INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

QUARTERLY NEWSLETTER

ICSJWG EXPANDING THE COMMUNITY

CISA CYBER+INFRASTRUCTURE

June 2019

Upcoming Events

- **July 17, 2019**
  ICSJWG Webinar Series
- **August 27-29, 2019**
  ICSJWG 2019 Fall Meeting
  Springfield, Massachusetts
- **September 30-Oct 4, 2019**
  November 11-15, 2019
  December 9-13, 2019
  Industrial Control Systems Cybersecurity (301) Training in Idaho Falls, Idaho
  Registration for this training will open about 90 days before the scheduled session 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 Biannual Meetings

The ICSJWG kicked off its 10th anniversary in Kansas City, Missouri. This meeting featured keynotes by Assistant Director John Felker and Marty Edwards, Director of Strategic Initiatives, ISA, showing the community how far it has come and where it could be headed. We heard from across the community on topics from product security to vulnerability disclosure to virtual reality. This meeting also featured three full days of technical discussions with hands on content through the technical workshop and a live demonstration of the kinetic impacts of risk to industrial control systems. The program office would like to extend a sincere thank you to all members of the community who work to make the ICSJWG a success.

We will be continuing the 10th anniversary celebration this fall. We hope you will join us in Springfield, Massachusetts, from August 27–29, 2019, for the ICSJWG Fall Meeting. Details can be found on the website at https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. The call for abstracts is open until July 26, 2019. Submit your abstracts to help the ICSJWG membership secure their systems.

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

ICSJWG Webinar Series

ICSJWG is continuing its webinar series this July. Dr. Vijay Ahuja and Devesh Ahuja of Cipher Solutions will be discussing the topic of 'Persistent Threat-Based Security for ICS Systems' on Wednesday, July 17, 2019. This webinar will outline an approach to strengthen the security of Operation Technology (OT) systems by proposing real-time, threat-based, adaptive protection against cyber threats and attacks.

To participate in this webinar, please RSVP to ICSJWG.Communications@hq.dhs.gov with your name, company's name, role (vendor, owner/operator, etc.), and sector affiliation by July 12, 2019.

Introducing the ICSJWG Steering Team (IST)

The ICSJWG established the ICSJWG Steering Team (IST) to facilitate the coordination and oversight of ICSJWG activities. The IST is comprised of representatives from the ICSJWG membership, in roles such as Asset Owners; Vendors; Federal, State, Local, Territorial, and Tribal government agencies; Industry Associations; University/Academic Institutes; Consultants/Integrators; and International Stakeholders. The IST plays a critical role in shaping the ICSJWG and we thank the members for serving as the voice of the community.

For those who were not able to join us at the Spring Meeting, we wanted

to introduce the current members. The current members of the IST are: Dr. Art Conklin (Co-Chair) (University/Academic), Janine Sheppard (Co-Chair) (Federal Government, ICSJWG Lead), Donovan Tindill (Vice Co-Chair) (Vendor), Randy Woods (Asset Owner), Blake Larsen (Asset Owner), Bryan Owen (Vendor), Dan Strachan (Industry Association), Jens Wiesner (International), Rob Pitcher (International), Todd Therrien (SLTT), Mark Heard (Industry Consultant), and John Cusimano (Industry Consultant). If you are interested in joining the IST in the future, please email ICSJWG.Communications@hq.dhs.gov.

CISA Relaunch of the Newly Integrated Website

The Cybersecurity and Infrastructure Security Agency (CISA) is excited to announce the launch of the unified and improved us-cert.gov. On June 25th, us-cert.gov and ics-cert.us-cert.gov combined to become the integrated us-cert.gov, providing a comprehensive, easy-to-navigate website with an updated look and feel.

All products published on the legacy us-cert.gov and ics-cert.us-cert.gov will remain the same, and you will still be able to access the same information and report on incidents and malware. With this consolidated web presence, CISA is better positioned to engage with partners to anticipate, prioritize, and proactively manage ICS risk—a top priority for CISA.

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.*

Soliciting feedback on Building Management Systems Cybersecurity Certification Program

By: Steve Griffith, National Electrical Manufacturers Association

Representatives from the Department of Defense (DOD), International Society of Automation (ISA), and the National Electrical Manufacturers Association (NEMA) outlined a new program to address the growing risk of unprotected and under-protected building control systems in the U.S. and abroad. The national program will incentivize the use of existing Standards for cybersecurity in building control systems. It will create easy-to-understand tiers for end-users to apply industry-accepted Standards to products, processes, and technology to allow end-users to market cyber protections and consumers to understand the level of security present. The program would also help building owners protect building automation systems, and provide a means for insurers and other stakeholders to offer incentives for buildings to incorporate safer and more secure systems and processes.

The working group that has been primarily responsible for developing a prospectus framework document for this program would like to open it up for broader additional stakeholder input. If you are interested in receiving a copy of the framework document please contact Steve Griffith, Industry Director at NEMA (email: Steve.Griffith@nema.org) directly.

NIST Releases Draft NISTIR 8183A (3 Volumes) "Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide" for Public Comment

By: National Institute of Standards and Technology

A draft implementation guide for the Cybersecurity Framework (CSF) Manufacturing Profile Low Security Level has been developed for managing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices.

This guide provides general implementation guidance (Volume 1) and two example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products, that are currently available today, can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based

manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement.

The CSF Manufacturing Profile is available free of charge from: https://doi.org/10.6028/NIST.IR.8183. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

The public comment period for these documents ends on July 8, 2019. See each of the publication links for a copy of the document and instructions for submitting comments.

• Draft NISTIR 8183A Volume 1, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance.* ***Volume 1 – General Implementation Guidance***

• Draft NISTIR 8183A Volume 2, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case.* ***Volume 2 – Process-based Manufacturing System Use Case***

• Draft NISTIR 8183A Volume 3, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case.* ***Volume 3 – Discrete-based Manufacturing System Use Case***

Should you have questions about the documents or issues with accessing these documents or the comments form, please contact NIST at csf_manufacturing_profile_implementation@nist.gov

Dangerous Cyber Attacks May Not Be Detected By Network Monitoring – Engineers Are Also Needed

By: Joe Weiss, Applied Control Solutions

Operational Technology (OT) network monitoring and threat detection is necessary for control system cyber security. What was clear about the 2017 Triconex cyber attack was network monitoring and threat detection were not sufficient. Luck and some mistakes kept the Saudi Arabian petrochemical plant from a dangerous explosion. Mistakes included the attackers' inadvertently tripping the plant twice - in June and then again in August. (A plant is said to “trip” when it ceases production for a reason related to safety.) Without the plant trips, it is questionable if the malware would have been found.

All of the presentations I had heard on the Triconex cyber attack, including those by national laboratories, focused on the malware found in the safety systems during the August 2017 outage. *Continue to “Cyber Attacks May Not Be Detected” article…*

In Depth Understanding of IoT and IIoT Ecosystems is Critical

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

The world will see a step forward towards the Internet of Things (IoT) and Industrial IoT (IIoT) ecosystems, when people will focus on in-depth understanding of how these ecosystems shall be structured without creating cyber security risks and how will they deliver operating and financial values. Important pointing out, that these end-point devices are not communicating each with other (peer-to-peer), but are collecting and sending data to their designated service providers, which upon analyzing the field conditions publish decision-oriented data. Once accepting these highlights, we may start talking about tens of billions IoT and IIoT devices expected in 2020 and 2030.

This paper is aimed to outlining the key considerations related to IoT and IIoT ecosystems, allowing you making business-wise decisions. You shall always verify that the proposed IOT or IIoT ecosystem concept is matching your expected goals and last but not least verify that the proposed ecosystem architecture

complies with IoT /IIoT cyber security challenges. *Continue to "Understanding IoT and IIot" article…*

Secure Operations Technology

By: Andrew Ginter, Waterfall Security Solutions

IT Security (IT-SEC) protects information. Secure Operations Technology (SEC-OT) protects physical operations *from* information, more specifically from attacks that may be embedded in information. All cyber attacks are information after all, and all information may encode an attack. SEC-OT is a perspective, a methodology and a set of best practices documented in my new book by the same name. *Continue to "Secure Operations Technology" article…*