INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

CISA CYBER+INFRASTRUCTURE

December 2019

Upcoming Events

- **ICSJWG Webinar**
  March 11, 2020
  "A *Modified Approach to Security and True IT/OT Convergence to Achieve a Robust VM Program*" presented by Rick Kaun of Verve Industrial Protection
- **Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho**

  Next open training session, March 16–20, 2020

  Training is scheduled for each month throughout the year. Registration for each training session opens 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.

2020 Spring Meeting — Salt Lake City

Please Save the Date for the next face-to-face meeting, in Salt Lake City, Utah, from April 14–16, 2020. As soon as the contracting phase with the venue is completed, we will send out the official announcement with registration information for the meeting and for the venue.

The Call-for-Abstracts has been released to the membership. The submission form allows for presentations, demonstrations, panels, and lightning rounds, as well as requests for Vendor Booth space at the Vendor Expo.

As we have over the past 10 years, we will continue to use member feedback to guide innovation to keep the meeting relevant and valuable to the participants. When ready, details will be made available on our website at https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.

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.

ICSJWG Webinar Series

ICSJWG is continuing its webinar series in March 2020 with Rick Kaun of Verve Industrial Protection. Mr. Kaun will be discussing "A Modified Approach to Security and True IT/OT Convergence to Achieve a Robust VM Program." This webinar will outline a "Think Global but Act Local" approach to security: a central team centrally monitors and identifies all OT assets in scope across multiple operational facilities. Security actions or trends that require execution or remediation are identified. This team, in conjunction with OT-specific representation at the site, will plan, schedule, and execute any tasks through automated technology with on-site OT oversight. This approach provides multiple benefits to the operating company, which will be elaborated on during the webinar.

The webinar will provide case studies of operating companies using this "Think Global but Act Local" approach to leverage IT technology with OT oversight to achieve measured, OT-safe control and protection.

To participate in this webinar, please RSVP using a work-related email to ICSJWG.Communications@hq.dhs.gov with your name, company name, role (vendor, owner/operator, etc.), and sector affiliation by March 10, 2020.

Cybersecurity Evaluation Tool (CSET®) Version 9.2 release

We would like to announce CSET® version 9.2. This version is available for download at https://github.com/cisagov/cset/wiki. The latest version of CSET® includes several exciting new feature enhancements and upgrades:

- Web based diagram editor,
- Enhanced reporting,
- A new capability maturity model for financial sector customers,
- NCUA ACET Standard,
- Financial sector risk assessment wizard,
- New analysis for network diagram questions,
- TSA-2018 Pipeline security standard,
- And the often-requested ISA-62443.

This new version continues to add to an already flexible open source platform allowing for easy installation via windows installer or build from source. Save time and money on a disciplined, repeatable process without having to wade through hundreds of pages of cybersecurity standards.

Fall 2019 ICSJWG Meeting – Summary of Brainstorming Sessions

The Fall 2019 Industrial Control Systems Joint Working Group (ICSJWG) Meeting provided multiple brain storming sessions to asset owners, integrators, vendors, and government representatives offering a new opportunity to voice thoughts, ideas, and suggestions in solving problems collectively. These moderated discussions provided an equal voice to all participants, inviting valuable input to the challenges we all face. Word clouds were used to help prioritize specific topics of interest from the audience. Highlights from each brainstorming session are included in the article and will be used to help drive CISA priorities and focus areas for future brainstorming sessions. *Continue to "Summary of Brainstorming Sessions" article…*

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.*

Managing the Energy Grid

By: Barry Jones, Western Area Power Administration, Sierra Nevada Region

When it comes to managing the electric grid (water, refineries, etc. too), it seems an easy proposition to virtualize Control Centers and host SCADA/ICS apps in the cloud. An operator launches the Energy Management System (EMS) or SCADA (supervisory control and data acquisition) apps and controls and monitors the grid from anywhere.

As a young technologist in the 1990's, I excitedly pitched this concept to my electric transmission director - how I could use my laptop, loaded with the Energy Management System (EMS) client, to monitor and control a portion of Southern California's grid from the parking lot inside my car. He was a very good boss because after the initial shock washed off his face he looked over the example sessions and listened to the principles, OSI model, and details. *Continue to "Managing the Energy Grid" article…*

The Supply Chain is Expanding the Attack Surface on your ICS

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Industry experts worldwide dealing with Industrial Control Systems (ICS) recognize the famous Stuxnet attack in 2010 (compromising a nuclear facility) as the formal starting point for dealing with cyber security. Until then, this concern did not get proper attention from vendors nor users, and only high level classified organizations implemented early-stage cyber defense solutions. The real game changer was triggered around 2014-2015, when several organizations worldwide suffered from real cyber-attacks.

Among these were externally generated attacks on the ICS through the IT zones of the organization and internal cyber-attacks done by disgruntled employees, external service people and others, who had authorized access to the ICS. Industry experts worried about these risks, but until the famous Target chain attack in 2013, caused by negligent processes of their subcontractor, the attention was minimal.

This paper specifically focuses on risks created by the supply chain, and outlines several considerations and scenarios which jointly combine into the "attack surface" term. Obviously, the wider the attack surface, the higher are the chances of cyber-attack against your organization. *Continue to "Supply Chain is Expanding the Attack Surface" article…*

The GAO and Disaggregation of Generating Assets in the North American Electric Grid

By: Courtney Schneider, Cyber Policy Research Manager, Waterfall Security Solutions

In August 2019, the US Government Accountability Office (GAO) published a Report to Congressional Requesters expressing concern regarding the current state of security and resilience for the US power grid. The GAO found that there are credible and sophisticated threat actors capable of targeting North American grid systems, and due to advancing digital technology installed in grid operations, the grid is becoming more vulnerable to cyberattacks by these actors. These concerns form the background for the GAO investigation and the report's recommendations to the Department of Energy (DOE) and the Federal Energy Regulatory Commission (FERC).

Our focus in this article is the GAO recommendation to FERC to:

"Evaluate the potential risk of a coordinated cyberattack on geographically distributed targets and … determine if changes are needed in the threshold for mandatory compliance with requirements in the full set of cybersecurity standards." *Continue to "GAO and Disaggregation of Generating Assets" article…*