December 2016

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- January 9-13: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, ID
- January 23-27: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, ID
- February 6-10: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, ID
- March 13-17*: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, ID

*Tentative

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.

ICSJWG Webinar Series

In the 2016 Fall Meeting Survey, many attendees expressed an interest in participating in a webinar, either as a presenter or as a participant. The ICSJWG Webinar Series is designed to inform the membership and general public about solutions to threats, vulnerabilities, and risks to critical infrastructure and control systems. If you have a topic you would like to share with the ICSJWG community, please consider an ICSJWG-hosted webinar. For more information, please contact ICSJWG.Communications@hq.dhs.gov.

2017 Spring Meeting Update

ICS-CERT and the ICSJWG are in the final stages of finalizing the venue for the ICSJWG 2017 Spring Meeting April 11-13, 2017, in Minneapolis, Minnesota! In the coming weeks, we will open the Call for Abstract and encourage all members of the community to submit an abstract. At that time, registration will also be open and additional details will be provided at the ICSJWG web page. We hope you all save the date and join us in Minneapolis!

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

Control is not Data

By: Andrew Ginter

IT gurus tell us that control system security is essentially the same as IT security, and that both are about "protecting the data." The gurus tell us that, yes, there are two kinds of "data" in control systems - monitoring data and control data - but "data is data." They tell us that all we need to do is protect the CIA, or AIC, or IAC, or something, of the data and we're done - we're secure. They are wrong. Full article available here.

Is "IoT" is a Debatable Term for Great Solutions?

By: Daniel Ehrenreich

The Internet of Things (IoT) was probably created as a combination of terms "IT", "OT" and "Internet" by Kevin Ashton while working for P&G in 1999. I believe, that the rational was to offer a term which will become an "umbrella" for connecting to a network smart industrial sensors, light controllers, CCTV cameras, home appliances, etc. using the IP data communication. Click here to read full article.

Security Focused Converged IdAM Platform

By: Howard Page

Recently the National Cybersecurity Center of Excellence (NCCoE) developed a platform designed to provide a secure network infrastructure for Identity and Access management systems. While the use case was designed for the Department of Energy, it is applicable to many control systems. NCCoE partnered with industry to pull together off-the-shelf components that can be assembled to improve the security posture. To continue reading click here.

Design Guidance for Cybersecurity of Facility-Related Control Systems

By: Michael Chipley, Daryl Haegley, and Eric J. Nickel

In September 2016, the Department of Defense published a much-anticipated new **Unified Facility Criteria, UFC 4-010-06 Cybersecurity Of Facility-Related Control Systems**. The UFC is the first cybersecurity design guidance written specifically for the architect, engineer, systems integrator and operators that plan, construct and operate the diverse number of DoD control systems. The UFC outlines the design sequence to follow the Risk Management Framework (RMF) and is one key milestone within the broader Cyber Security Efforts underway within the Office of Secretary of Defense, Energy, Installations and Environment (OSD EI&E) office. More information available here.

Your Building Control Systems Have Been Hacked. Now What?

By: Michael Chipley, Daryl Haegley, and Eric J. Nickel

Building owners and managers, facility engineers, and physical-security specialists, be warned: Building control systems (BCS) are now squarely in the sights of nation-state and criminal hackers. With the increased likelihood of BCS being attacked/exploited, U.S. Cyber Command (USCYBERCOM) developed the document "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)." (Note: The use of the word "industrial" can be misleading; the ACI TTP can be applied to any control system.) This article discusses use of the ACI TTP for detecting, responding to, and recovering from a cyber attack. For full article click here.

Contact ICS-CERT

Website: https://ics-cert.us-cert.gov/
Phone: 1-877-776-7585

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

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 web site 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 https://ics-cert.us-cert.gov and scroll to the bottom of the page to the "I Want To" selections. ICS-CERT will protect and anonymize your information and only share the technically relevant information with partners that have a need to know.