INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

CISA CYBER+INFRASTRUCTURE

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

March 2019

Upcoming Events

- **ICSJWG Webinar**
  Call for Abstracts is open
- **April 23-25, 2019**
  ICSJWG 2019 Spring Meeting, InterContinental Kansas City at the Plaza in Kansas City, Missouri
- **July 8-12, 2019** (Tentative)
  Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho
  Registration for this training will open about 90 days before the session 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 Spring Meeting Update

This is 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. We hope you will come celebrate with us in Kansas City, April 22-25, 2019! We are excited about the speaker lineup, including keynotes by NCCIC Director John Felker, and Marty Edwards, Director of Strategic Initiatives, ISA, and Managing Director of the Automation Federation. To see the full agenda, please visit the ICSJWG webpage.

The Spring Meeting will take place at the InterContinental Kansas City at the Plaza, located at 401 Ward Parkway, Kansas City, Missouri.
To register for the meeting, please use this registration link. Registration is due by April 17, 2019. (This registration link is for the meeting only.)

For room block reservations, call **1-866-856-9717** and specify group 'ICS' or 'ICSJWG Spring Meeting,' or use this room block link. The hotel will close the group rates for rooms on April 8, 2019.

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

Cybersecurity and Infrastructure Security Agency

In November 2018, the U.S. Congress enacted the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

CISA leads the national effort to defend critical infrastructure against the threats of today, working with partners across all levels of government as well as in the private sector to secure against the evolving risks of tomorrow.

The Agency is organized into the Cybersecurity Division, Infrastructure Security Division, and Emergency Communication Division in order to best address threats and assist partners.

Director Krebs has identified ICS as a top Agency priority and the ICSJWG looks forward to growing within CISA. We look forward to providing the same services the community has come to rely upon while leveraging a broader organization to deliver more value to the ICS community. Community members can continue to reach out through existing NCCIC channels as CISA continues to grow.

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.*

Design and Build Productive and Secure Industrial Systems

By: Kenneth G. Crowther, General Electric | Robert E. Lee, Dragos | K. Reid Wightman, Dragos

This series of three cybersecurity whitepapers is intended for engineers and designers of industrial control processes and the systems that control those processes. Throughout the papers, we emphasize the point that data is not exhaust left-over from a sensor-heavy process, but it is the driver of future value by enabling visibility, understanding, and ever-more-precise control of the processes. However, the activities to increase value by using ever more distributed information and system connectivity potentially expose systems to risk of cyber exploitation.

Building Security to Achieve Engineering and Business Requirements (Whitepaper 1)

Paper #1 demonstrates that greater value is derived from security when clear articulation of engineering and business requirements drive security, rather than the other way around. It provides a construct to capture basic connectivity between systems as a foundation for contextualizing threats and security solutions. *Continue to Whitepaper 1…*

Understanding Threats Will Promote the "Right Amount" of Security (Whitepaper 2)

Paper #2 focuses on articulating how to cost-effectively understand threats against industrial systems and drives the point that security should be adapted based on connectivity requirements from the business and the threats to the processes, rather than published vulnerabilities and exposures. *Continue to Whitepaper 2…*

Blending Resilience and Protection to Achieve Greatest Security for Business-Viable Industrial Systems (Whitepaper 3)

Paper #3 ties the two pieces together and further explores details of how engineers can guide the implementation of good industrial control system (ICS) security into the future as next generation control systems and connectivity requirements emerge. It assumes some knowledge of the basics, and focuses on what engineers should learn to design next-generation security around the business and engineering requirements of ICS. *Continue to Whitepaper 3…*

Threats to Small Defense Businesses Can Have an Outsized Impact

By: Dan Callahan, Owl Cyber Defense

Defense Industrial Base (DIB) manufacturers in the United States thoroughly understand the concepts of regulation and compliance. Almost no aspect of their business is outside the reach of some state-level or federal oversight agency or law. As some of the most sensitive organizations in existence, they are also no stranger to risk.

Risk exists at all levels, both inside and outside of the building, from physical locks to hiring trustworthy employees to finding honest (and secure) vendors and partners. Then of course there are the risks associated with a growing number of cyber threats, from passive malware-infected files and websites to sophisticated, persistent attacks. Cyber risk mitigation is the difference between business as usual, and a state-sponsored criminal burrowing deep into your network and planting a botnet node to steal sensitive information and turn your own devices against you. *Continue to "Threats" article…*

Inspecting your ICS for Cyber Vulnerabilities

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

Industrial Control Systems (ICS) Cyber security experts shall have many years of ICS technology experience as a prerequisite for leadership position in this field. Unfortunately, this is not a situation in most ICS related organizations and you may often hear a not-clearly-explained term "IT-OT convergence". The truth is, that ICS cyber security experts never agreed to this term, probably introduced by IT teams who seek including ICS Cyber security under their responsibility.

To address this topic, you may ask a valid question: "How do I assure the Safe and Reliable operation of the ICS, and achieve adequate level of Productivity (SRP)?" The simple answer to this challenging question is: "Adhere to the PPT Triad" (People-Policies-Technology). The PPT topic was already covered in my previous post, and in this paper, I will focus on best practices, organization processes and test-actions which are required to perform vulnerability inspection of your ICS. *Continue to “Inspecting” article…*