September 2018

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- **April 23–25**
  ICSJWG 2019 Spring Meeting
  Kansas City, Missouri
- **January 7–11, 2019**
  Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho
  Registration for this training will open on or about October 9, 2018 (~90 days before the session)
- *Tentative*
  ICSJWG Webinar Series December 2018

NCCIC Resources

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

NCCIC 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.

2018 Fall Meeting Recap

The 2018 Fall Industrial Control Systems Joint Working Group (ICSJWG) Meeting, which occurred August 27–30, 2018, in Cincinnati, Ohio, brought together 325 critical infrastructure stakeholders for three full days of collaborative discussions of current and pressing ICS security issues. Each day was kicked off with a keynote presentation. Deputy Assistant Secretary Richard Driggers opened the meeting by addressing the need for Partnering for Critical Infrastructure Security. Robert Lee of Dragos started the second day discussing lessons learned from the Industrial Threat Landscape. Joel Langill of AECOM kicked off the final day with observations made during a field assessment. During the meeting, there were a series of engaging and topically current breakout sessions led by either the private sector or DHS representatives, and there was a hands-on technical workshop led by the National Cybersecurity and Communications Integration Center (NCCIC) educating participants on Network Monitoring, Threat Detection, File Hashing, and File Validation Techniques.

The ICSJWG program office is incorporating feedback from the Fall Meeting into its planning of future Meetings. Thanks to all who contributed with evaluations.

2019 Spring Meeting—Update

Next year, 2019, will be the 10th anniversary of the ICSJWG as a driving force behind information sharing and stakeholder engagement for the security of our Nation's critical infrastructure. If you have any ideas to help celebrate this decade of growth, or to recognize those who have participated since the beginning, please let us know.

The ICSJWG team is excited to provide an update about the ICSJWG 2019 Spring Meeting, occurring April 23–25, 2019, in Kansas City. The ICSJWG is currently working with the venue to finalize the details so that we can make the formal announcement as soon as possible. We are also actively looking for regional asset owners to submit abstracts for presentations.

Be prepared for the Call for Abstracts to be available soon! Detailed information about the meeting will be updated and available on the ICSJWG web site: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

If you have any questions about the upcoming 2019 Spring Meeting, or generally about anything ICSJWG-related, please feel free to send us an email at ICSJWG.Communications@hq.dhs.gov.

ICSJWG Webinar series Update

We are proceeding with developing a schedule for the Webinar series. We will be contacting the volunteers we received from the meeting evaluations and those who contacted the ICSJWG directly to solicit for abstracts. The last webinar, "The Top 20 Cyberattacks on Industrial Control Systems," presented by Mr. Andrew Ginter of Waterfall Security Solutions, drew a large audience from both the United States and abroad. For copies of the presentation, please contact Mr. Ginter directly.

Webinars are typically scheduled near the end of each quarter (March, June, September, and December). If you have an idea to be developed for a webinar, please provide a Title, Abstract (2000 characters or less), approximate date range you could present, and whether the subject matter is time-sensitive. The ICSJWG Steering Team will review all of the abstracts received and we will schedule those selected through the end of calendar year 2019. For any idea to be presented during this year, we recommend providing the abstract no later than October 26, 2018.

Awareness Briefings on Protecting Enterprise Network Infrastructure Devices

The NCCIC will be conducting a series of awareness briefings on Protecting Enterprise Network Infrastructure Devices over the next two weeks. Each webinar will be held from 1:00PM–2:30PM EDT on the dates listed below. Register for a session here.

- Tuesday, October 2
- Thursday, October 4

Threat actors have long targeted network infrastructure devices—such as routers, switches, firewalls, and Network Intrusion Detection Systems—and this activity is only expected to continue. Widespread compromise of these devices could allow adversaries a foothold into critical infrastructure and enable coordinated disruption at a scale.

NCCIC encourages decision makers, network defenders, and procurement analysts to register for the webinar, which will feature a discussion on identified threats, trends in the field, and insights from DHS's binding operational directive impacting federal agencies.

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.*

Principal IoT vs IIoT Differences You Must Know

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Business opportunities created by the Internet of Things (IoT) and the Industrial IoT (IIoT) are among the most debated topics, as these are considered important for a broad range of consumer and industrial applications. Leading market research firms already estimate that by 2020 there will be over 20 billion installed end-point devices worldwide, defined as part of IoT or IIoT systems.

Although the forecasted number is growing every year, it is not clear whether these figures correctly refer to deployments which can be and which cannot be considered as an IoT or IIoT. For article, click here.