September 2017

Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter

— ICSJWG EXPANDING THE COMMUNITY —

Upcoming Events

- October 25: ICSJWG Webinar Series "Creating Predictable Fail Safe Conditions for Healthcare Facility-Related Control Systems and Medical Devices by Use of System Segmentation" **2:00 pm (EST)**
- October 9–13: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, Idaho
- October 23–27: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, Idaho
- November 13–17: Industrial Control Systems Cybersecurity (301) Training Idaho Falls, Idaho

ICS-CERT Resources

Training Resources
Incident Reporting
Assessments
CSET®
Alerts & Advisories
HSIN
Latest Monitor

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, or recommendations.

2017 Fall Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) hosted the 2017 Fall Meeting in Pittsburgh, Pennsylvania, on September 12–14, 2017. The Meeting attracted over 300 stakeholders from the ICS community, including ICS asset owners and operators, vendors, academics, and various others. During the 3-day event, attendees were able to experience seminars, presentations, and panels on a variety of ICS topics, intimate breakout sessions and lightning-round talks on specific subject matter, engage vendors and workshop demonstrations, and network with one another.

This meeting featured a keynote presentation from Joel Brenner, CIS Senior Research Fellow at MIT, in which he discussed significant sources of cyber insecurity in critical sectors, and highlighted the economic, political, and technological obstacles to creating more secure networks. John Felker, DHS/NCCIC Director of Operations, also provided a keynote address, exploring future services to the ICS community and maintaining ICS expertise in the National Cybersecurity and Communications Integration Center (NCCIC).

Throughout the event, the range of the presentations ensured attendees heard from a variety of perspectives from across the stakeholder community. Presentations were complemented by the availability of vendors and workshops for hands-on engagement. For future Meetings, we expect to refine this nexus to ensure attendees can continue benefitting from diverse ICS resources that the ICSJWG brings together.

2018 Spring Meeting Announcement

ICS-CERT is excited to announce the ICSJWG 2018 Spring Meeting! The meeting will take place in Albuquerque, New Mexico, on April 10–12, 2018. Please save the date and we hope that you will join us this spring.

The ICSJWG team will provide more information for the event on the ICSJWG web site when available: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG. In the meantime, if you have any questions, feel free to email us at ICSJWG.Communications@hq.dhs.gov.

Continuing the ICSJWG Webinar Series

ICS-CERT looks forward to continuing its webinar series. On October 25, 2017, Michael Schroeder, Director of Programs at 3 Territory Solutions, LLC, will present on "Creating Predictable Fail Safe Conditions for Healthcare Facility-Related Control Systems and Medical Devices by Use of System Segmentation." The webinar will commence at 2:00 pm (EST).

If you are interested in participating, please contact ICSJWG.Communications@hq.dhs.gov. The ICSJWG team has planned additional webinars for January and March of 2018.

If you have a topic you would like to share with the ICSJWG community, please consider an ICSJWG-hosted webinar. For more information, please contact ICSJWG.Communications@hq.dhs.gov.

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.***

We did not invest enough in cyber defense for ICS!

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

Over past years not enough resources have been allocated for protecting ICS serving manufacturing plants, controlling water and energy systems, etc. On the other hand, the same organizations invested in cyber defense for IT systems mainly due to published attacks, which made IT managers highly concerned. There are many reasons for different handling of IT and ICS cyber security. Some are justified and not caused by laziness or negligence of experts or the lack of budgets. The good news are already here, and in recent years tens of companies entered to this segment and focus on creative cyber defense for ICS. This change is happening primarily as a result of growing number of attacks on ICS and recent intention of attacker to harm critical infrastructure. To continue reading click here.