March 2017

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

—ICSJWG EXPANDING THE COMMUNITY—

Upcoming Events

- April 3–7:
  Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, ID
- April 11–13:
  ICSJWG 2017 Spring Meeting
  Minneapolis, MN
- May 1–5:
  Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, ID
- June 5–9:
  Industrial Control Systems Cybersecurity (301) Training
  Idaho Falls, ID
- June 19–23:
  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.

Upcoming ICSJWG 2017 Spring Meeting

The ICSJWG 2017 Spring Meeting will occur in just a few short weeks! The meeting will take place April 11 - 13, 2017, at the Loews Minneapolis Hotel in Minneapolis, Minnesota. The meeting will bring together public and private sector ICS cybersecurity experts from across industry for three days of presentations, demonstrations, and panels. The full agenda is available at https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. This meeting will feature keynote speeches by Marty Edwards, Director of ICS-CERT, and Ben Miller, Director of the Threat Operations Center, Dragos, Inc. In addition, this meeting will include the return of the Vendor Expo and "Ask Me Anything" sessions. We hope you will join us in Minneapolis!

To register, click here or go to https://secure.inl.gov/ics-cert-briefing/?campaignName=ICSJWG%20Spring%202017.

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.***

Building cyber-resilience of interconnected critical infrastructures: what is the role of public utility commissions?

By: Aaron Clark-Ginsberg, Rebecca Slayton, Noah Dormady, Ryan Ellis

Information technologies (IT) and communication networks permeate other critical infrastructures; transportation, electric power, natural gas, and water, and other sectors rely on complex IT and communications networks for their day-to-day operation. This reliance creates novel cross-sector interdependencies, cyber-vulnerabilities, and possibilities for disruption and catastrophic failure. For instance, the August 14th 2003 Northeast blackout occurred when a software bug caused an alarm system to fail. This IT failure prevented utilities from responding properly when a transmission line hit a tree branch, and the resulting cascading outage left 55 million people in Canada and the United States without power and shut down transport, communication, health, and water systems. Click here to read full article.

Selecting Very Strong OT Cyber Defense

By: Moti Barkan, HackNot, USA and Daniel Ehrenreich, SCCE, Israel

Operation of large Industrial Control systems (ICS), such as power plants and manufacturing operations, water desalination and distribution, nuclear and chemical facilities is among targets for severe cyber-attacks by hostile organizations, such as we often hear about. Among many reasons, this action can be possible due to known facts caused by use of legacy type DCS which manage the operation critical industrial facilities. The legacy type sensors and actuators deployed for control and monitoring systems for vibration, temperature and heat flow, etc. were built for operational performance and reliability and safety but a whole range of cyber security indications which may point on a problem and integrated cyber defense measures and risk mitigation solutions were not specified as a requirement. To continue reading click here.

Cyber Resilience Metrics for Bulk Power Systems

By: Sachin Shetty (Old Dominion University), Bheshaj Krishnappa (ReliabilityFirst) and David Nicol (University of Illinois)

The North American Bulk Power System is a complex technological network, and its cyberphysical interconnectivity allows for long-distance power transmission but presents a "surface" for cyber-attacks. The BPS is comprised of substations, control centers, energy management systems, multiple communication technologies, supervisory control, etc. The critical operation of BPS is to provide monitoring, protection and control based on information gathered from field units and decision making and control at multiple control centers. The components in the BPS that are vulnerable to cyber-attacks include, substations, control centers, communication links and networks. The cyber-attacks can manifest as, spear phishing, denial of service, man-in-the middle, timing, replay, integrity. There is a need to develop cyber resilience metrics for BPS to provide quantitative insights into ability of security controls to ensure operational resilience and development of cost-effective mitigation plan. More information available here.

MESA International is Helping to Address Industrial Cybersecurity

By: Eric C. Cosman, MESA Cybersecurity work group co-chair, Principal Consultant, OIT Concepts, LLC

The challenges associated with ensuring the security of industrial control systems (ICS) are complex, and have been with industry for years. The situation is improving through a combination of increasing awareness, improved risk assessment methods, more mitigation tools and improved technology. Nonetheless, there is still much to be done. Addressing the challenges and improving the situation requires contributions from a wide range of contributors and stakeholders, working at each stage of the solution life cycle. Full article here.

Contact ICS-CERT

Web site: http://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 http://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.