NCCIC/ICS-CERT Year in Review

National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team

FY 2015

Homeland Security

What’s Inside

Welcome

NCCIC

With the continued increase in the frequency and sophistication of cyber threats against America's critical infrastructure (CI), the National Cybersecurity and Communications Integration Center's (NCCIC) role as the Nation's 24x7 cyber situational awareness, incident response, and management center grows ever more important.

In 2015, the NCCIC as a whole received 145,566 reports of cybersecurity incidents. Also this year, because of NCCIC's central importance to the Department of Homeland Security's (DHS) cybersecurity mission, DHS Secretary Jeh C. Johnson emphasized the focus upon the NCCIC within the DHS structure. In January, President Barack Obama visited the NCCIC watch floor in Arlington, Virginia, to announce his proposal for new cybersecurity legislation. In August, the NCCIC's third and latest watch floor went operational in Pensacola, Florida.

2015 was clearly a big year for the NCCIC. After the President's speech on the NCCIC watch floor in January, he thanked NCCIC personnel for doing a great job and said, "You are helping to keep the nation safe and secure." I agree. I am proud of the hard work and commitment of the NCCIC team, and I am excited about the opportunity to play a part in the important work they do. We look for ways to be more effective every day, and we count on a continuing dialogue with our partners in government, industry, and the critical infrastructure community to inform that path to effectiveness.

Sincerely,

John Felker, Director of Operations
NCCIC
Department of Homeland Security

ICS-CERT

As time and technology advance, and as Americans increasingly rely on CI to provide many important services, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) continues to pursue its mission to reduce cybersecurity risk to the Nation's CI.

In this 2015 Year in Review, we look back on the accomplishments of ICS-CERT and see continued growth and success. In May, ICS-CERT was announced as runner-up for the 12th Annual U.S. Government Information Security Leadership Awards (GISLA) Community Awareness Award for its Action Campaign to educate CI asset owners about the BlackEnergy and Havex malware threat. This recognition exemplifies the dedication of the ICS-CERT to protecting critical infrastructure.

In FY 2015, ICS-CERT responded to 295 cyber incidents, handled 486 vulnerabilities, performed in-depth analysis on 175 malware samples, conducted 112 assessments, released two new versions of the Cyber Security Evaluation Tool (CSET®), upgraded the Virtual Learning Portal, hosted multiple regional trainings around the country, and hosted two successful Industrial Control Systems Joint Working Group (ICSJWG) meetings in Washington, D.C., and Savannah, Georgia.

As we review ICS-CERT's work at the close of another year, I am once again impressed with the ICS-CERT team and proud of what they have accomplished. As we move forward, ICS-CERT will continue to work toward its mission and defend against whatever new cyber threats the year 2016 brings.

Best regards,

Marty Edwards, Director
ICS-CERT
Department of Homeland Security
ICSJWG Government Coordinating Council (GCC) Chair

NCCIC/ICS-CERT Introduction

The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. The NCCIC vision is a secure and resilient cyber and communications infrastructure that supports homeland security, a vibrant economy, and the health and safety of the American people. The NCCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical information technology and communications networks.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is one of NCCIC's four branches. ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure (CI) by strengthening control systems security and resilience through public-private partnerships. The United States depends on CI to support national defense, public health and safety, economic vitality, and overarching societal well-being. Disruptions or significant damage to CI could result in potentially catastrophic and cascading consequences to the Nation. Presidential Policy Directive-21 (PPD-21) identifies 16 CI sectors (see table below). ICS-CERT works closely with government at all levels and the private sector to coordinate and share capabilities, services, and tools that help control systems owners and operators to prevent, protect against, mitigate, respond to, and recover from cyber threats and incidents. ICS-CERT's activities include four operations functions and four risk reduction functions. Operations functions include watch floor operations (Page 4), incident response (Page 6), vulnerability coordination (Page 7), and technical analysis (Page 8). Risk reduction functions include cybersecurity assessments (Page 10), distribution of the Cyber Security Evaluation Tool (CSET) (Page 11), training (Page 12), and Industrial Control Systems Joint Working Group (ICSJWG) activities (Page 14).

The **NCCIC vision** is a secure and resilient cyber and communications infrastructure that supports **homeland security**, a **vibrant economy**, and the **health and safety** of the American people.

16 Critical Infrastructure Sectors			
Chemical	Dams	Financial Services	Information Technology
Commercial Facilities	Defense Industrial Base	Food and Agriculture	Nuclear Reactors, Materials, and Waste
Communications	Emergency Services	Government Facilities	Transportation Systems
Critical Manufacturing	Energy	Healthcare and Public Health	Water and Wastewater Systems

FY 2015 Highlights and Accomplishments

- **The President on the NCCIC Watch Floor:** On January 13, 2015, the President of the United States visited the NCCIC watch floor to discuss his proposal for new cybersecurity legislation. In his 10-minute speech, the President emphasized that cyber threats pose an enormous challenge to the Nation and highlighted the need for greater trust and information sharing and collaboration between the government and the private sector.
- **ICS-CERT Runner-up for Industry Award:** In May, ICS-CERT was announced as runner-up for the 12th Annual U.S. Government Information Security Leadership Awards (GISLA) Community Awareness Award. ICS-CERT received the runner-up GISLA award for its Action Campaign to educate CI asset owners about the BlackEnergy and Havex malware threat.
- **Incident Response:** In FY 2015, ICS-CERT responded to 295 cyber incidents. This represented a 20 percent increase over FY 2014. The Critical Manufacturing Sector nearly doubled to a record 97 incidents, becoming the leading sector for ICS-CERT in FY 2015. The Energy Sector had the second most incidents with 46 incidents, and the Water and Wastewater Systems Sector was third with 25.
- **Vulnerability Coordination:** ICS-CERT handled 486 vulnerabilities. The vulnerability coordination team also reduced the average number of days to close a ticket from 108 days in 2014 to 55 days in 2015 and closed 76 percent of tickets that have been open over 365 days.
- **Assessments:** ICS-CERT conducted 112 onsite cybersecurity assessments across eight of the 16 CI sectors in 22 states and Washington, D.C. Of these 112 assessments, 38 were CSET assessments, 46 were Design Architecture Review (DAR) assessments, and 28 were Network Architecture Verification and Validation (NAVV) assessments. In August, the assessments team also released its annual report, "Industrial Control Systems Assessments FY 2014 Overview and Analysis."
- **Training:** The ICS-CERT training program upgraded the existing Virtual Learning Portal (VLP) in August 2015. This upgrade better aligns the program with the federal guidelines for cloud-based applications, improves the graphical user interface, and reduces operational costs. The new VLP will also facilitate the program's goal of offering continuing education units.
- **CSET 6.2 and 7.0:** The CSET development team released two new versions of CSET in 2015. The team released CSET 6.2 in January and CSET 7.0 in August. The latest version includes a new interface, new standards, improved functionality, and the ability to encrypt assessments files within CSET. In FY 2015, ICS-CERT distributed 7,565 copies of CSET in 120 countries.
- **NCCIC/ICS-CERT Becomes Operational in Pensacola, Florida:** This year the NCCIC expanded watch floor operations in Pensacola. In August, ICS-CERT reassigned its production chief from Arlington, Virginia, to Pensacola. The senior watch officer began watch operations in Pensacola in September.
- **GovDelivery:** ICS-CERT launched a new digital subscription system with GovDelivery. New subscribers have the capability to go to the website and sign up for ICS-CERT announcements and products, including Alerts, Advisories, Monitor Newsletters, and the Year in Review.

Barry Bahler / DHS Public Affairs

DHS Secretary Jeh Johnson and President Barack Obama on the NCCIC Arlington watch floor.

Watch Floor Operations

NCCIC's watch floor operations are the primary entry point for threat, vulnerability, and incident reporting, as well as classified and unclassified information dissemination from ICS-CERT to its stakeholders. Watch floor operations serve as the operational "traffic cop" between stakeholders and ICS-CERT by ingesting, triaging, and tracking incidents to resolution. Approximately two dozen analysts and incident handlers staff the NCCIC watch floor across three geographically separate watch floor locations. NCCIC maintains watch floor operations capabilities in Idaho Falls, Idaho; Pensacola, Florida; and Arlington, Virginia. The Pensacola watch floor is the newest, becoming operational in August. Arlington watch floor operations are a physically integrated component of and co-located with the primary NCCIC watch floor, while Idaho Falls and Pensacola are networked into NCCIC so that they can assume continuity of operations responsibilities during emergencies.

NCCIC's watch floor operations ensure proper operating tempo, coordinating with other ICS-CERT and NCCIC components, the law enforcement and intelligence community, and other external partners. NCCIC's watch floor operations provide all aspects of incident response services, including digital media analysis and onsite response; recovery and mitigation support; vulnerability coordination and disclosure; and situational awareness alerts and advisories to warn of cyber threats affecting the Nation's CI.

ICS-CERT works closely with Information Sharing and Analysis Centers (ISACs), researchers, vendors, Sector-Specific Agencies (SSAs), industry associations, and other partners across the Nation's 16 CI sectors to coordinate cyber risk reduction efforts. In fact, it is these strong partnerships with key stakeholders across all sectors and government agencies that put ICS-CERT in the unique position of providing clear situational awareness of the threat landscape and associated defensive measures. Timely and accurate information is essential to cybersecurity preparedness.

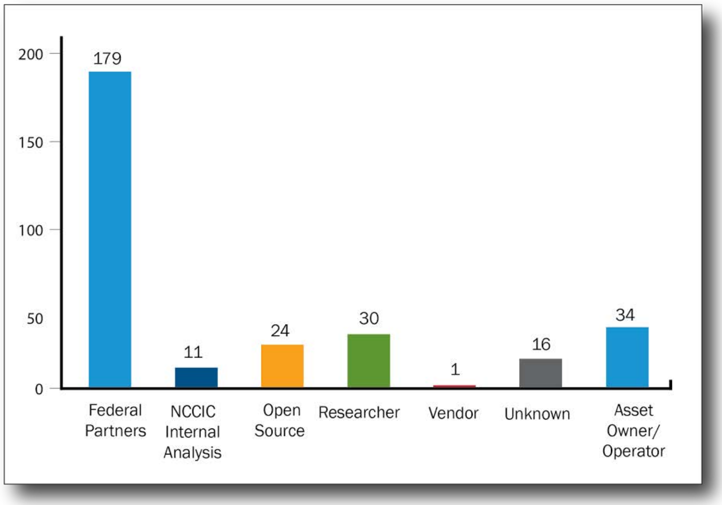
Other core watch operations functions include providing input for briefings to senior government officials; supporting the cybersecurity common operational picture by providing threat information and analysis inputs; and leading operational information management processes, including operation of ICS-CERT's incident management system.

In FY 2015, ICS-CERT continued significant outreach efforts to raise awareness of a sophisticated malware campaign that has compromised several industrial control systems (ICS) environments using a variant of the BlackEnergy malware, named BlackEnergy2. This malware activity has been ongoing since at least 2011, with the most recent activity observed in late September 2014.

ICS-CERT conducted 6 webinars, 200 presentations, and 136 teleconferences for stakeholders to help them understand the threats to CI. At the request of stakeholders, ICS-CERT published and distributed a presentation titled "Current Risks to Industrial Control Systems." Included in the presentation was additional instruction specifically intended to assist recipients in briefing their organization with this information. The presentation is located in our secure portal and was distributed to all SSAs and formally recognized ISACs. The presentation is intended to be shared within stakeholder organizations to raise awareness for control system personnel, information technology personnel, and up to C-Level executives (high-ranking executives, e.g., CEOs, CFOs, COOs).

At this time, DHS has not identified any attempts to damage, modify, or otherwise disrupt any of the BlackEnergy 2 victim systems' control processes. ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised human-machine interface (HMI) into the underlying control system, but the investigation is still ongoing. As of January 2016, open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system. Based on the technical artifacts ICS-CERT and US-CERT have been provided, we cannot confirm a causal link between the power outage with the presence of the malware.

FY 2015 Incidents by Reporting Entity (295 total)



Incident Response

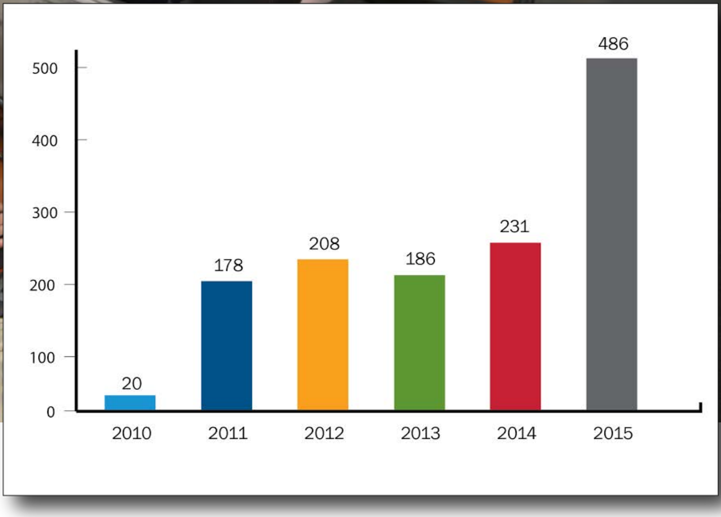
Incident response is fundamental to ICS-CERT's mission to reduce risk to the Nation's CI. The incident response team responds to and helps mitigate cybersecurity incidents impacting ICSs in each of the 16 CI sectors across the United States. At the request of private industry asset owners, ICS-CERT provides incident response services to assess the extent of the compromise, identify the threat actor's techniques and tactics, and assist the asset owner to develop strategies for mitigation, recovery, and improving cyber defenses for the future.

ICS-CERT also collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. The coordination among these partners provides ICS-CERT with a unique perspective of the overall cyber risk landscape and emerging threats. ICS-CERT conveys this information through outreach activities, briefings, and information products, such as alerts and advisories, as well as technical information papers recommending strategies for improving cyber defense.

Every year, new malware families target ICS-specific functionality, underscoring the evolving landscape and the recognition by adversaries of high-stakes ICS targets. ICS-CERT provides onsite incident response support, conducts technical analysis of artifacts and malware, develops mitigation strategies for owners and operators, and provides configuration analysis on new systems to ensure sufficient detection and prevention of the evolving threats.

Incident Response in FY 2015

In FY 2015, ICS-CERT received and responded to 295 incidents. The Critical Manufacturing Sector accounted for 97 of these incidents, while the Energy Sector had 46 and the Water and Wastewater Systems Sector had 25. Spear-phishing represented 37 percent of these incidents, making it the leading access vector for FY 2015 incidents reported to ICS-CERT. Network scanning and probing accounted for 11 percent of ICS-CERT's FY 2015 incidents. Federal partners were once again the leading reporting source for incidents. They reported 179 incidents, which accounted for 61 percent of FY 2015 incidents reported to ICS-CERT. Asset owners were the second largest reporting source with 34 incidents, accounting for 12 percent of incidents reported. Researchers reported 30 incidents, accounting for 10 percent (see Incident Response FY 2015 Metrics on Page 17).



Reported Vulnerabilities, FY 2010 through FY 2015

Vulnerability Coordination

The primary objective of ICS-CERT's vulnerability coordination work is the timely mitigation of vulnerabilities to reduce the likelihood of a successful cyber attack against the Nation's CI. Vulnerability coordination requires technical expertise, documentation, and close trusted partnerships with key ICS community stakeholders, including vendors; manufacturers; integrators; CI owners; researchers; federal, state, and local government organizations; and international partners. ICS-CERT's vulnerability handling process involves five basic steps:

Detection/Collection. The vulnerability team collects vulnerability reports through vulnerability analysis, monitoring of public sources, and direct receipt of vulnerability information. Upon learning of a vulnerability or receiving a report, the team first eliminates duplicates and false alarms and then catalogs each vulnerability.

Analysis. Once the vulnerabilities are catalogued, the vulnerability team and vendor analysts work to understand the vulnerabilities by examining and identifying the issues, as well as the potential threat.

Mitigation Coordination. After analyzing a vulnerability, the team works with the vendor for mitigation and patch issuance. The vulnerability team works with vendors to allow sufficient time to effectively resolve and perform patch regression testing against any given vulnerability.

Application of Mitigation. The vulnerability team works with vendors to allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to disclosure.

Disclosure. After coordinating with vendors and gathering technical and threat information, the team takes the appropriate steps to notify end users about vulnerabilities. ICS-CERT strives to disclose accurate, neutral, objective information, and will reference other available information and correct misinformation when possible.

Vulnerability Coordination in FY 2015

In FY 2015, the ICS-CERT vulnerability coordination team handled 486 vulnerabilities. ICS-CERT reduced the average number of days to close a ticket from 108 days in 2014 to 55 days in 2015 and closed 76 percent of tickets that had been open over 365 days. The vulnerability coordination team gave presentations on two high visibility vulnerabilities at the DEF CON conference held in Las Vegas. The presentations covered the Uconnect Jeep Fiat auto hack and Hospira medical pumps. ICS-CERT released six alerts as a result of its attendance at the DEF CON and Black Hat conferences. The vulnerability team again saw an increase in medical device vulnerabilities. Notably, the team successfully coordinated the release of patches and advisories for medical devices with Baxter, Hospira, and the Food and Drug Administration.

Technical Analysis

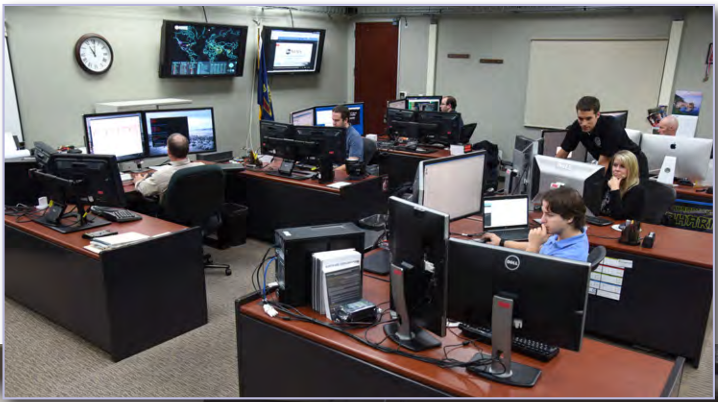
The Advanced Analytical Laboratory (AAL) provides technical analysis in support of ICS-CERT's mission to reduce risk to the Nation's CI. Technical analysis includes all aspects of malware analysis, digital analysis, reverse engineering and longer-term analysis; exploring systemic vulnerabilities and potential future threats, tactics, techniques, and procedures; and more intractable long-term problems.

The AAL also provides research and analysis capabilities in support of the incident response, assessment, and vulnerability coordination activities of ICS-CERT. The AAL's expert cybersecurity researchers can respond to cyber incidents with both onsite and remote capacity. When possible, analytical efforts are performed remotely in a laboratory environment using custom tools and techniques. In some cases, however, onsite analysis is required, and a team is deployed to perform analytical efforts directly on the owner's network.

Technical Analysis in FY 2015

In FY 2015, the AAL performed in-depth analysis on 175 malware samples. This work helped uncover sophisticated threat actor techniques and tactics and allowed ICS-CERT to publish multiple alerts warning the ICS community of the threat and provide information for detecting and mitigating intrusion activity.

Also in FY 2015, the AAL continued to focus on automating and streamlining the lab's analytical capabilities. Initial efforts have begun to shift the AAL's output to a Structured Threat Information Expression (STIX) based format. When completed, this effort will allow the AAL to provide threat information in an automated, machine-readable format that will reduce the amount of time necessary to provide this data to customers.



U.S. DEPARTMENT OF HOMELAND SECURITY
National Cybersecurity &
Communications Integration Center
UNITED WE STAND

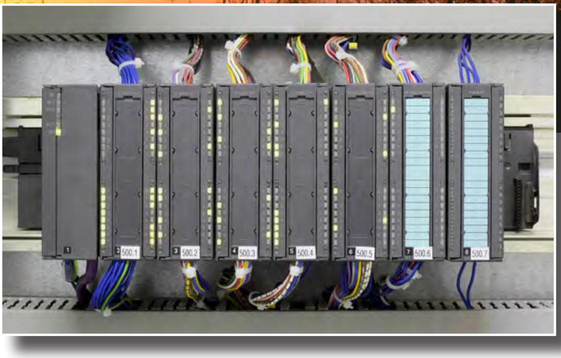
The AAL has continued work on the automation and integration of forensic analysis tools in a suite called the Analyst Network Tool (ANT). ANT brings together custom and commercial forensic tools in an integrated environment, allowing multiple drive images to be processed simultaneously, reducing the amount of analyst hands-on time. ANT has greatly reduced the turnaround time for digital forensic analysis, providing faster results to customers responding to a compromise. The AAL has also begun adding additional capability to meet the growing demand by our customers for our services. This has included hiring additional staff, expanding the physical space where we operate our laboratory, and both adding and prototyping new tools.

Sandia National Laboratory

Sandia National Laboratory (SNL) performs year-round research work and develops prototype tools on behalf of the ICS-CERT. In addition, SNL assists the AAL with malware analysis when requested. SNL's recent efforts have been aimed at developing tools and methods to examine firmware and business logic on programmable logic controllers for signs of tampering and to examine Modbus protocols on the network for out-of-bounds conditions.

Air Force Institute of Technology

For the past five years, the Air Force Institute of Technology (AFIT) has conducted significant research efforts supporting ICS-CERT. As a research-based graduate school, AFIT's contributions for FY 2015 include nine Masters students and one PhD student working toward safer and more reliable industrial control and automation systems. AFIT's highlights for FY 2015 include three journal articles that investigate ICS honeypot development and wireless defenses. Students also presented their work at the 9th Annual International Conference on Critical Infrastructure Protection. Current graduate research is advancing the fields of ICS incident response, cyber insurance models, reverse engineering, wireless vulnerability assessment, and the development of ICS cyber range technology.



Assessments

As a core part of its mission to reduce risk to the Nation's CI, ICS-CERT provides onsite cybersecurity assessments to CI asset owners and operators to strengthen the cybersecurity posture of their ICS. ICS-CERT assessments are based on standards, guidelines, and best practices and are provided to CI asset owners and operators at no cost using our Congressional funding. The assessment methodology provides a structured framework that asset owners and operators can use repeatedly to assess, re-assess, protect, detect, and continually validate the cybersecurity of their ICS networks. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing their cybersecurity posture.

ICS-CERT's onsite cybersecurity assessment services include guided Cyber Security Evaluation Tool (CSET) assessments, Design Architecture Review (DAR) assessments, and Network Architecture Verification and Validation (NAVV) assessments.

CSET is a stand-alone software tool used to conduct cybersecurity assessments (see CSET section on Page 11.) The DAR assessment provides ICS asset owners with a comprehensive evaluation and discovery process, focusing on defense strategies associated with an asset owner's specific control systems network. The DAR includes an in-depth review and evaluation of the control system's network design, configuration, interdependencies, and its applications. ICS-CERT provides a detailed DAR report, and with expert consultation, positions the requesting facility's ICS for improved security and resiliency.

The NAVV assessment provides a sophisticated analysis of network packet-data, which is collected by the asset owners from within their control system network environment. ICS-CERT passively analyzes the data using a combination of open source and commercially available tools, and develops detailed representation of the communications flows and relationships between devices. The NAVV also provides a practical method for asset owners to baseline the deterministic network traffic occurring within the control systems environment. In addition, the service offering provides asset owners with a means to identify anomalous and potentially suspicious communications sourced from, or destined for, control systems assets.

Assessments in FY 2015

In FY 2015, ICS-CERT conducted 112 onsite cybersecurity assessments across eight of the 16 CI sectors in 22 states and the District of Columbia. Of these 112 assessments, 38 were CSET assessments, 46 were DAR assessments, and 28 were NAVV assessments (see Assessment FY 2015 Metrics on Page 18).

CSET®

The Cyber Security Evaluation Tool (CSET) is a stand-alone software tool that guides asset owners and operators through a step-by-step process to analyze their ICS and IT network security practices using many recognized government and industry standards and recommendations. CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture.

ICS-CERT released two new versions of the CSET tool in 2015: CSET 6.2 in January, and CSET 7.0 in August.

CSET 6.2 introduced two new standards: 1) the Committee on National Security Systems Instruction (CNSSI) No. 1253 (ICS), Security Categorization and Control Selection for National Security Systems, Baseline Update; and 2) the North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP), Revision 5. Additional enhancements included revisions to the network diagram interface, the ability to model multiple services in a single component on the diagram, Grass Marlin integration, additional Department of Defense (DOD) identification fields and export capabilities, and the addition of a new Security Assurance Level determination wizard that allows users to add special factors from the National Institute of Standards and Technology (NIST) Special Publication 800-60.

CSET 7.0 introduced three new standards: 1) the Cybersecurity Capability Maturity Model (C2M2), Version 1.1; 2) DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT); and 3) the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 Volume 1, Revision 1, Guidelines for Smart Grid Cybersecurity. Additional enhancements included a complete redesign of the interface for a more intuitive experience, increased use of tabbed sections throughout the application, additional instructional "landing pages" at each major step in the process, consolidation of existing tabs on the diagram screen to refine network drawing time, improved responsiveness of the questions screen, the ability to support multiple screen resolutions (including mobile and large resolution capability), and encryption capability within CSET.

In FY 2015, ICS-CERT distributed 7,565 copies of CSET in 120 countries. In addition to independent assessments, CSET was used in 38 assessments performed by the ICS-CERT assessment team.

CSET®
CYBER SECURITY EVALUATION TOOL
Version 7.0
U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland Security
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

Houston, Texas
ICS-CERT Regional Training, October 2014.

Training

Training is a fundamental component of any robust cybersecurity strategy. ICS-CERT continues to support CI sectors and the control system community by offering multiple training courses, ranging in difficulty, at numerous locations around the country and online. These trainings are provided specifically for personnel responsible for the oversight, design, and operation of control systems. All courses are offered free of charge. In FY 2015, online and classroom course materials were updated multiple times to include the latest data on threats and vulnerabilities and their appropriate mitigations from cybersecurity experts. ICS-CERT is currently sponsoring 15 training courses.

ICS-CERT online training courses are as follows:

- Operational Security (OPSEC) for Control Systems (100W)
- 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).

The 100W course is designed to increase awareness and provide students the tools to recognize potential weaknesses in daily operations. The 210W series of courses are designed to cover a broad range of topics related to cybersecurity for control systems. For the most comprehensive training, they should be taken in order, 210W-01 through 210W-10. In FY 2015, 8,804 professionals registered for online training.

> The training was well executed and provided measurable benefits to all in attendance. Your whole team did a great job. Overall, I think you opened a lot of eyes on this and other topics, including threats, vulnerabilities, exploits, mitigation and overall risk. I hope to have the opportunity to continue the series for myself, later this year, by taking the 301 course in Idaho.
>
> *—Trainee from Phoenix Regional Training*

Phoenix, Arizona
ICS-CERT Regional Training, April 2015

Salt Lake City, Utah
ICS-CERT Regional Training, June 2015.

ICS-CERT classroom training courses are as follows:

- Introduction to Control Systems Cybersecurity (101)
- Intermediate Cybersecurity for Industrial Control Systems (201), lecture only
- Intermediate Cybersecurity for Industrial Control Systems (202), with lab/exercises
- Advanced Cybersecurity for Industrial Control Systems (301), with lab/exercises.

The 101, 201, and 202 courses are presented in various locations, multiple times per year. Accompanying networks are used to demonstrate exploits and mitigation tactics in the numerous exercises. In FY 2015, regional training sessions were hosted for over 800 attendees in Houston, Texas; Phoenix, Arizona; Salt Lake City, Utah; and Oklahoma City, Oklahoma.

Regional Training in Salt Lake City.

The 301 course is taught in Idaho Falls, Idaho, and includes a week of hands-on training featuring a very competitive Red Team / Blue Team exercise that takes place within an actual control systems environment. ICS-CERT Training presented this course 12 times in FY 2015 and hosted 484 students.

As part of its mission to continually provide first-rate response to reported cybersecurity incidents, ICS-CERT conducted a job and task analysis for the NCCIC incident handler job functions. Based on results from the analysis, a new training program is being developed to incorporate both onsite and remote incident response responsibilities.

In FY 2015, the Virtual Learning Portal (VLP) was upgraded. The VLP is an online application for the administration, documentation, tracking, reporting, and delivery of training courses. This upgrade was completed to better align the program with the federal guidelines (such as FISMA and FedRAMP) for cloud-based applications, to improve the graphical user interface, and to reduce operational costs. The new VLP will also facilitate the program's goal of offering continuing education units to attendees as many professions require continuous training from accredited sources to keep their skills and licenses current. The process of becoming accredited through the International Association for Continuing Education and Training (IACET) was started in 2015 and is expected to be completed in 2016.

Oklahoma City, Oklahoma
ICS-CERT Regional Training, August 2015.

Washington, D.C.
ICS-CERT ICSJWG 2015 Spring Meeting.

Industrial Control Systems Joint Working Group

ICS-CERT established the Industrial Control Systems Joint Working Group (ICSJWG) to enhance collaboration between ICS stakeholders and facilitate partnerships between the Federal Government and private sector owners and operators in all CI sectors. The working group is a principal component of the Strategy for Securing Control Systems, providing a coordination group for sharing information and facilitating stakeholder efforts to manage cybersecurity risk.

The ICSJWG helps the control systems community network and collaborate through its two-tiered approach of face-to-face meetings and webinars. Face-to-face meetings provide the opportunity to network in person and to share information formally or informally through presentations, panels, demonstrations, and ad hoc discussions among peers from all sectors, industries, and agencies. Webinars are held quarterly or when requested by ICS-CERT and address issues that are of concern to ICS asset owners/operators, vendors, researchers, integrators, and others. These issues may be technical solutions to problems or newly found vulnerabilities with corresponding mitigation techniques.

NCCIC Director of Operations John Felker Speaking at the ICSJWG 2015 Fall Meeting in Savannah, Georgia.

The face-to-face meetings are unique in that they target the ICS community and include all sectors with subject matter experts from both the public and private sector. While the information exchanged is relevant to both newcomers to the ICS space and established experts, the focus on networking and collaboration is what sets the ICSJWG meetings apart from a mere conference with presentations. ICSJWG members consistently give the face-to-face meetings high ratings for their relevance and value to members' professional lives.

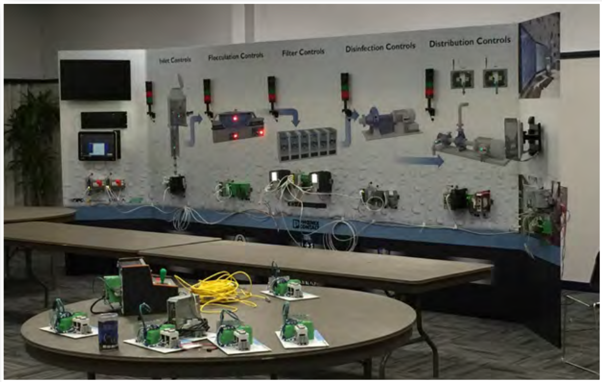
The more recently developed webinar series is a direct result of feedback received from the ICSJWG membership. Speakers who cannot be included in the ICSJWG face-to-face meeting agenda may convert their presentation to a webinar or, alternatively, should the membership or the ICSJWG Steering Team (IST) request such, a special webinar on a specific important topic may be planned and produced. In addition, ICS-CERT has used ICSJWG resources to produce more technically specific webinars about relevant and high-profile issues that affect the entire community.

In addition to face-to-face meetings and webinars, the ICSJWG provides informational products to the broader ICS community that help to raise awareness regarding a particular issue or to address a specific need. Following collaboration with the IST and other stakeholders, ICS-CERT produced, "ICS Cybersecurity for the C-Level," a document that helps bridge the communication divide that often exists between ICS cybersecurity personnel and C-Level executives. ICS-CERT and the ICSJWG have received positive feedback regarding the document and its usage, and the ICSJWG continues to communicate with the ICS community regarding further informational product development.

The ICSJWG spans the gap between ICS-CERT announcements or advisories and the ICS community working to improve the security of the Nation's infrastructure and control systems. It facilitates collaboration and conversation about security flaws and how to fix them.

The ICSJWG Steering Team

The IST continues to meet on a regular basis to discuss a variety of topics, most notably how best to move the working group forward in this ever changing landscape. The IST is made up of members representing roles such as asset owners; vendors; state, local, and tribal governments; industry associations; universities; consultants/integrators; and the international community.



ICS Village, provided by Phoenix Contact

By bringing this diverse group together and leveraging its professional networks, the ICSJWG hopes to improve the partnership between the public and private sectors in working together to secure our Nation's CI. Because the members of the IST are leaders in the ICS community, they can also tap resources from many areas in order to enhance the diversity of meeting venues and the depth of meeting contents.

2015 Spring Meeting

The ICSJWG 2015 Spring Meeting was held in Washington, DC, on June 23-24 and brought together over 200 people, including asset owners and operators, government professionals, vendors, systems integrators, and academic professionals from around the globe. Key highlights from the meeting included a Q&A session with Director Marty Edwards and a classified threat briefing. The meeting also covered a wide variety of topics in plenary presentations, panel discussions, and demonstrations providing an opportunity for attendees to present and discuss pressing issues across all of our CI sectors.

2015 Fall Meeting

The 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 keynote speakers, practical demonstrations, presentations, panels, lightning round talks, and unclassified briefings. Highlights from the 2015 Fall meeting included feature presentations from NCCIC Director of Operations John Felker, President of the Technology Association of Georgia Tino Mantella, Independent Security Researcher Marina Krotofil, and Robert Lee from the SANS Institute. The meeting also featured the ICS Village, which was provided by Phoenix Contact and included a replica of a typical water plant network setup with hands-on isolated industrial equipment stations.

ICSJWG Webinars

FY 2015 Webinars included ICS-CERT focused information sharing with restricted access due to the nature of the briefing. During FY 2015, ICSJWG webinars covered various topics, including the following:

- Action Campaign Briefing 4 (TLP:AMBER)
- A Call to Action: Current Risks to Industrial Control Systems (TLP:AMBER)
- BlackEnergy and Havex Briefing for Partners (TLP:AMBER)
- Protecting M2M Systems at the Edge.

Savannah, GA.
ICS-CERT ICSJWG 2015 Fall Meeting.

Moving Forward

In 2016, ICS-CERT will continue to improve cybersecurity capabilities and extend services in support of all ICS stakeholders in the 16 CI sectors. ICS-CERT will continue coordination efforts with industry and government partners to mitigate cyber risks to CI through timely and effective sharing of situational awareness information and focused mitigation strategies.

To handle increased demand for onsite assessments, ICS-CERT is hiring additional personnel and will pursue more one-on-one engagements with CI asset owners on the use of DARs and NAVVs and assist them in identifying gaps and developing strategies for improving their defensive posture. A new responsibility in 2016 is to assist federal facilities with control systems assessments. Federal facilities are becoming more aware of vulnerabilities and threat vectors that can impact their control systems operations similar to private sector CI facilities.

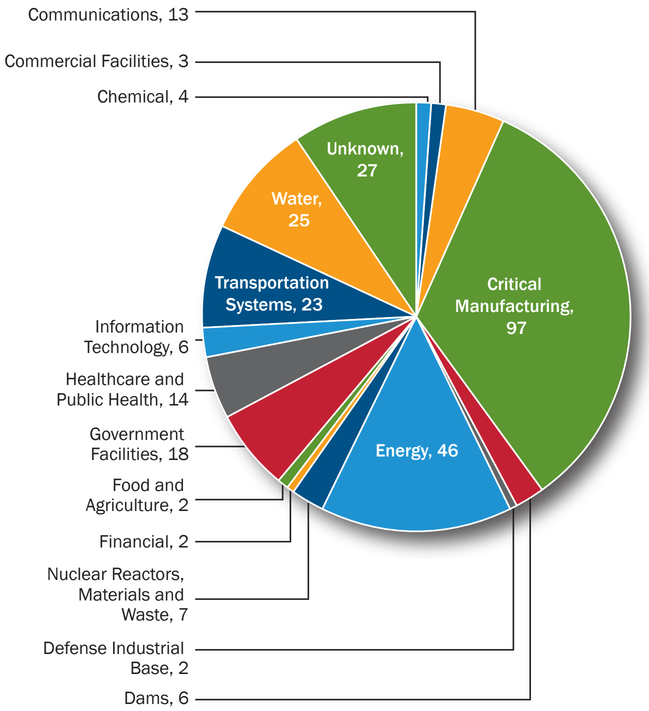
Other goals for 2016 include improving and expanding ICS-CERT incident response technical teams and tools, which will provide greater value during incident response and assessment activities. We will continue to refine and update training offerings that will allow CI asset owners to better meet the demands of challenging and evolving technical issues in control system security.

ICS-CERT will expand its presence in Pensacola beyond watch operations to include incident response and site assessment personnel. ICS-CERT will continue to hold biannual ICSJWG meetings in 2016 as we continue our public private partnership collaboration. Through our interactions with asset owners, vendors, and researchers, we receive many requests for more information about our work, so we will provide a 2015 version of our site assessment work similar to what we published for 2014. In addition, we plan to develop vulnerability and incident response reports with detailed information from our work in 2015.

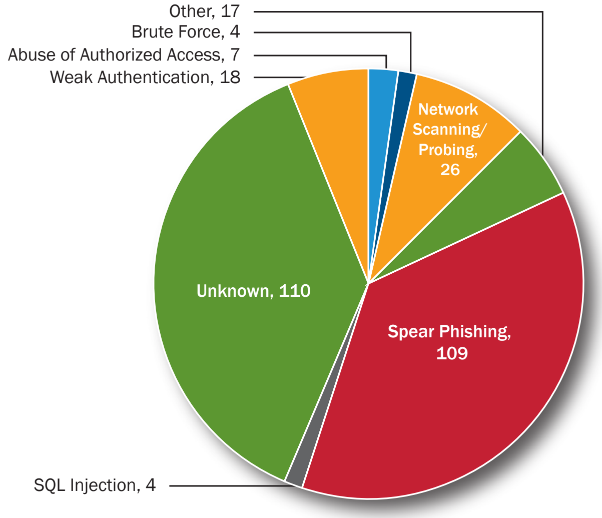
It is uncertain what new cybersecurity threats will emerge in 2016, but ICS-CERT stands prepared to react quickly and evolve to meet the challenge. We will continue our efforts to help CI asset owners prevent attacks or mitigate their harmful effects like we have for over a decade. We will make our alerts and advisories more actionable with additional information, e.g., Yara Rules and instructions for Yara use, to further assist CI asset owners. In addition, we are looking to improve the distribution of our information through newly formed ISACs in oil and natural gas (ONG) and foresee the development of additional Information Sharing and Analysis Organizations (ISAOs) to share with the private sector. If you have additional ideas about how we can better assist you in your cybersecurity efforts, please email us at ics-cert@hq.dhs.gov.

Incident Response FY 2015 Metrics

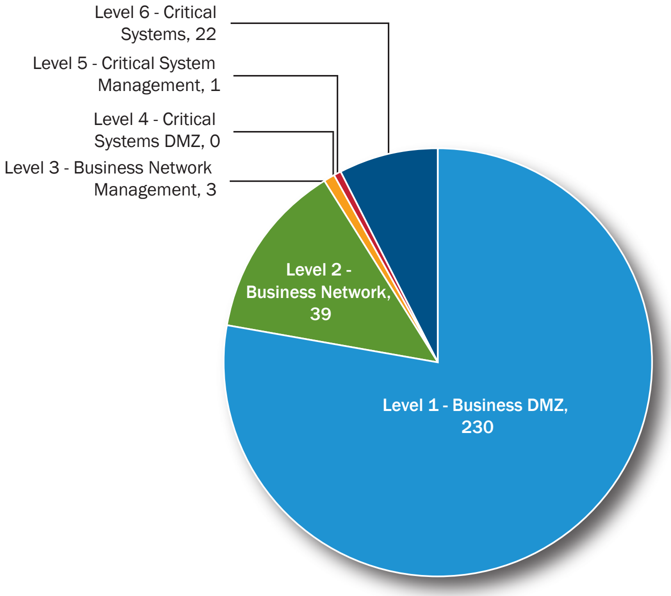
FY 2015 Incidents by Sector (295 total)



FY 2015 Incidents by Infection Vector (295 total)



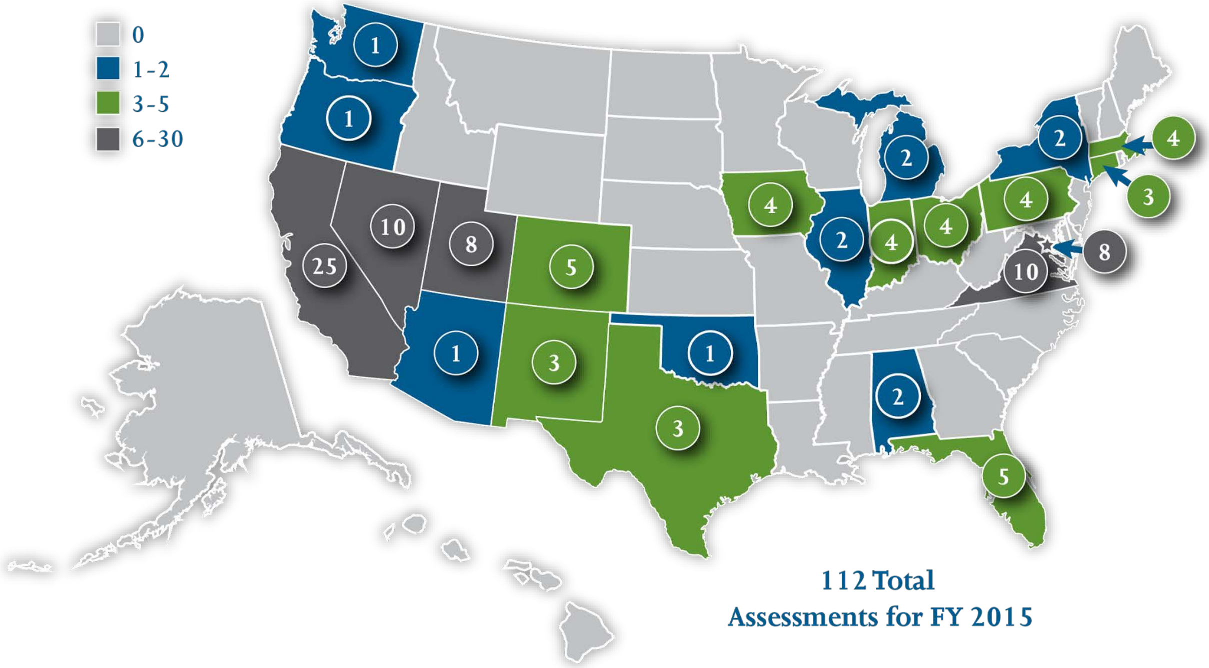
FY 2015 Observed Depth of Intrusion



Assessment FY 2015 Metrics

Sector	FY 2012	FY 2013	FY 2014	FY 2015
Chemical Sector	4	0	1	3
Commercial Facilities Sector	2	0	2	0
Communications Sector	0	2	0	0
Critical Manufacturing Sector	1	0	0	0
Dams Sector	0	0	0	0
Defense Industrial Base Sector	12	1	0	3
Emergency Services Sector	3	0	0	10
Energy Sector	7	19	43	33
Financial Services Sector	6	0	0	0
Food and Agricultural Sector	0	0	0	0
Government Facilities Sector	3	2	5	12
Healthcare and Public Health Sector	1	5	0	0
Information Technology Sector	5	2	0	3
Nuclear Reactors, Materials, and Waste Sector	8	8	5	0
Transportation Systems Sector	10	10	10	9
Water and Wastewater Systems Sector	25	23	38	39
Totals	**87**	**72**	**104**	**112**
Number of Sectors Assessed	**13/16**	**9/16**	**7/16**	**8/16**

FY 2015 Onsite Assessments by State



112 Total
Assessments for FY 2015

NCCIC/ICS-CERT Fiscal Year 2015 Metrics

NCCIC/ICS-CERT FY Metrics	2012 totals	2013 totals	2014 totals	2015 Totals
ICS Incident Reported - Tickets	197	257	245	295
ICS Incident Response Onsite Deployments	6	7	4	5
ICS-Related Vulnerability Report - Tickets	137	187	159	189
NCCIC/ICS-CERT Information Products	347	295	339	332
Distributed or Downloaded CSET	6,631	5,085	5,132	7,565
Onsite Assessments	89	72	104	112
Professionals Trained	2,327	693	800	1,330
Number of Training Sessions	56	17	21	29
ICSJWG Membership	1,371	1,476	1,726	1,912
Speaking Engagements	205	162	168	342
Conference Exhibitions	22	2	0	0

NCCIC/ICS-CERT Calendar Year 2015 Metrics

NCCIC/ICS-CERT CY Metrics	2012 totals	2013 totals	2014 totals	2015 Totals
ICS Incident Reported - Tickets	138	256	232	303
ICS Incident Response Onsite Deployments	6	4	6	4
ICS-Related Vulnerability Report - Tickets	147	181	167	177
NCCIC/ICS-CERT Information Products	343	285	362	316
Distributed or Downloaded CSET	5,584	4,175	6,364	7,800
Onsite Assessments	89	78	106	123
Professionals Trained	2,241	445	1,048	1,542
Number of Training Sessions	52	12	27	29
ICSJWG Membership	1,416	1,544	1,733	2,000
Speaking Engagements	200	147	188	380
Conference Exhibitions	19	1	0	0

Assistance from ICS-CERT is only a phone call away

ICS-CERT encourages you to report suspicious cyber activity and vulnerabilities affecting critical infrastructure control systems.

To report control systems cyber incidents and vulnerabilities, contact ICS-CERT:

Toll Free: 1-877-776-7585

International Callers: 1-208-526-0900

ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting, visit:

http://ics-cert.us-cert.gov

For more information about ICS-CERT, visit:

https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

Homeland Security

15-50569