

## Upcoming Events

- July 11 – 15:  
Industrial Control Systems Cybersecurity (301) Training  
Idaho Falls, ID
- September 13-15:  
ICSJWG 2016 Fall Meeting  
Ft. Lauderdale, FL
- September 26-30:  
Industrial Control Systems Cybersecurity (301) Training  
Idaho Falls, ID

## 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.

### Spring 2016 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) 2016 Spring Meeting was held at Chaparral Suites – Scottsdale, in Scottsdale, AZ, on May 3-5, 2016. This was the largest ICSJWG Meeting to date, bringing together over 300 stakeholders from the ICS community. Over the course of 3 days, attendees had the opportunity to attend numerous seminars and interact with the community through demonstrations, presentations, panels, and lightning round talks.

Highlights of the 2016 Spring Meeting included keynote presentations from Deputy Assistant Secretary for Cybersecurity and Communications Gregory Touhill, President & CEO of Arizona Cyber Threat Response Alliance (ACTRA) Frank Grimmelmann, President & Chief Scientist of Lofty Perch Mark Fabro, and Director of ICS-CERT Marty Edwards. The meeting also featured, a Hands-On Forensics Technical Workshop which allowed attendees to learn recommended best practices for performing hard drive and memory captures on a live system, the second ICSJWG Vendor Expo, and an “Ask Me Anything” session with Marty Edwards.

### 2016 Fall Meeting Preview

We are excited to announce that the ICSJWG 2016 Fall Meeting will take place September 13-15, 2016 at Embassy Suites Ft. Lauderdale – 17<sup>th</sup> Street in Ft. Lauderdale, Florida. Registration is now open and the ICSJWG is accepting abstracts until July 8<sup>th</sup>. The Call for Abstracts form can be found at <https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>.

This meeting will feature keynote presentations from John Felker, DHS/NCCIC Director of Operations, and Billy Rios, founder of WhiteScope. The 2016 Fall Meeting will also feature the return of a hands-on technical workshop and training focused on Network Monitoring of ICS and Google Hacking/Shodan, an “Ask Me Anything” session with NCCIC/ICS-CERT Director Marty Edwards, and the popular “Viewing Your Network Through the Eyes of an Attacker” session. We’ve also added an ICS Vulnerability Research Panel.

To register for the meeting please go to <https://secure.inl.gov/ics-cert-briefing/?campaignName=ICSJWG%20Fall%202016> and to participate in room block at the Embassy Suites, please go to <http://embassysuites.hilton.com/en/es/groups/personalized/F/FLLSOES-ICS-20160908/index.jhtml>.

Contributed Content Disclaimer: *The advice and instructions provided in the contributed content are provided as is, with no warranties, and should be confirmed and tested prior to implementation.*

## ***The Stakeholders Have Spoken: NIST to Refine Cybersecurity Framework***

The National Institute of Standards and Technology (NIST) is developing a minor update of its [Cybersecurity Framework](#) based on feedback from its users. In the just released [Cybersecurity Framework Feedback: What We Heard and Next Steps](#), NIST is announcing that a draft of the update will be published for comment in early 2017. For more information, please go to <http://www.nist.gov/itl/csd/the-stakeholders-have-spoken-nist-to-refine-cybersecurity-framework.cfm>.

## ***Training for Building Control Systems Professionals***

*By: Michael Chipley*

The PMC Group, in conjunction with the National Institute of Building Sciences, is pleased to offer three courses in cybersecurity. These courses, offered once per quarter, will be available in July and October 2016. These courses are now included in the National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog. For more information on the specific course descriptions, [please click here](#).

## ***Core Principles of an ICS Cybersecurity Program***

*By: Krish Sridhar, Business Manager – Industrial Cybersecurity, aeSolutions*

The design and implementation of Industrial Control Systems (ICS) cybersecurity program poses significant challenges due to the stringent requirements of a manufacturing plant and how control systems and their networks are engineered, operated and maintained. While industry has made significant strides in gaining awareness and applying resources to address these requirements, many organizations have also come to realize that implementing cybersecurity measures in the ICS environment – also referred to as Operations Technology or OT, is challenging and quite different from implementing cybersecurity in the enterprise IT environment. Many of the concepts proven and accepted in enterprise IT are either too difficult and/or complex to execute or simply not relevant to the operating environment. Guidance provide by the NIST framework and other publications are helpful to getting started, and experience also dictates that there are a core set of cybersecurity elements for the ICS environment that must be done right. This paper highlights the uniqueness of the ICS environment and offers core principles for a successful development and launch of an ICS cybersecurity program. [Full article available here](#).

### **Contact ICS-CERT**

Website: <http://ics-cert.us-cert.gov/>

Email: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) or [icsjwg@hq.dhs.gov](mailto:icsjwg@hq.dhs.gov)

Phone: 1-877-776-7585

ICS-CERT publishes alerts and advisories to provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks and current security issues, vulnerabilities, and exploits. These notifications are available on the ICS-CERT website under Information Products or via GovDelivery.

If you have a question regarding these products and what they mean for your organization, please contact ICS-CERT at [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov). If you have an ICS incident or software vulnerability to report, please go to <http://ics-cert.us-cert.gov> and scroll to the bottom of the page to the “I Want To” selections. Additional online reporting information is available at <http://www.dhs.gov/report-cyber-risks> and at the bottom of the ICS-CERT Webpage. ICS-CERT will protect and anonymize your information and only share the technically relevant information with partners that have a need to know.