Journal of the National Institute of Building Sciences* (JNIBS), a publication of the Washington, D.C.-based National Institute of Building Sciences. It has been reproduced here with permission from the Institute. Learn more about JNIBS at <http://www.nibs.org/?page=journals>, and receive free issue(s) by subscribing at http://www.wbdg.org/account/subscribe_jnibs.php.

Five Cyber Security Best Practices to Mitigate Remote Access Vulnerabilities

By: Alex Leemon, CyberArk

Recently, I attended several ICS Security and energy sector events. This year’s topics revolved around meeting key regulations such as NERC CIP v5 and sharing best practices, lessons learned and emerging security trends. One key point stood out [as the sophistication and number of cyber-attacks on critical infrastructure](#) increases: it’s more important than ever to understand the landscape of entry points into your OT networks and industrial control systems. The increased connectivity between IT and OT effectively extends this landscape of entry points to include business users and applications accessing critical assets as well as outside vendors accessing your systems remotely. [To continue reading please click here](#)

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

By: Anis Bishara, Application Engineer (U.S), and Gil Kroyzer, Founder & CEO, 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. [Full article available here](#)

NIST Seeks Comments on Cybersecurity Framework Use, Potential Updates and Future Management

The National Institute of Standards and Technology (NIST) is seeking information on how its voluntary [“Framework for Improving Critical Infrastructure Cybersecurity”](#) is being used, as well as feedback on possible changes to the Framework and its future management. A preview copy of the [Request for Information](#) was posted to the *Federal Register*. The comment period closes Feb. 9, 2016. [More 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

Online reporting information, as well as ICS-CERT Alerts and Advisories, may be found on the ICS-CERT webpage.

Thank you to everyone who submitted content for this newsletter. ICSJWG relies on its 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.