INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

CISA CYBER+INFRASTRUCTURE

September 2019

Upcoming Events

- **ICSJWG Webinar**
  November 13, 2019
  "*Secure Operations Technology*" presented by Andrew Ginter of Waterfall Security Solutions
- **Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho**

  Training is scheduled for each month throughout each year.

  Registration for each training session will open about 90 days before the session's scheduled start date.

CISA Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Information Products

CISA Service Menus
Federal Government
Private Industry
State-Local-Tribal-Territorial
International Partners

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, linguistic styles, or recommendations.

2019 Biannual Meetings – Springfield

The ICSJWG continued its 10th anniversary celebration at the August biannual meeting in Springfield, Mass. This meeting was kicked off by CISA Cybersecurity Division Deputy Assistant Director Richard Driggers and included a keynote by Joe Slowik, Principal Adversary Hunter of Dragos. Plenary events included a panel moderated by Andre Ristaino of ISA and sessions by CISA, including the United Kingdom NCSC Liaison to DHS. This meeting also introduced a boot camp on "Becoming an ICS Cyber Analyst" and three full days of technical discussions with hands on content through the technical workshop. The workshop also introduced a "Capture the Flag" event, running throughout the course of the meeting. The program office would like to extend a sincere thank you to all members of the community who work to make the ICSJWG a success.

With the innovations we have developed throughout the past 10 years, we will continue to make our meeting relevant and valuable to the participants. Our next meeting is scheduled for April 2020 in the Northwestern United States. Details will be made available when they are available on our website at https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. The call for abstracts will open soon.

If you have any questions about the upcoming 2020 Spring Meeting, or about anything else ICSJWG-related, please feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

National Cybersecurity Awareness Month

Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online.

NCSAM 2019 will emphasize personal accountability and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. This year's overarching message—Own IT. Secure IT. Protect IT.—will focus on key areas including citizen privacy, consumer devices, and ecommerce security.

Learn more about National Cybersecurity Awareness Month here.

ICSJWG Webinar Series

ICSJWG is continuing its webinar series this November. Andrew Ginter of Waterfall Security Solutions will be discussing the topic of "Secure Operations Technology" on Wednesday, November 13, 2019. This webinar will outline Secure Operations Technology as a perspective, a methodology, and a set of best practices used by thoroughly secured sites. Secure Operations Technology takes measures to physically block or otherwise discipline the entire inventory of inbound information/attack flows.

To participate in this webinar, please RSVP to ICSJWG.Communications@hq.dhs.gov with your name, company's name, role (vendor, owner/operator, etc.), and sector affiliation by November 12th.

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.*

Searching Beyond Traditional Solutions for Protecting ICS

By: Daniel Ehrenreich, Consultant and Lecturer, Secure Communications and Control Experts (SCCE)

Deployment of a strong and effective cyber defense for Industrial Control Systems (ICS) remains a challenge for experts worldwide. We all know the famous statement "there is no silver bullet", and therefore experts must search for innovative technologies beyond the passive Intrusion Detection System (IDS), however without violating important principles and limitations. Considering a solution which requires changing the ICS architecture or an Intrusion Prevention System (IPS) which might interrupt the process or a pen-testing of the ICS (similar to IT inspection), are all not appropriate choices. While being exposed to a broad range of ICS Cyber defense technologies for protecting manufacturing operations and critical utility infrastructure, even experts might face difficulties when trying to determine which one is right for a specific ICS used in their organization.

In this paper I'll describe four independent approaches, which may effectively help you reducing the ICS cyber-attack risks against your organization. Selecting the right method must take into consideration your architecture, the level of probability and the impact of an attack. *Continue to "Searching Beyond Traditional Solutions for Protecting ICS" article…*

Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure

By: Daniel Kapellmann of FireEye and Rhyner Washburn of University of Maryland

Vulnerability management remains a significant challenge for organizations that handle critical infrastructure worldwide. Hallmark cyber-physical incidents with disruptive and destructive capabilities like Stuxnet (2010) and Triton (2017) have exploited known vulnerabilities in information technology (IT) and operational technology (OT) assets throughout the attack lifecycle. However, the global critical infrastructure security community is still nascent in the field of industrial control systems (ICS) vulnerability management, especially in information-sharing. While their counterparts in IT security have spent years elaborating multiple resources to track and disseminate information about known vulnerabilities, the ICS community lacks specialized mechanisms for knowledge-sharing. Multiple challenges exist when addressing this issue: a general lack of awareness about ICS cybersecurity, the need to consider multiple industry sectors and unique network architectures, and the need to find a balance between protecting and releasing sensitive information regarding critical infrastructure organizations or proprietary vendor knowledge. *Continue to "Call to Action" article…*