



**Homeland  
Security**

# ICS-CERT MONITOR

## Contents

Incident Response Activity  
Onsite Assessment Summary  
Situational Awareness  
ICS-CERT News  
Recent Product Releases  
Open Source Situational  
Awareness Highlights  
Coordinated Vulnerability Disclosure  
Upcoming Events

## National Cybersecurity and Communications Integration Center

### ICS-CERT

This is a publication of the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT). ICS-CERT is a component of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). ICS-CERT coordinates control systems-related security incidents and information sharing with federal agencies; state, local, tribal, and territorial governments; and control systems owners, operators, and vendors to reduce the risk of cyber attack against the Nation's critical infrastructure.

This issue and past issues of the ICS-CERT Monitor can be found here: <https://ics-cert.us-cert.gov/monitors>

### Contact Information

For questions related to this report or to contact ICS-CERT:

NCCIC/ICS-CERT Operations Center  
Toll Free: 1-877-776-7585  
International: 1-208-526-0900  
Email: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov)  
Web site: <http://ics-cert.us-cert.gov>

[Report an ICS incident to ICS-CERT](#)

[Report an ICS software vulnerability](#)

[Get information about reporting](#)

### Joining the Secure Portal

ICS-CERT encourages US asset owners and operators to join the Control Systems Compartment of the US-CERT secure portal to receive up-to-date alerts and advisories related to industrial control systems (ICS) cybersecurity. To request a portal account, send your name, telephone contact number, email address, and company affiliation to [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

### Downloading PGP/GPG Keys

[ICS-CERT PGP](#) [Pub](#) [Key.asc](#)

## Incident Response Activity

### Information Sharing

An asset owner contacted ICS-CERT to report a possible "hit" on an indicator of compromise after the release of an alert on the US-CERT Portal. The alert included a number of indicators, which the asset owner used to scan its internal networks. This produced a partial match to an indicator. A single system was quarantined, and a forensic image was sent to ICS-CERT for analysis. As part of the internal forensic investigation, the asset owner asked the user if the system had been exhibiting any suspicious activity. Fortunately, the analysis of the drive image did not show evidence of compromise, and the user reported no suspicious activity.

Good logging and regular network scanning were key in identifying this as a false-positive. Being a member of the US-CERT Portal provides advanced notice of vulnerability mitigation information and makes indicators of compromise available to asset owners. Having a plan that outlines how to respond to suspicious network activity, in addition to contacting ICS-CERT, allowed the asset owner to mitigate this issue quickly. If you are an asset owner or operator of critical infrastructure and would like access to the Control Systems compartment of the US-CERT Portal, please send an email to [ICS-CERT@hq.dhs.gov](mailto:ICS-CERT@hq.dhs.gov) from a company email address and request an invitation.

**Having a plan that outlines how to respond to suspicious network activity, in addition to contacting ICS-CERT, allowed the asset owner to mitigate this issue quickly.**



This product is provided "as is" for informational purposes only. DHS does not provide any warranties of any kind regarding any information contained herein. DHS does not endorse any commercial product or service referenced in this publication or otherwise.

## Onsite Assessments Summary

# ICS-CERT Assessment Activity for September/October 2015

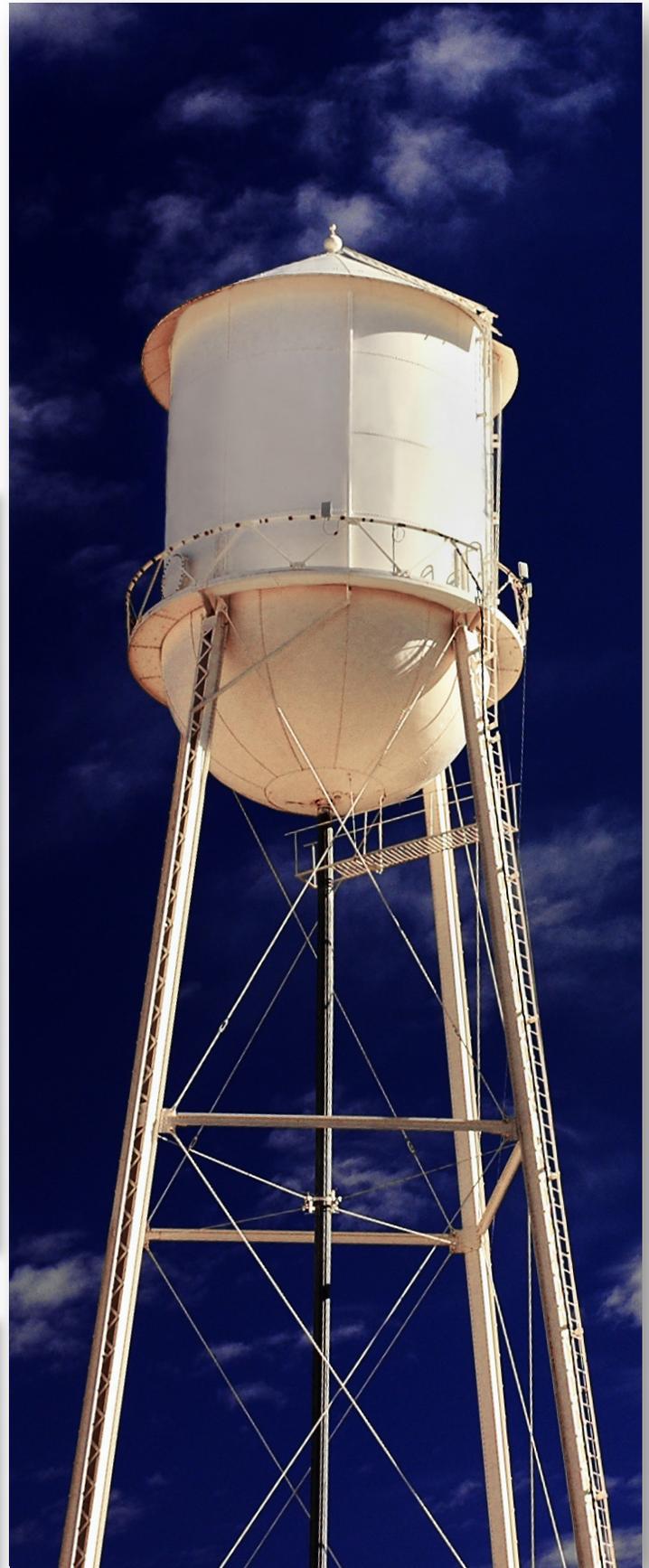
ICS-CERT conducts onsite cybersecurity assessments of industrial control systems (ICSs) to help strengthen the cybersecurity posture of critical infrastructure owners and operators and of ICS manufacturers. In September/October 2015, ICS-CERT conducted 13 onsite assessments across five sectors (Table 1). Of these 13 assessments, two were Cyber Security Evaluation Tool (CSET®) assessments, six were Design Architecture Review (DAR) assessments, and five were Network Architecture Verification and Validation (NAVV) assessments (Table 2). For detailed information on ICS-CERT's CSET, DAR, and NAVV assessments, go to <https://ics-cert.us-cert.gov/assessments>.

Table 1. Assessments by sector, September/October 2015.

Assessments by Sector	September 2015	October 2015	September/October Totals
Chemical			
Commercial Facilities			
Communications			
Critical Manufacturing		2	2
Dams			
Defense Industrial Base			
Emergency Services			
Energy	2	3	5
Financial Services			
Food and Agriculture			
Government Facilities		2	2
Healthcare and Public Health			
Information Technology	1		1
Nuclear Reactors, Materials, and Waste			
Transportation Systems			
Water and Wastewater Systems		3	3
<b>Monthly Totals</b>	<b>3</b>	<b>10</b>	<b>13 Total Assessments</b>

Table 2. Assessments by type, September/October 2015.

Assessments by Type	September 2015	October 2015	September/October Totals
CSET		2	2
DAR	2	4	6
NAVV	1	4	5
<b>Monthly Totals</b>	<b>3</b>	<b>10</b>	<b>13 Total Assessments</b>



### Trends in Malware

By ICS-CERT's Advanced Analytical Laboratory (AAL)

Over the past decade, software has grown and adapted to new environments at an incredible pace. Advancements in technology, from traditional personal computers (PCs) to mobile devices and smart appliances, have substantially changed how we interact with the connected world. As these new technologies emerge, malware authors have intently watched and adapted to the new vectors of attack made available to them.

With the monumental growth in attack vectors and individual online presence, vulnerability discovery and system exploitation have become irresistible to threat actors from nearly every perspective, including criminal, nation-state, and offensive activism. With each new perspective involved in the creation of malicious applications, the functionality and variations of malware are in constant flux. Researchers classify these varieties based on functionality (Trojans, Backdoors, Spyware, etc.). Over time, attackers reveal new categories to the known classifications through previously unseen tactics or begin to leverage older techniques with newly discovered vulnerabilities.

Ransomware, such as Cryptolocker or TeslaCrypt, is currently one of the most prolific categories of malware growth, rising 165 percent in varieties seen between the fourth quarter of 2014 and the first quarter of 2015. Malware in this category obstructs victims' access to their device, often through the encryption of files with a key accessible only to the

attacker. The malware then displays a message containing demands for the release of the system or files, which is typically payment via some form of cryptocurrency or untraceable prepaid card. The victim is given a period of time, as defined by the attacker, to comply with the ransom demands or face loss of system or files.

This strategy exemplifies the concept of "crimeware"—malware engineered to steal user account information, valuable personal information, or money. This type of malware is aimed squarely at consumers, particularly their personal financial information. In addition to ransomware, this type of attack can be seen with point of sale (PoS) malware, which is designed to steal credit card numbers and PINs.



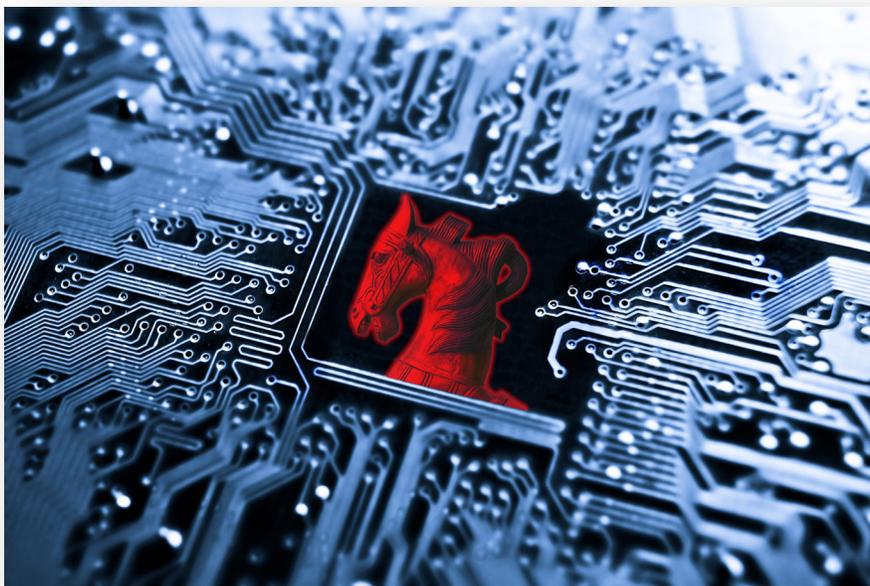
The rising prevalence of malware and increasingly intricate tactics have spurred anti-malware researchers to become more aggressive in locating and identifying malware. This, in turn, has driven attackers to more advanced mechanisms of persistence and secrecy.

Every device that connects to a computer runs low-level code to provide the control needed for the device to communicate as expected. This code, known as the device firmware, is generally trusted implicitly by the device owner and the devices with which it communicates. Malware residing at this level—such as the firmware level in USB devices, the firmware of hard drives, or the Basic Input-Output System (BIOS)

of PCs—creates new and difficult challenges for system security because of the trust models that were designed into these devices' standards. As anti-malware research continues to advance, some of these inherent issues have been addressed, but they remain a high concern that has not yet been solved.

As the variety of attacks and target space of new devices and platforms expand, the amount of valuable information for attackers grows as well. More information is being generated about everyone in the connected world than ever before. Social networking, media consumption, transitions to electronic records, online banking, electronic billing, and countless other common online behaviors generate a massive amount of information that attackers could potentially use against their victims.

This information, exchanged electronically both on and offline, is a double-edged sword. Many of the great aspects of current technology are made possible by customization and by the adapta-



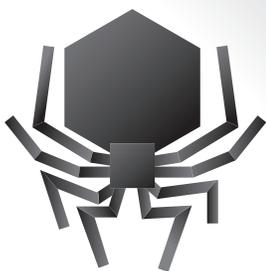
tion of devices to our personal needs. However, this same information in the wrong hands can generate a much more effective attack. Spear-phishing campaigns designed to encourage users to download malware through email attachments or links are much more effective in situations where the attackers are able to craft a personalized email with strong knowledge of their victim. Reconnaissance is still one of the biggest areas of focus for malware authors targeting corporate or nation-state networks and devices. Most of the attacks on these organizations throughout the past several years contain an information collection component with a varying array of functionality. Anything from keylogging to file and system monitoring can be of great value to an attacker in these environments.



The trend of connectivity continues with devices such as smartphones, connected automobiles, and Internet of Things (IoT) devices (i.e., connected appliances, thermostats, cameras). Each of these connected devices is a relative newcomer in our lives, and each has become a major source of new data and a new potential target for exploitation. In the case of mobile devices, operating systems, such as Android and IOS, use system design techniques to avoid many of the security concerns found in traditional PCs. However, this relief is temporary and will only last as long as it takes for attackers to learn the new mobile playing field and find any loopholes.

Until recently, these devices were not prevalent enough to draw a large amount of malicious attention when compared to the wealth of information stored on traditional PCs. This is changing with the rapid increase in sales of mobile devices. As of April 2015, [64 percent](#) of American adults own smartphones, compared to 35 percent in 2011. During this time, we have seen a corresponding increase in malware targeted at mobile devices. The number of new malware samples found on Android devices has increased over time at an alarming rate, with a [27 percent](#) increase in volume in the second quarter of 2015 over the first quarter of 2015 alone.

This advancement is much more visible in the consumer market, but it has had an impact on systems around the world. Critical infrastructure systems may appear isolated from mobile and IoT devices; but from an attacker's perspective, there are many [crossovers](#) and [similarities](#). As mobile operating systems have grown in prevalence, solutions for the management of ICS components through apps made for these operating systems have become a hot topic for both [existing](#) and [emerging](#) companies, expanding the scope of vulnerabilities in mobile operating systems into the ICS world.



These new consumer devices, as well as the comparatively ancient ICSs, are relatively new targets for those looking to exploit and for those seeking to protect, providing new challenges across the board. When many ICS devices were created, security was not widely considered to be an issue. This is not surprising. Many of these devices predate the widespread availability of the Internet, especially in the case of remote management. As such, these devices were never intended to be networked out of the facilities in which they were placed. Security came not from the system being hardened but by the authentication of users gaining physical access.

Isolated ICSs became a difficulty as businesses expanded; technicians and engineers needed access to the devices from increasingly diverse locations to prevent downtime. This had many ramifications for ICS device security. Many networks supporting ICS administration were made to allow easy communication with the devices, and some were never revised when new security concerns and solutions came along.

This easy accessibility for technicians also means that many ICS machines are accessible through standard corporate connected machines and sometimes even the Internet directly. ICSs provide a particularly enticing target for both nation-state and hacktivist threat actors because of how deeply the surrounding communities depend on them. Since the news of Stuxnet in 2010, there has been a notable increase in new malware targeting ICS environments around the world.



So what can be done about all this? The best approach for users is the same as it's been in the past: think before you act and employ [good security practices](#). New pieces of software should only be downloaded from trusted sources. Hardware on corporate networks should be used exclusively in that environment, with policy preventing outside devices from being connected.

In the [July/August 2015 issue of the ICS-CERT Monitor](#), we discussed the importance of logging and of being aware of unusual activity on systems and networks. The same principle applies here—especially in the case of corporate and nation-state environments. Administrators must be aware of unusual activity on their networks and devices in order to take appropriate action. As the activity from malware authors has increased over the years, vendors have responded by putting a great deal of focus on patches. Regular system updates, avoiding suspicious sites, reporting of suspicious emails or messages to network administrators, strong credentials, and careful IT monitoring and management will go a long way toward preventing infection and keeping both personal and corporate devices safe.

## When End-of-Life is Not End-of-Use

From the Spring 2015 Industrial Control Systems Joint Working Group (ICSJWG) presentation by ICS-CERT's Steven Tom

Most companies have end-of-life policies for sensitive electronic equipment. But do these companies have procedures to instruct personnel what to do with sensitive electronic equipment at end-of-life? Do your personnel know and understand what sensitive electronic equipment is and what might be the vulnerable components that contain sensitive data? Would they know what to do with this equipment to make sure it is sanitized or reset to true factory settings?

All very good questions, especially in light of a test conducted last fall by researchers K. Reid Wighman of Digital Bond, Chris Sistrunk of Mandiant, and Michael Toecker of Context Industrial Security. These researchers found some used SCADA servers on eBay, purchased them to see what they could get, and volunteered to share the information they found with ICS-CERT.

For less than \$20, the researchers obtained operational servers containing configuration files, single line diagrams and other data files, protected with weak or no passwords. The previous company's name and system administrators name were also found on physical tags attached to the casing.

With a little Internet searching, ICS-CERT discovered the organizational chart of personnel at that company and information identifying operational substations. ICS-CERT then proceeded to contact this company, and the manager of the identified system administrator, with the purpose of finding out how it was possible that this equipment was available on eBay. This equipment could have been stolen and their sensitive information could have been made publicly available. ICS-CERT was told that the company recently upgraded its equipment and followed its end-of-life policy. The company stated it sanitized its sensitive equipment at its bone yard before being sent away and expressed surprise that all the data files were intact. The company did not have specific sanitizing procedures, just the end-of-life policy.



Many organizations in many of the 16 critical infrastructure sectors have end-of-life policies. However, these policies must be specific and complete and must give personnel a chance to properly do their job. Here are some specific items that should be spelled out in a quality end-of-life policy:

- Identify what equipment is considered sensitive and why. Provide examples of electronic equipment such as computers, servers, industrial controllers, printers, Blackberry and cell phones, Ethernet switches, firewalls, and intrusion detection devices. Any device that a person can “update” from a web site will contain sensitive information in the form of configuration data, access data, user names, passwords, network loops, latch routines, and alarm settings to name a few.
- Provide pictures of each item. Several industrial servers do not have monitors and keyboards like normal business computers and may not look like a server.
- Identify how to remove your configuration information, your backup passwords, and how to return your equipment to factory settings.
- Instruct personnel to read the manual for each piece of equipment. Some equipment, such as servers or Ethernet switches, have multiple procedures to remove and sanitize configurations, remove maintenance passwords, and remove user names and passwords.
- Remove all removable electronic media, thumb drives, memory chips/devices, etc.
- Remove all batteries and short out the battery containers to bleed capacitive memory devices.
- Remove hard drives.
- Sponsor a university doing research in industrial control security and donate your old equipment to them with the provision they notify you if any sensitive data are found. This may provide benefits in growing your own future security force.

Following these guidelines and creating specific and complete end-of-life policies will help ensure that your sensitive information stays protected when your equipment's end-of-life is not end-of-use.

## John Felker Named NCCIC Director of Operations

In August, Department of Homeland Security (DHS) Secretary Jeh C. Johnson named John Felker as Director of Operations for the National Cybersecurity and Communications Integration Center (NCCIC), with responsibility for day-to-day NCCIC operations.

Prior to joining DHS, Felker served as Director of Cyber and Intelligence Strategy for HP Enterprise Services. During a 30-year career in the U.S. Coast Guard, Felker served, among other positions, as Deputy Commander of Coast Guard Cyber Command, where he was responsible for the day-to-day staff leadership and also for the stand-up of the Command. He also commanded the U.S. Coast Guard Cryptologic Group, which spanned subordinate units from Hawaii to Afghanistan performing signals intelligence missions and developing Coast Guard signals intelligence capability. Felker also served as executive assistant to the Director of Coast Guard Intelligence, where he coordinated



director activities within the National Intelligence Community management enterprise.

His military awards include the Defense Superior Service Medal, the Legion of Merit and the Meritorious Service Medal. Felker graduated from Ithaca College with a Bachelor of Science in

1978 and earned his Master of Arts in Public Administration from the Maxwell School of Citizenship and Public Affairs at Syracuse University in 1995.

The move comes as part of Secretary Johnson's decision to elevate NCCIC within the DHS structure because of the importance of its cybersecurity mission. The NCCIC is the U.S. Government's 24/7 hub for cybersecurity information sharing, incident response, and coordination. As part of that decision, Dr. Andy Ozment will remain as the Assistant Secretary of the Office of Cybersecurity and Communications (CS&C) and assume direct responsibility for NCCIC as the NCCIC Director. Brigadier General (retired) Greg Touhill remains as Deputy Assistant Secretary of CS&C.

Secretary of CS&C.

## ICS-CERT at DEF CON and Black Hat

The Black Hat and DEF CON security conferences have become enormously popular as the interest in information security and cyber physical systems continues to boom. The number of attendees for DEF CON alone exceeded 20,000 people, with attendance at Black Hat exceeding an estimated 11,000 attendees. ICS-CERT team members attended both early-August conferences, as in previous years, to follow trends in the research community, interface with researchers, provide ICS demonstrations, and to be ready to respond to unanticipated vulnerability disclosures.

Both conferences hosted technical presentations that covered topics in exploiting weaknesses in ICSs, medical devices, and satellite communications, to name a few. Presentations were similar to

academic presentations. While the entertainment value was high at these events, so was the value of security information and professional contacts gained.

During the course of these conferences, ICS-CERT team members met with numerous researchers to better understand their current

research objects and future objectives. These face-to-face interactions help ICS-CERT to better understand and address relevant security trends. ICS-CERT personnel also attended presentations to identify and respond to unanticipated vulnerability disclosures. This year alone, ICS-CERT took action to address concerns raised in a dozen presentations, resulting in six ICS-CERT alerts about vulnerabilities in multiple ICS products. This level of situational awareness

helps ensure that potential threats to critical infrastructure can be responded to rapidly, with as much real-time information as possible. In addition, ICS-CERT uses these conferences to interact with IT and ICS vendors to learn more about their products and to foster and strengthen relationships. For these conferences, ICS-CERT team members put together the popular ICS Village, which provides insights into the operation of ICSs and helps stimulate dialog about responsible disclosure and security.

ICS-CERT's attendance and participation at these conferences

enhances situational awareness and facilitates community engagement. Coordination with cybersecurity researchers and ICS product vendors at these conferences helps ICS-CERT to further its mission of building a long-term common vision of effective risk management and cybersecurity for ICSs.



## Section 508 and Accessibility

### Making information available to everyone, regardless of physical challenges

Congress amended the 1973 Rehabilitation Act in 1986, adding Section 508, Electronic and Information Technology. Section 508 (S508) requires that the Federal Government provide equal access for all citizens to electronic and information technology (including published documents and web site content), regardless of any physical limitations on the part of any citizen.

Within the National Cybersecurity and Communications Integration Center (NCCIC), ICS-CERT has developed a Section 508 Compliance Plan that guides the ICS-CERT Production Group when developing ICS-CERT products. The ICS-CERT S508 Plan addresses two major areas: released products (Word, and PDF files for web, portal, or other distribution); and web site content (HTML, Flash).

DHS Office of Accessible Systems and Technology (OAST) has developed testing procedures for confirming the accessibility of web site content (HTML pages, embedded software, etc.), Word documents (.doc; .docx), and PDF documents (.pdf).

DHS OAST also provides training to certify S508 Trusted Testers within the various components of the agency. Several ICS-CERT personnel have attended the OAST S508 Trusted Tester training.

As ICS-CERT proceeds with product testing, the ICS-CERT Production Group has begun the remediation process, when possible, to improve accessibility of individual documents posted on the ICS-CERT web site and in the Control Systems Center of the US-CERT secure portal.

Meanwhile, the ICS-CERT Production Group is also actively engaged in revising internal processes and procedures to integrate S508 compliance in the product development process. ICS-CERT's goal is to routinely produce compliant (accessible) products as our normal output from a process that is transparent to our users.

Compliance with Section 508 requirements is not as much a destination as a continuous journey. ICS-CERT is committed to the overall DHS effort to make all information accessible to all citizens, regardless of physical challenges.

With the formal S508 Compliance Plan in place, ICS-CERT has begun a significant course correction related to product development. Most external users will not see much difference in our products. However, persons who employ assistive technologies to access our products should begin to see an improvement in the accessibility of those products.

## ICS-CERT Virtual Learning Portal Upgrade

The ICS-CERT training program upgraded the existing Virtual Learning Portal (VLP) in August 2015. The VLP is an online application for the administration, documentation, tracking, reporting, and delivery of training courses. This upgrade better aligns the program with the federal guidelines for cloud-based applications, improves the graphical user interface (GUI), and reduces operational costs.

In conjunction with the upgrade, the existing online course titled "Cybersecurity for Industrial Control Systems (210W)" was separated into 10 individual courses. Those courses are now as follows:

- Differences in Deployments of ICS (210W-01)
- Influence of Common IT Components on ICS (210W-02)
- Common ICS Components (210W-03)
- Cybersecurity within IT and ICS Domains (210W-04)
- Cybersecurity Risk (210W-05)
- Current Threat Trends in ICS (210W-06)
- Current Vulnerability Trends in ICS (210W-07)
- Determining the Impacts of a Cybersecurity Incident (210W-08)
- Attack Methodologies in IT and ICS (210W-09)
- Mapping IT Defense-In-Depth Security Solutions to ICS (210W-10).

For the most comprehensive training, students should take the courses in order, 210W-01 through 210W-10, but this change in format allows for the creation of custom learning paths for industry professionals.

# Industrial Control Systems Joint Working Group Meetings

## Fall 2015 Meeting Recap

The Industrial Control Systems Joint Working Group (ICSJWG) 2015 Fall Meeting was held at the Coastal Georgia Center in downtown Savannah, Georgia, on October 27–29, and brought together approximately 200 stakeholders from the ICS community. The Meeting included 2 ½ days of interactions and discussions through keynote speakers, practical demonstrations, presentations, panels, lightning round talks, and non-classified briefings. Highlights from the 2015 Fall Meeting include the following:

- Feature presentations from Director of the NCCIC John Felker, President of the Technology Association of Georgia Tino Mantella, Independent Security Researcher Marina Krotofil, and Robert Lee from the SANS Institute
- ICSJWG’s first ever Vendor Expo
- The ICS Village, which included a replica of a typical water plant network setup with hands-on isolated industrial equipment stations
- “Ask Me Anything” session with representatives from NCCIC/ICS-CERT
- Break-out/networking session exclusively for our international partners.

## Spring 2016 Meeting

The planning phase for the ICSJWG Spring 2016 meeting is underway. When available, information and registration will be posted here: <https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>.

## ICS-Cybersecurity for the C-Level

ICS-CERT, with direction from the ICSJWG, created a new document, “ICS Cybersecurity for the C-Level,” in response to growing demand from stakeholders for a concise document that can effectively communicate the need for better ICS cybersecurity practices to the C-Level. This document aims to support that need by providing a succinct overview of basic cybersecurity principles and best practices for ICS-related organizations.

This document provides information regarding two sophisticated malware campaigns, describes key ICS cybersecurity questions and risk management concepts, and details specific services and activities that ICS-CERT can provide to help improve the cybersecurity of the Nation’s critical infrastructure.

## NCCIC/ICS-CERT in the News

An interview with Dr. Andy Ozment, Assistant Secretary of DHS’s Office of Cybersecurity and Communications (CS&C) and NCCIC Director:

<http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Where-Next-for-Government-Cybersecurity.html>

Article by ICS-CERT Director Marty Edwards for Control Design:

<https://www.controldesign.com/articles/2015/u-s-government-resources-for-cybersecurity/>

ICS-CERT Director Marty Edwards quoted in article on medical device cyber security:

<http://breakthroughs.kera.org/smart-medical-devices-call-for-smarter-cyber-security/>

## Recent Product Releases

### Alerts

[ICS-ALERT-15-288-01](#) SDG Technologies Plug and Play SCADA XSS Vulnerability, 10/15/2015.

### Advisories

[ICSA-15-300-01](#) Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability, 10/27/2015.

[ICSA-15-300-02](#) Infinite Automation Systems Mango Automation Vulnerabilities, 10/27/2015.

[ICSA-15-300-03](#) Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities, 10/27/2015.

[ICSA-15-265-03](#) Janitza UMG Power Quality Measuring Products Vulnerabilities, 10/22/2015.

[ICSA-15-293-01](#) IniNet Solutions embeddedWebServer Cleartext Storage Vulnerability, 10/20/2015.

[ICSA-15-293-02](#) IniNet Solutions SCADA Web Server Vulnerabilities, 10/20/2015.

[ICSA-15-293-03](#) 3S CODESYS Gateway Null Pointer Exception Vulnerability, 10/20/2015.

[ICSA-15-288-01](#) 3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability, 10/15/2015.

[ICSA-15-286-01](#) Nordex NC2 XSS Vulnerability, 10/13/2015.

[ICSA-15-274-01](#) Omron Multiple Product Vulnerabilities, 10/1/2015.

[ICSA-15-272-01](#) Honeywell Experion PKS Directory Traversal Vulnerability, 9/29/2015.

[ICSA-15-146-01](#) Mitsubishi Electric MELSEC FX-Series Controllers Denial of Service, 9/29/2015.

[ICSA-15-181-01](#) Baxter SIGMA Spectrum Infusion System Vulnerabilities, 9/29/2015.

[ICSA-15-267-01](#) Endress+Hauser Fieldcare/CodeWrights HART Comm DTM XML Injection Vulnerability, 9/24/2015.

[ICSA-15-237-02](#) EasyIO-30P-SF Hard-Coded Credential Vulnerability, 9/24/2015.

[ICSA-15-237-02-Supplement](#) Supplement to ICSA-15-237-02 EasyIO-30P-SF Hard-Coded Credential Vulnerability, 9/24/2015.

[ICSA-15-265-01](#) Resource Data Management Privilege Escalation Vulnerability, 9/22/2015.

[ICSA-15-265-02](#) IBC Solar ServeMaster Source Code Vulnerability, 9/22/2015.

[ICSA-15-232-01](#) Everest Software PeakHMI Pointer Dereference Vulnerabilities, 9/22/2015.

[ICSA-15-260-01](#) Harman-Kardon Uconnect Vulnerability, 9/17/2015.

[ICSA-15-258-01](#) Schneider Electric StruxureWare Building Expert Plaintext Credentials Vulnerability, 9/15/2015.

[ICSA-15-258-02](#) 3S CODESYS Gateway Server Buffer Overflow Vulnerability, 9/15/2015.

[ICSA-15-258-03](#) GE MDS PulseNET Vulnerabilities, 9/15/2015.

[ICSA-15-258-04](#) Advantech WebAccess Stack-Based Buffer Overflow Vulnerability, 9/15/2015.

[ICSA-15-253-01](#) Yokogawa Multiple Products Buffer Overflow Vulnerabilities, 9/10/2015.

[ICSA-15-251-01A](#) Advantech WebAccess Buffer Overflow Vulnerability, 9/8/2015.

[ICSA-15-246-01](#) Cogent DataHub Code Injection Vulnerability, 9/3/2015.

[ICSA-15-246-02](#) Schneider Electric Modicon PLC Vulnerabilities, 9/3/2015.

[ICSA-15-246-03](#) Moxa Industrial Managed Switch Vulnerabilities, 9/3/2015.

[ICSA-15-181-02A](#) SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability, 9/3/2015.

[ICSA-15-244-01](#) Siemens RUGGEDCOM ROS IP Forwarding Vulnerability, 9/1/2015.

## Other

[Six Questions Every C-Level Executive Should Be Asking](#), 9-16-15.

## Open Source Situational Awareness Highlights

### Why Aren't There Better Cybersecurity Regulations for Medical Devices?

2015-10-19

<http://motherboard.vice.com/read/why-arent-there-better-cybersecurity-regulations-for-medical-devices>

### 10 Basic Cybersecurity Measures

2015-10-14

<https://ics-cert.us-cert.gov/10-Basic-Cybersecurity-Measures>

### A New Defense for Navy Ships: Protection from Cyber Attacks

2015-09-18

[http://www.ecnmag.com/news/2015/09/new-defense-navy-ships-protection-cyber-attacks?et\\_cid=4823349&et rid=745317555&location=top](http://www.ecnmag.com/news/2015/09/new-defense-navy-ships-protection-cyber-attacks?et_cid=4823349&et rid=745317555&location=top)

## Coordinated Vulnerability Disclosure

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) or toll free at 1 877 776 7585.

## Researchers Assisting ICS-CERT with Products Published September/October 2015

ICS-CERT appreciates having worked with the following researchers:

### Advisories

- David Formby and Raheem Beyah of Georgia Tech, ICSA-15-300-01 Siemens RuggedCom Improper Ethernet Frame Padding Vulnerability, 10/27/2015.
- Steven Seeley of Source Incite and Gjoko Krstic of Zero Science Lab, ICSA-15-300-02 Infinite Automation Systems Mango Automation Vulnerabilities, 10/27/2015.
- Ilya Karpov of Positive Technologies, David Atch of CyberX, and independent researcher Aditya Sood, ICSA-15-300-03 Rockwell Automation Micrologix 1100 and 1400 PLC Systems Vulnerabilities, 10/27/2015.
- Mattijs van Ommereen of Applied Risk, ICSA-15-265-03 Janitza UMG Power Quality Measuring Products Vulnerabilities, 10/22/2015.
- Aleksandr Timorin of Positive Technologies, ICSA-15-293-01 IniNet Solutions embeddedWebServer Cleartext Storage Vulnerability, 10/20/2015.
- Kirill Nesterov and Aleksandr Timorin of Positive Technologies, ICSA-15-293-02 IniNet Solutions SCADA Web Server Vulnerabilities, 10/20/2015.
- Ashish Kamble of Qualys, Inc., ICSA-15-293-03 3S CODESYS Gateway Null Pointer Exception Vulnerability, 10/20/2015.
- Nicholas Miles of Tenable Network Security, ICSA-15-288-01 3S CODESYS Runtime Toolkit Null Pointer Dereference Vulnerability, 10/15/2015.
- Karn Ganeshen, ICSA-15-286-01 Nordex NC2 XSS Vulnerability, 10/13/2015.
- Stephen Dunlap of Air Force Institute of Technology, ICSA-15-274-01 Omron Multiple Product Vulnerabilities, 10/1/2015.
- Joel Langill, ICSA-15-272-01 Honeywell Experion PKS Directory Traversal Vulnerability, 9/29/2015.
- Ralf Spenneberg of OpenSource Security, ICSA-15-146-01 Mitsubishi Electric MELSEC FX-Series Controllers Denial of Service, 9/29/2015.
- Jared Bird with Allina IS Security, ICSA-15-181-01 Baxter SIG-MA Spectrum Infusion System Vulnerabilities, 9/29/2015.
- Alexander Bolshev of Digital Security, ICSA-15-267-01 Endress+Hauser Fieldcare/CodeWrights HART Comm DTM XML Injection Vulnerability, 9/24/2015.
- Maxim Rupp, ICSA-15-237-02 EasyIO-30P-SF Hard-Coded Credential Vulnerability, 9/24/2015.
- Maxim Rupp, ICSA-15-265-01 Resource Data Management Privilege Escalation Vulnerability, 9/22/2015.
- Maxim Rupp, ICSA-15-265-02 IBC Solar ServeMaster Source Code Vulnerability, 9/22/2015.
- Josep Pi Rodriguez, ICSA-15-232-01 Everest Software PeakHMI Pointer Dereference Vulnerabilities, 9/22/2015.
- Chris Valasek of IOActive and Dr. Charlie Miller of Twitter, ICSA-15-260-01 Harman-Kardon Uconnect Vulnerability, 9/17/2015.
- Artyom Kurbatov, ICSA-15-258-01 Schneider Electric StructureWare Building Expert Plaintext Credentials Vulnerability, 9/15/2015.
- HP's Zero Day Initiative (ZDI), ICSA-15-258-02 3S CODESYS Gateway Server Buffer Overflow Vulnerability, 9/15/2015.
- ZDI, ICSA-15-258-03 GE MDS PulseNET Vulnerabilities, 9/15/2015.
- Ivan Sanchez from Nullcode Team, ICSA-15-258-04 Advantech WebAccess Stack-Based Buffer Overflow Vulnerability, 9/15/2015.
- Praveen Darshanam, ICSA-15-251-01A Advantech WebAccess Buffer Overflow Vulnerability, 9/8/2015.
- Aditya K. Sood, ICSA-15-246-02 Schneider Electric Modicon PLC Vulnerabilities, 9/3/2015.
- Erwin Paternotte of Applied Risk, ICSA-15-246-03 Moxa Industrial Managed Switch Vulnerabilities, 9/3/2015.
- Aleksandr Timorin of PT Security, ICSA-15-181-02A SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability, 9/3/2015.
- Stephen Craven of the Tennessee Valley Authority, ICSA-15-244-01 Siemens RUGGEDCOM ROS IP Forwarding Vulnerability, 9/1/2015.



Follow ICS-CERT on Twitter: [@icscert](https://twitter.com/icscert)

# Upcoming Events

## December 2015

Industrial Control Systems Cyber-security (301) Training (5 days)

December 7–11

Idaho Falls, Idaho

Course Closed

## January 2016

Industrial Control Systems Cyber-security (301) Training (5 days)

January 11–15

Idaho Falls, Idaho

Course Closed

## February 2016

Industrial Control Systems Cyber-security (301) Training (5 days)

February 8 - 12

Idaho Falls, ID

[Course description and registration](#)

### JANUARY

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

### FEBRUARY

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

### MARCH

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

### APRIL

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

### MAY

Su	Mo	Tu	We	Th	Fr	Sa
				1		
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

### JUNE

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

### JULY

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

### AUGUST

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

### SEPTEMBER

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

### OCTOBER

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

### NOVEMBER

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

### DECEMBER

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

For a current schedule of events that the ICS-CERT is supporting and may be of interest to control system individuals involved in security, go to <https://ics-cert.us-cert.gov/Calendar>.

## We Want to Hear From You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

### Reporting Incidents

Please let us know if you have experienced a cyber intrusion or anomalous activity on your network. Reporting to ICS-CERT is completely voluntary; however, your information is extremely useful for understanding the current threat landscape, including the techniques adversaries are using, types of malware, possible intent of campaigns, and sectors targeted. Prompt and detailed reporting can lead to early detection and prevent incidents from occurring against the nation's critical infrastructure.

Your information will be protected. ICS-CERT's policy is to keep confidential any reported information specific to your organization

or activity. Organizations can also leverage the PCII program to further protect and safeguard their information (<http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program>).

### What is the publication schedule for this newsletter?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT Web page at: <http://ics-cert.us-cert.gov>.

Please direct all questions or comments about the content or suggestions for future content to ICS CERT at: [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov).

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: <https://www.us-cert.gov/forms/feedback>.