CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

March 2023

UPCOMING EVENTS

Register to Attend!

ICSJWG 2023 Spring Meeting
May 9-11, Salt Lake City, Utah
Register Today!

ICSJWG March Quarterly Webinar
Wednesday March 29, 2023, 1:00-2:15PM
Register Today!

Trainings:

Quarterly ChemLock Trainings
April 12 & July 13
Course Information -- April Registration -- July Registration

Industrial Control Systems Cybersecurity (401v) Online Virtual Training
March 6-24
Course information -- Registration

Industrial Control Systems Evaluation (301v) Online Virtual Training
March 6-24
Course information -- Registration

Industrial Control Systems Evaluation (301L) In-Person Training
March 13-16
Course information -- Registration

Industrial Control Systems Cybersecurity (401L) In-Person Training
March 28-30
Course information -- Registration

Additional ICS Training
CISA Virtual Learning Portal

ICSJWG 2023 Spring Meeting Updates!

ICSJWG is thrilled to announce that Registration for the 2023 Spring Meeting is now open! This event will be in-person in Salt Lake City, Utah, on May 9-11 at the Radisson Hotel Salt Lake City Downtown.

The Spring Meeting will feature three full days of stakeholder presentations as well as a virtual Capture the Flag activity.

Additional highlights include presentations by CISA Threat Hunting, a demonstration of the ICS Control Environment Lab Resource (CELR), and instructional training by CISA Cyber Defense Education & Training (CDET).

CDET will for the first time provide an Escape Room activity. We are also pleased to bring back the Vendor Expo.

ICSJWG Meetings are open to all who are interested and are free for attendees. Additional information on registration and accommodations can be found on our ICSJWG webpage.

Interested in presenting? The Call for Abstracts for the Spring Meeting is still open, and we need presenters! Please keep in mind that no pre-recorded presentations will be accepted as all submissions are required to be presented live and in-person. The deadline to submit an abstract for review is March 10, 2023. If you are interested in submitting an abstract, please fill out this Interest Form.

This form is also used to save your spot for a vendor booth. Spaces are limited, so act now!

We look forward to seeing you in person this spring to continue building our partnership and sharing ideas that make our country safer!

Join Us for Our Upcoming March Webinar!

Join us for *Defense in Depth: How Election Officials Approach Voting System Security* on March 29 from 1:00-2:15 PM ET. Representatives from CISA's Election Security and Resilience team will discuss the technological, physical, and procedural controls used across the election infrastructure subsector to mitigate cybersecurity risk and ensure that voting systems function as intended. Registration for this event is now open!

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.

Join Our Steering Team!

The objective of the ICSJWG Steering Team (IST) is to enhance and grow ICSJWG collaboration efforts and provide guidance on programming efforts. The IST is comprised of a diverse group of representatives from the Industrial Control Systems (ICS) community, and we are actively searching for new members! If you or a colleague is interested in learning more about this opportunity, please contact us at ICSJWGCommunications@cisa.dhs.gov.

How to Proactively Use an SBOM for Vulnerability Monitoring

By: Dick Brooks

An SBOM, in combination with a NIST Vulnerability Disclosure Report, can help software consumers identify risky software vulnerabilities proactively, before procurement and before software installation in a device. Using a tool such as Dependency Track, a software consumer can implement ongoing monitoring for new vulnerabilities in software products that are already installed in a company ecosystem, enabling a consumer to shrink the window of susceptibility when new vulnerabilities are reported, by enacting mitigating actions before hackers have to an opportunity to exploit a new vulnerability.

Continue to full article…

The Hunt for Deeper Level Asset Data and Why It Matters for Security

By: Aaron Crow

Visibility and the collection of detailed data from industrial environments is not "cybersecurity" in and of itself, but it is the foundation of most cybersecurity programs. Asset visibility refers to the ability to see and track assets within an industrial control system (ICS) environment. OT asset management, on the other hand, refers to the process of managing and maintaining the assets within an ICS environment. OT asset management entails building upon asset visibility with deeper level asset data and gaining a better understanding of the state of systems within the OT environment. Both OT asset visibility and OT asset management are important for protecting critical infrastructure and integrating the two is a significant step towards security maturity for ICS environments. Having a single source of truth for asset owners that combines people, processes, and technologies to aggregate all these methods is essential for OT security progress.

Continue to full article…

Segregating the ICS-OT "Insecure by Design" Architecture

By: Daniel Ehrenreich

Industrial Control Systems (ICS)/Operation Technology (OT) experts already agree that ICS-OT and IT systems must be separately designed, deployed and assessed to verify their operation performance. Upon completing such testing, they can be securely interconnected but must never be built as "converged networks". Considering the growing number of vulnerabilities detected in Programmable Logic Controllers (PLC) to minimize the risks created by exploitable vulnerabilities, experts now consider deploying segregating appliances within the ICS-OT zone. In order to understand whether ICS-OT cyber security architects are allowed to deploy segregating devices within that zone, the applicable considerations for correctly deployed segregation within the ICS-OT system must be explored.

Continue to full article…

Using "Man-in-the-Middle" to Build a Zero Trust Architecture for ICS

By: Jim Birmingham

Designing a Zero Trust Architecture often means starting from the basics of what Zero Trust is and what it means to your organization. A starting point must then be identified, followed by the development of an execution plan which can be as simple as using known strategies from adversaries to combat them. Could designing a "man-in-the middle" mitigation propel you on your journey of achieving a Zero Trust architecture? Discussing how the approach of being "in the middle" allows you to broker trust relationships and increase your security will provide further insight on how to solve for Zero Trust.

Continue to full article…

Cybersecuring Control Systems, Cyber Training and Cybersecurity Compliance Maturity Model Updates

By: Michael Chipley

Cyber-securing control systems and contractor business systems that have CUI are an evolving practice, but it is essential that organizations that hold the sensitive information on how the systems were designed, installed, commissioned, and operate have robust and state of the practice cyber hygiene in place. Loss of the information could result in a compromise of the systems and become a cyber incident that could result in physical destruction, loss of life or property, and direct mission impact. Industry and Organizations are becoming more cyber aware, and training is available for Hunt and Defend, Cyber Incident Response, and protecting CUI.

Continue to full article…

More Than 17 Million Control System Cyber Incidents Are Hidden In Plain Sight

By: Joe Weiss

Control system cyber incidents are more plentiful and impactful than most observers expect - more than 17 million directly resulting in more than 34,000 deaths. While there have been more than 1,200 electric grid cyber-related incidents, that doesn't adequately reflect the true impact on customers and the economy. The majority of the 17 million plus control system cyber incidents were malicious but not unintentional. By number of incidents, most of the control system cyber incidents were engineering-based attacks used to camouflage a deficiency in the design of the product or to cause physical damage. These attacks did not involve the Internet, Windows, or OT networks to carry out the attacks. Consequently, these incidents were not identifiable by network cyber forensics and would not fall under the CISO's domain. This means most of these incidents would not be addressed by existing government and industry cyber security guidance, nor make its way to the Boards as cyber events. In addition, the diesel cheat scandal lays bare the philosophical differences in how offensive cyber attackers and cyber defenders' approach cyber security. The impacts from the diesel cheat scandal were huge, more than $35 Billion in damages and several people went to jail, yet many defenders would not consider these to be malicious cyberattacks because they weren't the type of attacks they were expecting. Until the OT network-focused regulators and practitioners are willing to address engineering-based incidents and attacks, critical infrastructures cannot be secured.

Continue to full article…