INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

June 2020

Upcoming Events

Industrial Control Systems Cybersecurity Training provided by INL or in Idaho Falls, Idaho

Next open training sessions
Jul 6—10, 2020 (301P) *
Jul 13—17, 2020 (301P) *
Jul 20—24, 2020 (301P) *
Jul 27—31, 2020 (301P) *
Aug 17—21, 2020 **
Sep 14—18, 2020 (301)
Oct 12—16, 2020 **
Nov 9—13, 2020 (301)
Dec 7—11, 2020 **

** Online training*
*** 401 Training – must have completed 301 to attend this session.*

CISA Resources

COVID-19
Training Resources
Incident Reporting
Assessments
CSET®
Alerts
Advisories
HSIN
Information Products

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.

UPDATE! ICSJWG 2020 Spring Virtual Meeting

On June 9—10, CISA presented the first virtual version of the Industrial Control Systems Joint Working Group (ICSJWG) bi-annual event, the ICSJWG Spring 2020 Virtual Meeting.

The virtual meeting featured keynotes by CISA Director Chris Krebs and the founder of ioSentrix, Omair Manzoor. Innovations included in this meeting were based on recommendations from attendees at previous meetings. On Day 1, ICS partners delivered presentations . Day 2 provided an overview of the new CISA ICS Training, which was introduced during the month of June 2020. Day 2 continued with additional technical workshop style presentations. Additionally, a "Capture the Flag" activity for the participants was held over both days of the meeting.

The meeting was attended by ICS community members from around the globe, including those new to the concepts as well as subject matter experts with years of experience. All presenter-approved presentations are available on the ICSJWG Engagement Hub until the ICSJWG Fall 2020 Meeting. The link to available presentations is here.

Over the course of the meeting we received almost 500 requests for membership. We also received a tremendous amount of positive feedback from attendees, as well as constructive feedback that we will evaluate for improvements during the fall event. We look forward to continually building our partnership with the ICS community.

UPDATE! ICSJWG 2020 Fall Virtual Meeting

Save the Date for the ICSJWG 2020 Fall Virtual meeting currently being planned for September 22—23, 2020. As we develop the site for the meeting, we hope to have as many appealing speakers as we had for the Spring. Watch for the ICSJWG to send out the Call for Abstracts soon so we can provide another exciting information sharing event.

Securing Industrial Control Systems: A Unified Initiative

The Cybersecurity and Infrastructure Security Agency (CISA) released a strategy to strengthen and unify industrial control systems cybersecurity for a more aligned, proactive, and collaborative approach to protect the essential services that Americans use every day.

The strategy, *Securing Industrial Control Systems: A Unified Initiative,* is intended to help architects, owners and operators, vendors, integrators, researchers, and others in the ICS community build capabilities that lead to more secure ICS operations. Ultimately, it strives to move CISA and the ICS community beyond reactive measures to a more proactive ICS security focus.

"In recent years, we have seen industrial control systems targeted from various persistent and imaginative adversaries, causing disruption and negatively impacting essential services," said Chris Krebs, Director of the

Cybersecurity and Infrastructure Security Agency. "With the ICS industry and interagency community, this-strategy that will lead us to new, unified initiatives and security capabilities that will markedly improve the way we defend and secure ICS."

Although ICS owners and operators manage their own security, it is CISA's mission to assist through delivery of a broad portfolio of ICS security products and services, especially when an exploitation may threaten people or property or undermine confidence in critical infrastructure, safety, and reliability.

The CISA ICS initiative is a five-year plan that builds on the collaborative work already done and the existing support CISA provides to the community. It also elevates ICS security as a priority within CISA, coalescing CISA's organizational attention around the implementation of a unified "One CISA" strategy. The initiative organizes our efforts around four guiding pillars:

Pillar 1: Ask more of the ICS community; deliver more to them.

Pillar 2: Develop and utilize technology to mature collective ICS cyber defense.

Pillar 3: Build "deep data" capabilities to analyze and deliver information that the ICS community can use to disrupt the ICS cyber-kill chain.

Pillar 4: Enable informed and proactive security investments by understanding and anticipating ICS risk.

The CISA ICS strategy can be found at https://www.cisa.gov/ics under Resources.

Up-to-Date Information about the Nationwide Medical Crisis

You can find up-to-date information, releases, and updates regarding COVID-19 at www.CISA.gov/coronavirus. These include the following:

- The CDC has guidance for discontinuation of isolation for persons with non-test confirmed COVID-19 in a non-healthcare setting. Persons with COVID-19 who have symptoms and were directed to care for themselves at home may discontinue isolation under the following conditions: (1) At least three days (72 hours) have passed since recovery, defined as resolution of fever without the use of fever-reducing medications; (2) Improvement in respiratory symptoms (e.g., cough, shortness of breath); and (3) At least seven days have passed since symptoms first appeared.
- The UK and CISA published a joint advisory on cybercriminals and advanced, persistent threat groups targeting individuals and organizations with a range of ransomware and malware. The assessment includes indicators of compromise and guidance on how to decrease the risk of cyber attacks.
- A Frequently Referenced Contact Information section to advertise the various avenues to access information, including previous recordings of the Tuesday/Thursday CISA ESF 14 Broad Stakeholder calls.
- FEMA created a Rumor Control page to provide ground truth on rumors and facts at https://www.fema.gov/coronavirus-rumor-control.

DHS Telework Guidance "Protection of Remote Technologies in a Telework Environment"

CISA, the FBI, and other federal entities have released various articles to help workers who are currently working from alternative spaces as a result of the COVID-19 pandemic and consequential stay-at-home orders. Alternative technological methods are being accessed by new users who may be unaware of some of the vulnerabilities and limitations of these solutions. Two current sources of information include the CISA TIC Interim Guidance, which can be found on the CISA Trusted Internet Connections page, and a warning from the Federal Bureau of investigation (FBI) about teleconferencing and online classroom hijacking.

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.*

Recent Activities in Sweden to Counter Antagonistic Electromagnetic Threats

Submitted By: Gustav Söderlind, The Swedish Civil Contingencies Agency (MSB)

Electromagnetic threats can disrupt information systems by affecting the electronics used to run the systems, and/or the wireless communications they often depend on.

Jammers, although generally illegal to use (in Sweden also illegal to possess), are readily available to the general public. High Power Microwave (HPM) generators are offered for sale to law enforcement as vehicle stoppers at short ranges, and knowledge of how to construct HPM devices is spreading online. Larger devices that can be hidden in a small truck can be used to disrupt the operation of unshielded IT-systems at ranges of up to several

hundred meters. *Continue to complete "Recent Activities in Sweden" article…*

Consequences of a Cyber-Attack on an Industrial Plant

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

The cyber defense for Industrial Control Systems (ICS) is a role for experts, who acquired in-depth understanding on ICS technologies and applications, as well as on cyber risks and defense technologies. While IT systems are built to protect financial and personal data through assurance of the CIA Triad (Confidentiality-Integrity-Availability), the cyber defense for industrial and utility operations must be assured through the SRP Triad (Safety-Reliability-Productivity).

But, how would you differ between a cyber-attack risk on a non-critical facility, versus a chemical or nuclear plant? The differences will be in figures referring to the probability of the attack (P) and the impact (I) on the facility' used for calculating of the risk factor (R). Consequently, you must consider taking proactive steps to reduce the risk of lengthy outages trough Business Continuity planning (BCP), Incident Response (IR) and Disaster Recovery Planning (DRP) processes. *Continue to complete "Consequences of a Cyber-Attack" article…*