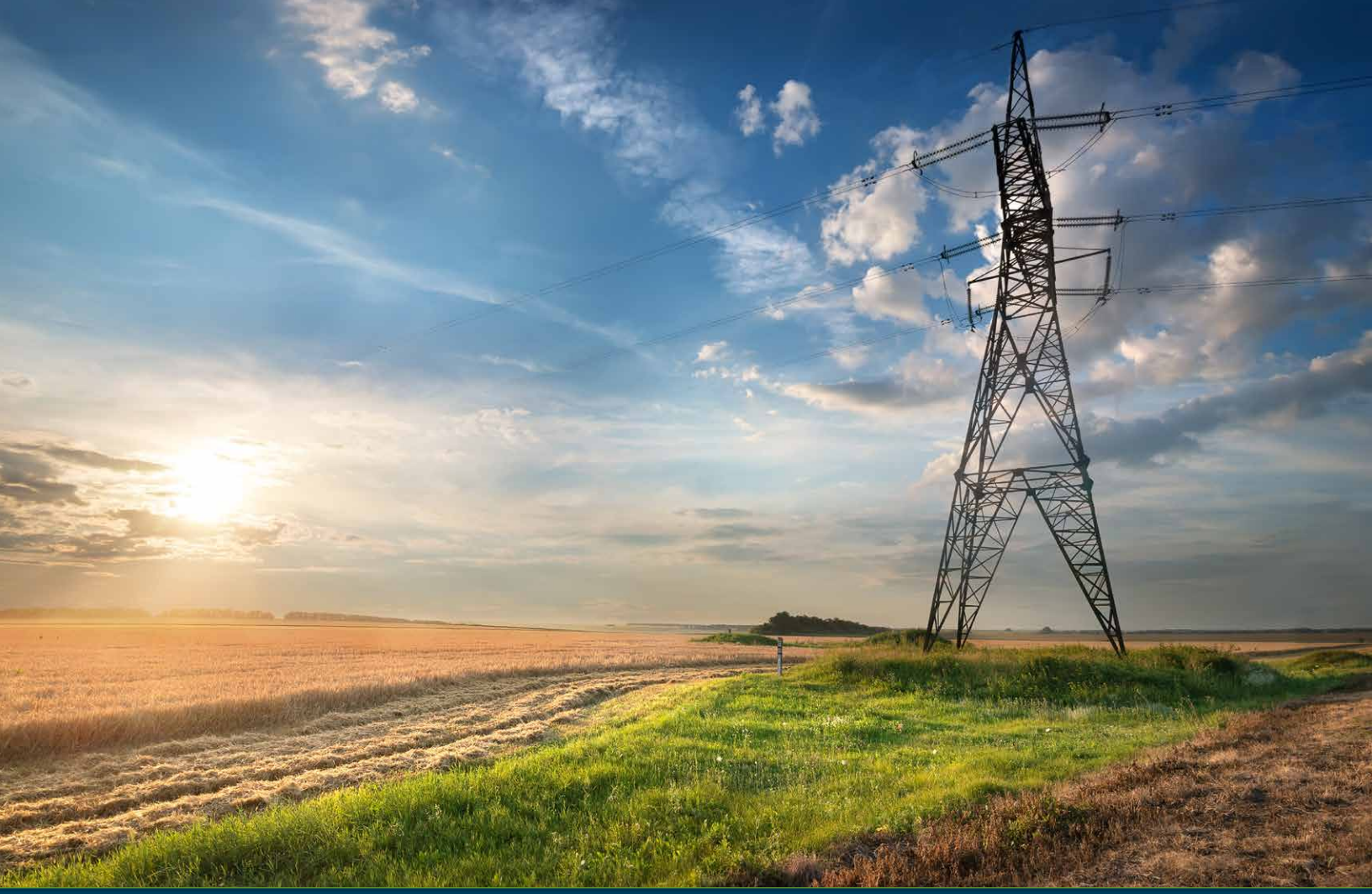


ICS-CERT Year in Review

Industrial Control Systems Cyber Emergency Response Team

2016

NCCIC

Contents

Welcome

NCCIC

In 2016, the National Cybersecurity and Communications Integration Center's (NCCIC) role within the Department of Homeland Security's (DHS) cybersecurity mission continued to evolve and expand. In July, President Obama issued Presidential Policy Directive (PPD)-41, which identifies the Federal Government's principles concerning cyber incident coordination among federal agencies. The directive identifies the five principles for incident response through three lines of effort. PPD-41 designates NCCIC as the lead for asset response, one of the three lines of effort. NCCIC will respond to an incident at the request of the affected asset owner to stop the attack, mitigate its affects, and provide the asset owner with guidance on making its system more secure. NCCIC will then share anonymized information about the attack with other asset owners so they can learn from each incident and better protect their systems.

Also this year, NCCIC and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) joined an interagency team in travelling to Ukraine after cyber attacks on the country's power infrastructure. These attacks, which occurred on December 23, 2015, caused unscheduled power outages, affecting many Ukrainian power customers. The team worked with the Ukrainian government to understand and gain insight about the attacks.

It has been another busy and successful year for NCCIC, and once again, I am proud of all that they have accomplished. Moving into 2017, we continue to look for ways to be more effective in the fight against cyber threats, and we look forward to continuing the dialogue with our partners in government, industry, and the critical infrastructure (CI) community that helps us do so.

Sincerely,

John Felker
NCCIC Director of Operations
Department of Homeland Security

ICS-CERT

As we move into a new year, ICS-CERT continues unceasingly to combat the ever-increasing threats to the CI that provides the important services Americans rely on each day in their personal and professional lives. In this 2016 Year in Review, however, we pause to look back on ICS-CERT's accomplishments over the past year.

In 2016, ICS-CERT joined with the Federal Protective Services (FPS) and the General Services Administration (GSA) to form the Federal Facility Control Systems Security Program (FFCSSP). This program assesses security in Federal facilities, with ICS-CERT conducting the cybersecurity portion of the assessment. The ICS-CERT private sector Assessment team conducted a cybersecurity assessment at Levi's Stadium in advance of Super Bowl 50 and was onsite at the game to monitor, coordinate, and report any cybersecurity threats or incidents. In March and April, ICS-CERT and the Federal Bureau of Investigation (FBI) conducted unclassified in-person briefings and online webinars concerning the attacks against Ukrainian power infrastructure in December 2015.

Overall, this past year, ICS-CERT completed work on 290 cyber incidents, coordinated 305 vulnerabilities, analyzed 100 malware samples, conducted 130 cybersecurity assessments, released two new versions of the Cyber Security Evaluation Tool (CSET®), and released a new edition of the Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies document. In addition, ICS-CERT again hosted multiple regional trainings around the country, including one in Lisbon, Portugal, and two Industrial Control Systems Joint Working Group (ICSJWG) meetings, one in Scottsdale, Arizona, and one in Ft. Lauderdale, Florida.

As the threat to the Nation's CI expands, ICS-CERT continues to grow to meet each new challenge. I am impressed with how ICS-CERT has continued its excellent work as our team continues to expand. I am proud of what the team has accomplished, and I am sure they will accomplish even more in 2017.

Sincerely,

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

NCCIC

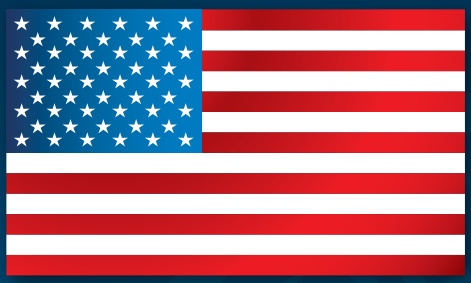
NCCIC

The 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.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is one of NCCIC's four branches. (ICS-CERT works closely with private sector asset owners, vendors, and government agencies at all levels (Federal, state, local, and tribal) to protect America's critical infrastructure (CI) from cyber attacks. With these entities, ICS-CERT works to coordinates the sharing of information, services, and tools to help CI asset owners prevent, mitigate, and recover from cyber incidents and attacks. The United States depends on CI to support national defense, economic stability, and public health and safety. Presidential Policy Directive (PPD)-21 identifies 16 CI sectors. Any disruptions or destruction to CI could be catastrophic for the Nation. ICS-CERT's activities include eight main functions. Four are operations functions, which include situational awareness, incident response, vulnerability coordination, and technical analysis. The other four are risk reduction functions, including cybersecurity assessments, distribution of the Cyber Security Evaluation Tool (CSET), training, and Industrial Control Systems Joint Working Group (ICSJWG) activities.

ICS-CERT



With honor and integrity, we will safeguard the American people, our homeland, and our values.

DHS Mission Statement

With honor and integrity, we will safeguard the American people, our homeland, and our values.

NCCIC Vision

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.

NCCIC Mission

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.

ICS-CERT Mission

ICS-CERT's mission is to reduce risk to the Nation's critical infrastructure by strengthening control systems security and resilience through public-private partnerships.

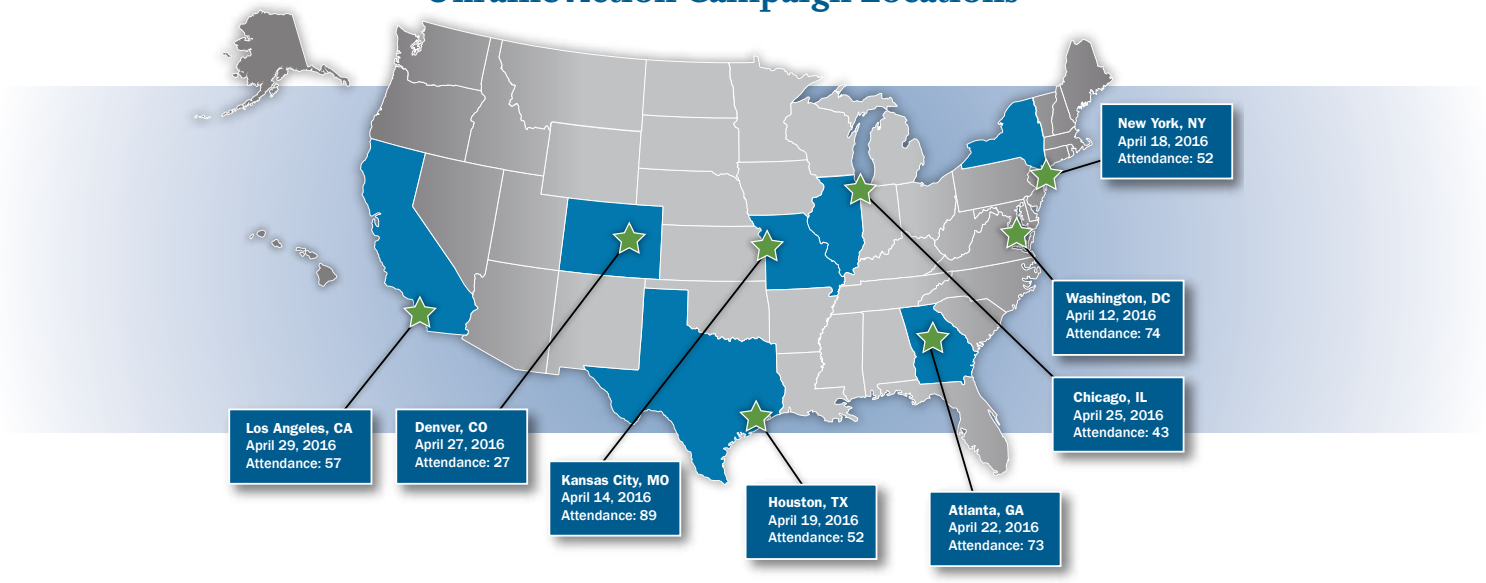
FY 2016 Highlights and Accomplishments

- **Assessments:** ICS-CERT conducted 130 onsite and remote cybersecurity assessments across 12 of the 16 CI sectors in 19 states, Washington D.C., and Guam. Of these 130 assessments, 32 were CSET assessments, 55 were Design Architecture Review (DAR) assessments, and 43 were Network Architecture Verification and Validation (NAVV) assessments. In August, the Assessments team also released its FY 2015 annual report, NCCIC/ICS-CERT Industrial Control Systems Assessments Summary Report.
- **CSET 7.1 and 8.0:** The CSET development team released two new versions of CSET in 2016. The team released CSET 7.1 in February and CSET 8.0 in September. The latest version includes new standards, a simplified user interface, protected modules, custom questionnaires, and enhanced network diagramming window, and additional network components. In FY 2016, ICS-CERT distributed over 10,000 copies of CSET in 120 countries.
- **ICSJWG:** This year, the ICSJWG team again hosted two successful ICSJWG meetings, with a total of 594 attendees. The team hosted the Spring Meeting at the Chaparral Suites in Scottsdale, Arizona, on May 3–5. This meeting was the largest to date, bringing together 306 stakeholders from the ICS community. The ICSJWG 2016 Fall Meeting took place on September 13–15 at Embassy Suites Ft. Lauderdale—17th Street in Ft. Lauderdale, Florida. This meeting brought together 288 attendees. Over the course of each three-day ICSJWG meeting, the 594 attendees had the opportunity to network and interact through demonstrations, presentations, panels, and lightning-round talks.
- **Incident Response:** In FY 2016, the ICS-CERT Incident Response team completed work on 290 incidents. The Critical Manufacturing Sector accounted for 63 of these incidents, while the Communications Sector had 62 and the Energy Sector had 59. Spear phishing represented 26 percent of these incidents, making it the leading access vector for ICS-CERT's FY 2016 incidents. Network scanning and probing accounted for 12 percent.
- **Information Products.** In August, ICS-CERT released the NCCIC/ICS-CERT Industrial Control Systems Assessment Summary report. In September, ICS-CERT released the Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies document and the NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report. In November, ICS-CERT released a Malware Trends white paper.
- **Super Bowl 50 Assessment.** ICS-CERT conducted a cybersecurity assessment at Levi's Stadium in advance of Super Bowl 50 in Santa Clara, California, and the

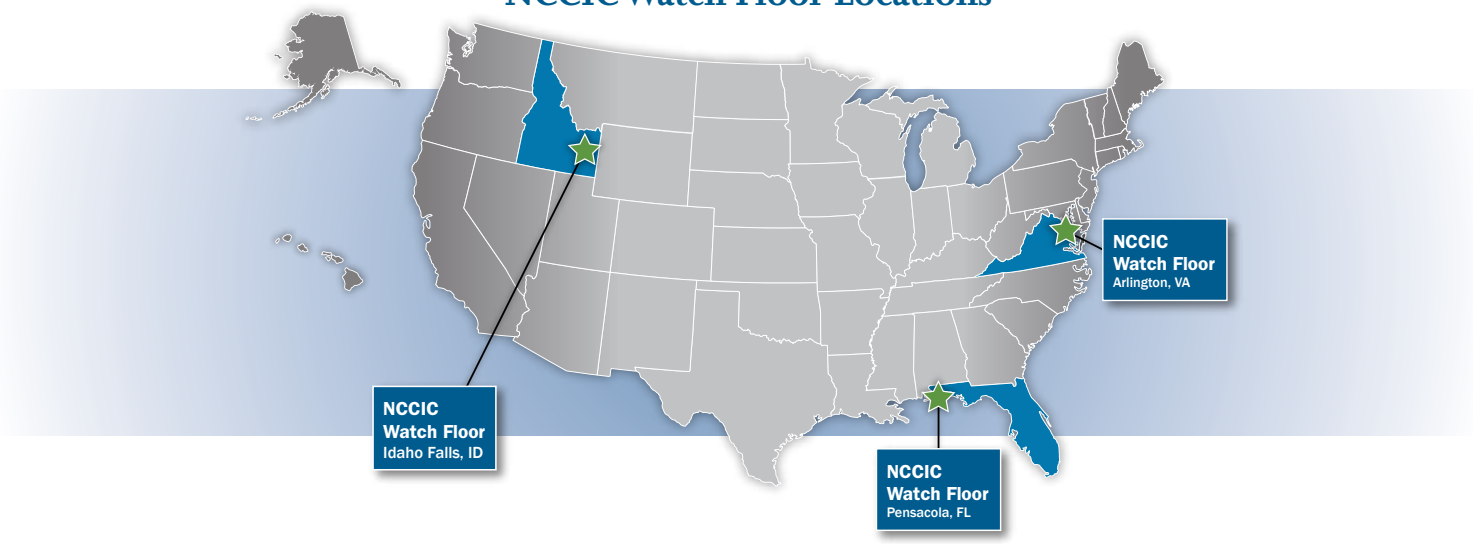
team was onsite at the Super Bowl 50 Operations Center monitoring, coordinating, and reporting activities relating to cyber or communications threats and incidents.

- **Technical Analysis:** In FY 2016, the Advanced Analytical Laboratory (AAL) performed in-depth analysis on 100 malware samples, the results of which contributed to multiple ICS-CERT alerts and advisories. Also this year, the AAL has continued modernization efforts to keep pace with changing technology.
- **Training:** In FY 2016, 24,350 students registered and 17,773 students completed at least one of the online courses offered. The Training team hosted regional training sessions for 1,076 attendees in Pittsburgh, Pennsylvania; Baton Rouge, Louisiana; Boston, Massachusetts; and Lisbon, Portugal (conducted for EUCOM). ICS-CERT Training presented the Red Team/Blue Team exercise 12 times in FY 2016 and hosted 506 students. In early April, the Training team conducted the pilot of an Incident Responder course and developed a new instructional course for CSET. The team completed a major systems upgrade to the Control Systems Analysis Center (CSAC), integrating additional control system hardware and software into the Red Team/Blue Team exercise networks.
- **Ukraine Action Campaign.** After the attacks against Ukrainian power infrastructure on December 23, 2015, DHS's NCCIC and ICS-CERT, along with the Federal Bureau of Investigation (FBI), the Department of Energy (DOE), and other Federal agencies, worked with the government of Ukraine to understand the attacks. In March and April, ICS-CERT and the FBI conducted unclassified in-person briefings and online webinars for asset owners and representatives from all levels of government to increase awareness of the threat and provide additional information. The briefing sessions provided details about the events surrounding the attack, techniques used by the threat actors, and strategies for mitigating risks and improving the cyber defensive posture of an organization.
- **US-CERT Portal Migration to HSIN.** This year, DHS consolidated all secure portal capabilities into a single platform, the Homeland Security Information Network (HSIN). HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information with streamlined collaboration and real-time communications throughout all homeland security mission areas. The US-CERT Portal (NC4 Mission Center) migrated all content to HSIN (including the ICS-CERT compartment). This migration provides significant functionality, features, and enhanced security, and it enables greater customization and configuration for the communities (formerly compartments) that move to HSIN.
- **Vulnerability Coordination:** ICS-CERT handled 187 vulnerability tickets and coordinated 305 unique vulnerabilities.

Ukraine Action Campaign Locations



NCCIC Watch Floor Locations



Watch Floor Operations

NCCIC maintains watch floor operations capabilities in three geographically separate locations: Idaho Falls, Idaho; Pensacola, Florida; and Arlington, Virginia. NCCIC's watch floor operations are the primary entry point for threat, vulnerability, and incident reporting, as well as classified and unclassified information dissemination. Watch floor operations coordinate the interaction between stakeholders and ICS-CERT by ingesting, triaging, and tracking incidents to resolution. Watch floor operations coordinate with other ICS-CERT and NCCIC components, the law enforcement and intelligence community, and other external partners. NCCIC's watch floor operations provide 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. 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 the operation of ICS-CERT's incident management system.

ICS-CERT conducted 10 webinars, 137 presentations, and 196 teleconferences for stakeholders to help them understand the threats to CI. At the request of stakeholders, ICS-CERT published and distributed a document titled Seven Steps to Effectively Defend Industrial Control Systems. The guide highlights strategies that if implemented correctly could have mitigated all major incidents reported to ICS-CERT in FY 2015. The document is available on the ICS-CERT web site.

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages affecting a large number of customers in Ukraine. An interagency team composed of representatives from the NCCIC/ICS-CERT, U.S. Computer Emergency Readiness Team (US-CERT), DOE, FBI, and the North American Electric Reliability Corporation (NERC) traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber attacks. Although analysis is still ongoing, the team of both U.S and Ukrainian government officials has not been able to confirm a causal link between the power outage with the presence of the malware. In the wake of this event, ICS-CERT conducted four webinars and eight presentations describing the events to assist stakeholders in understanding the event.

Idaho National Laboratory

Idaho National Laboratory (INL) is a Department of Energy (DOE) National Laboratory located in Idaho Falls, Idaho. When DHS was formed, Congress directed DHS to utilize the DOE laboratories, and ICS-CERT has done this for over 10 years in Idaho. DHS ICS-CERT leverages a significant amount of INL's top level talent, such as control systems and cybesecurity expertise through an Inter Agency Agreement (IAA) with DOE. INL personnel make up a majority of ICS-CERT's overall staff and provide support for all ICS-CERT functions, as well as hosting one of the three NCCIC watch floors and the AAL.

ICS-CERT Director Marty Edwards talks with DHS NPPD Under Secretary Suzanne Spaulding during a visit to the NCCIC watch floor in Idaho Falls, Idaho.

ICS-CERT and NCCIC fall under DHS's Office of Cybersecurity and Communications (CS&C) and the National Protection and Programs Directorate (NPPD). NPPD, CS&C, and NCCIC leadership regularly travel to ICS-CERT's site at INL in Idaho Falls, Idaho. In August, ICS-CERT hosted NPPD Under Secretary Suzanne Spaulding, the highest ranking DHS official to visit INL. On these visits, NPPD, CS&C, and NCCIC leadership meet with the team and leadership to discuss cybersecurity and departmental issues and to gain the perspective of personnel doing ICS-CERT's cybersecurity work. These visits also include a tour of ICS-CERT's facilities, as well as many of INL's non ICS-CERT facilities and capabilities.

NPPD Under Secretary Suzanne Spaulding speaks to the ICS-CERT team in Idaho Falls, Idaho.

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 affecting industrial control systems (ICS) 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 in developing strategies for mitigation, recovery, and improving ongoing cyber defenses.

ICS-CERT also collaborates with international and private sector Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) 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, adversaries develop increasingly sophisticated attacks against control system networks. ICS-CERT provides onsite incident response, conducts technical analysis of artifacts and malware, develops mitigation strategies for asset owners, and provides configuration analysis to help detect and prevent evolving threats. ICS-CERT assists asset owners with tools and services beyond traditional network monitoring in identifying potential threat actors present in control system networks.

Incident Response in FY 2016

In FY 2016, the ICS-CERT Incident Response team completed work on 290 incidents. The Critical Manufacturing Sector accounted for 63 of these incidents, while the Communications Sector had 62 and the Energy Sector had 59. Spear phishing represented 26 percent of these incidents, making it the leading access vector for ICS-CERT's FY 2016 incidents. Network scanning and probing accounted for 12 percent.

Also in FY 2016, the team responded to the first known cyberattack to result in physical impact to a power grid. In another instance, they responded to an incident where an asset owner found low-level malware with persistent malicious remote access in its water control system. Because of these events, ICS-CERT published a number of alerts and advisories, as well as conducted a national outreach campaign to share lessons learned and technical artifacts with critical infrastructure asset owners.

ICS-CERT's Vulnerability Coordination Process

1. Detection and Collection,
2. Analysis,
3. Mitigation Coordination,
4. Application of Mitigation, and
5. Disclosure.

Vulnerability Coordination

The primary objective of the ICS-CERT Vulnerability Coordination team's work is the timely mitigation of vulnerabilities to reduce the likelihood of a successful cyber attack against the Nation's CI. In this effort, the Vulnerability Coordination team engages with Federal, state, local, and tribal governments and with ICS owners, operators, and vendors in the private sector. Vulnerability coordination requires technical expertise and close trusted partnerships with each of these key stakeholders in the ICS community.

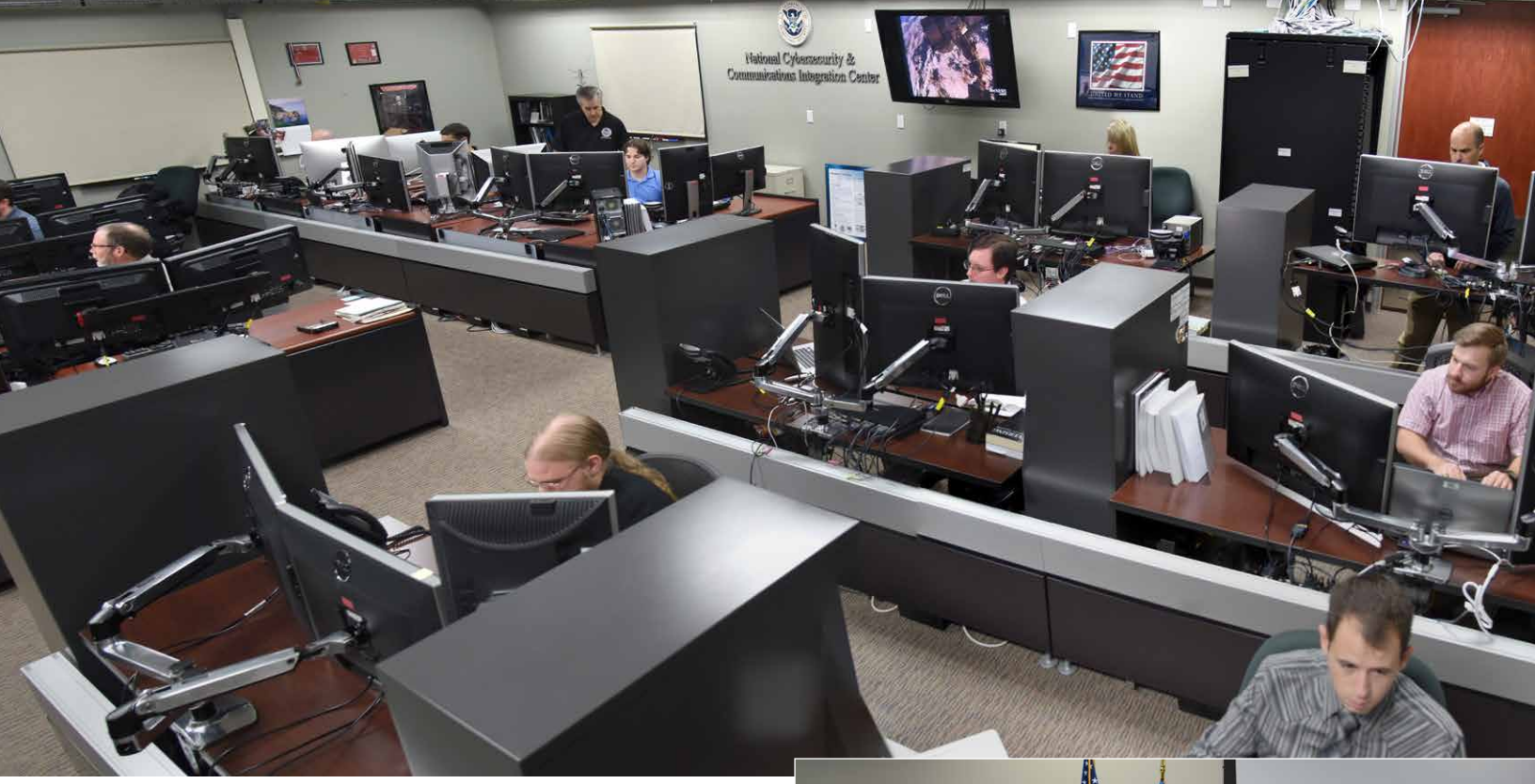
ICS-CERT's vulnerability coordination process includes five basic steps (listed above next column). In the detection and collection step, the Vulnerability Coordination team collects vulnerability reports through vulnerability analysis and monitoring of public sources or they receive vulnerability information directly from researchers. Upon learning of a vulnerability, the team eliminates duplicates and false alarms and they catalog each vulnerability. In the analysis step, the team works with vendor analysts to examine the vulnerability and identify all its potential threats. In the mitigation coordination step, the team works with the vendor for mitigation and patch issuance. The Vulnerability Coordination team allows sufficient time for the vendor to effectively resolve and perform patch regression testing against any given vulnerability. In the application of mitigation step, the team coordinates with vendors to allow sufficient time for affected end users to obtain, test, and apply mitigation strategies prior to ICS-CERT's public disclosure of the vulnerability. In the disclosure step, after coordinating with vendors and gathering technical and threat information, the team publishes an alert or advisory to notify end users about the vulnerabilities. ICS-CERT strives to disclose accurate, neutral, objective information. ICS-CERT references other available information on vulnerabilities and corrects misinformation when necessary.

Vulnerability Coordination in FY 2016

ICS-CERT handled 187 vulnerability tickets and coordinated 305 unique vulnerabilities. The Vulnerability Coordination team worked closely with researchers and vendors to encourage patching of validated vulnerabilities. The Vulnerability Coordination team also put together two different research panel discussions for the fall 2016 ICSJWG meeting. The two panels consisted of vulnerability researchers and medical research companies that provided different perspectives in the ICS community.

Vulnerability Coordination Case Study from 2016

This past August, NCCIC/ICS-CERT received notice that a remote attacker had used a zero-day exploit against the maritime transportation sector. The attacker exploited an SQL injection vulnerability in a web-based application used by multiple U.S. ports that provides real-time access to operational logistics information, resulting in a loss of valuable data. Once notified of this cyber attack, ICS-CERT issued an alert detailing the vulnerability and providing mitigation measures. ICS-CERT also contacted the vendor of the application to learn additional details and the status of a patch to mitigate the vulnerability. ICS-CERT then successfully notified all U.S. ports using the software and confirmed that they acquired and installed the necessary patch. ICS-CERT also shared the alert with relevant international partners and encouraged them to install the patch. Thanks to these efforts, the maritime transportation sector is more secure, resilient, and better prepared to respond to the next cyber attack.



Technical Analysis

ICS-CERT's Technical Analysis team consists of several groups working toward a common goal. Technical analysis includes all aspects of malware analysis; reverse engineering; log and artifact analysis; long-term analysis exploring systemic vulnerabilities, potential future threats, tactics, techniques, and procedures; and other intractable long-term problems. The AAL performs ICS-CERT's primary technical analysis work. The AAL performs most of the malware and artifact analysis. Primary backup support for the AAL and the majority of our applied research projects takes place at Sandia National Laboratory (SNL). We also have an agreement with and sponsor research by the Air Force Institute of Technology (AFIT).

Advanced Analytical Laboratory

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

DHS NPPD Under Secretary Suzanne Spaulding presents ICS-CERT's AAL team with a DHS NPPD appreciation award.

In FY 2016, the AAL performed in-depth analysis on 100 malware samples. This work helped ICS-CERT to publish multiple alerts warning the ICS community of the threats involved and provided information for detecting and mitigating intrusion activity.

The AAL continues to host summer interns looking for advanced exposure to ICS security work. This year, the AAL hosted an intern from the University of Nebraska at Omaha at its facilities on the Idaho National Laboratory campus in Idaho Falls, Idaho, providing experience with our malware analysis and artifact analysis processes. This intern was also able to participate in a review of Structured Threat Information Expression (STIX) modernization efforts and a project to scope an ICS hardware laboratory.

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 focus has been on analysis efforts in multiple data locations within the ICS network space and visualizing this analysis for responders. These efforts include the following:

- The Process Logic Extraction and Analysis Tool (PEAT) enables business/process logic verification through extraction of logic over the network and "disassembly" of multiple Process Logic formats into human-readable formats.
- BroBounds simplifies the process of writing intrusion detection system (IDS) scripts for the Modbus protocol in the Bro IDS tool by auto generating the script from choices the user makes in the interface.
- Archimedes expands on BroBounds by providing an interface to the Elasticsearch, Logstash, Kibana (ELK) stack for simple analysis of Bro data; visualizations that Kibana cannot perform; analytics that are too situation-specific for Kibana; analytics that are capable of machine learning; and providing the means to write new analytics on the fly.
- The Inquisit binary analysis tool received many performance enhancements for binary analysis of all types of files, particularly binary comparison features for use with process logic.

Air Force Institute of Technology

ICS-CERT's relationship with the Air Force Institute of Technology (AFIT) is in its sixth year and continues to expand. In FY 2016, ICS-CERT supported AFIT's groundbreaking research program, including twelve Masters students, one PhD student, and two faculty researchers dedicated to protecting critical infrastructure. Highlights for FY 2016 include three journal articles that seek to improve ICS cyber range capabilities, cyber insurance modelling for CI owners, and anomaly detection using timing-based side channels for ICS. In addition to the journal articles, AFIT published two separate peer-reviewed book chapters that researched organizational structure for cyber first responders and examined a practical application of ICS honeypot emulation. Students have also presented their research at the 10th Annual International Conference on Critical Infrastructure Protection and the International Conference on Cyber Warfare and Security.

AFIT's current graduate research efforts include the following:

- Expanding capabilities to evaluate cyber warriors and defenders,
- Advancing ICS honeypot research (leveraging proxy technology) to protect critical assets by surrounding key components with decoys,
- Enhancing cyber insurance models for CI asset owners,
- Threat intelligence applied to ICS,
- Adapting risk methodologies for medical device protection within care-giver spaces, and
- Anomaly detection for level 0 field devices running 4-20 ma current loops.

AFIT's research is publicly available at the following URL: http://www.afit.edu/CCR/

Assessments

ICS-CERT Private Sector Assessments

As a core part of its mission to reduce risk to the Nation's CI, ICS-CERT provides onsite and remote cybersecurity assessments to CI asset owners and operators to strengthen the cybersecurity posture of their ICS. ICS-CERT bases its assessments on standards, guidelines, and best practices and provides them 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 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 private sector Assessment team works with asset owners to determine which set of assessment services best fits the needs of that particular organization. The services provided may include a combination of a facilitated CSET, DAR, and/or NAVV assessment, depending on the current state and goals of the organization. The services provided by the private sector Assessment team are transitioning from individual CSET, DAR, and NAVV assessments to an integrated process including all the assessment offerings along with more advanced analytics to provide improved actionable feedback to asset owners. The assessment process includes a baseline assessment using CSET, a deep-dive design architecture review of the ICS, communications, and networking architecture, and analysis of the network data communications. Moving forward, the ICS-CERT Assessment team is working to include log analysis to the overall assessment services in FY 2017.

This integrated assessment approach has been evolving in FY 2016 and has notably found abnormal network traffic that indicated a potential system breach during several assessments. On such occasions, the ICS-CERT Assessment team handed the asset owner over to the ICS-CERT Incident Response team to provide assistance through the identification and mitigation process.

Assessments in FY 2016

In FY 2016, ICS-CERT conducted 130 cybersecurity assessments across 12 of the 16 CI sectors in 19 states, Washington D.C., and Guam. Of these 130 assessments, 32 were CSET assessments, 55 were DAR assessments, and 43 were NAVV assessments.

In addition, ICS-CERT is supporting broader DHS efforts by providing assessments for the Regional Resiliency Assessment Program (RRAP). RRAP is a cooperative assessment of specific CI within a designated geographic area and includes a regional analysis of the surrounding infrastructure. In FY 2016, ICS-CERT conducted 16 cybersecurity assessments with Infrastructure Protection (IP) in coordination with RRAP.

ICS-CERT is also working to develop the FY 2016 NCCIC/ICS-CERT Annual Assessment report, which will provide a year-end summary of ICS-CERT's private sector assessment activities to include FY 2016 assessment findings and observations, as well as highlighting cybersecurity vulnerabilities and risk mitigation. ICS-CERT will post this report to its web site once completed.

Federal Facility Control Systems Security Program

New to FY 2016 is the Federal Facility Control Systems Security Program (FFCSSP), a joint effort by ICS-CERT, Federal Protective Services (FPS), and General Services Administration (GSA), to assess control systems (building automation) used by government-owned and leased facilities and occupied by Federal employees for non-military activities. The Facility Security Level (FSL) of each facility's Facility Security Committees (FSC) will determine the prioritization of these assessments. Facilities with a security level of 3, 4, or 5 are considered high-risk facilities and will be ICS-CERT's top priorities at the onset of execution and in sustainment of all risk assessment activities.

The FFCSSP will conduct assessments in Tiers (I, II, and III), and ICS-CERT will be primarily responsible for cybersecurity assessments (Tier III). FPS will be responsible for physical security technology assessments (Tiers I and II) and GSA for the overall responsibility for supporting assessments and applying countermeasures. These assessments involve a comprehensive review of systems and network architectures and encompass topology verification, operational processes, communication protocols, evaluation of security controls, and other areas related to the control system. These assessments also offer detailed mitigation plans and recommendations; FFCSSP will perform them on the most complex and critical facilities in the portfolio. Lastly, the assessments will provide Federal tenants and owner-operators with technical knowledge of their systems and include plans to address security issues as well as provide countermeasures and facility risk factors.

CSET®

CSET is a self-contained software tool that runs on a desktop or laptop computer. CSET provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It does not require connection to the Internet or to any control system or corporate network. CSET guides asset owners and operators through a step-by-step process to evaluate ICS and information technology (IT) network security practices. CSET's developers designed it to focus user time in the areas that are most effective for conducting a self-assessment. The application contains a feature-rich network diagramming capability, provides a comprehensive analysis of the network's adherence to industry recognized cybersecurity standards, and produces executive level, summary, and detailed reports.

ICS-CERT released CSET Version 7.1 in February 2016. This release included:

- **NIST SP800-161**—Supply Chain Risk Management Practices for Federal Information Systems and Organizations. SP800-161 added additional supply chain management controls to CSET.
- **NERC CIP priority list**—Using the NERC Critical Infrastructure Protection (CIP) Violation Risk Factors, CSET now provides a priority ranked list of an asset owner's NERC-CIP controls.
- **Enhanced dashboard**—The CSET team redesigned the gaps analysis dashboard to include additional information, simplified navigation, and improved access to detail charts.
- **Requirements organized by standard**—CSET now presents questions and requirements in the order of the standard. Users can also now perform text searches directly on the question screen, as well as sort and reorder questions based on how they apply to different standards.
- **Custom parameter values**—Users can now enter custom parameter values for standards with requirements that include parameters and they can customize and store these parameter values in CSET.

- **New network components**—The number of network components is double what it was and now includes stencils for ICS, IT, medical, and emergency management radio components.

ICS-CERT released CSET Version 8.0 in September 2016. This release included:

- **Simplified User Interface**—Enhanced and additional assistance to help users select their standards, determine security assurance levels, and prepare for an assessment.
- **HIPAA—**Health Insurance Portability and Accountability Act, the standard for protecting sensitive patient data.
- **SANS CSC top 20**—The Critical Security Controls are a recommended set of actions for cyber defense.
- **CCIs**—Control Correlation Identifiers, descriptions for "singular, actionable statements" that comprise a security control or security best practice.
- **NIST SP800-171**—A standard designed to protect controlled unclassified information (CUI) outside the government.
- **Protected modules**—Custom private questionnaire support. The ability for organizations to request that custom questionnaires be integrated into the tool enabled by a protected key.
- **Custom questionnaires**—Users now have the ability to create custom questionnaires from any of the existing CSET Questions.
- **Enhanced network-diagramming window**—The diagramming functionality is now in its own separate window that provides more screen space and facilitates working other CSET functions independently.
- **Additional network components**—New network components including a System Information and Event Management System (SIEMS), Windows Update Server (WUS), Logging Server, Power over Ethernet Switches and eighteen specialized medical devices.

In FY 2016, ICS-CERT distributed 10,249 copies of CSET in 120 countries.

Training

Training is a fundamental component of any robust cybersecurity strategy. ICS-CERT supports CI sectors and the control system community by offering multiple training courses, ranging in difficulty at numerous locations around the country and online. ICS-CERT provides these trainings specifically for the personnel responsible for the oversight, design, and operation of control systems. All courses are offered free of charge. In FY 2016, the Training team updated the online and classroom course materials 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 and developing two more.

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), and
- Mapping IT Defense-In-Depth Security Solutions to ICS (210W-10).

The Training team designed the 100W course to increase awareness and provide students the tools to recognize potential weaknesses in daily operations. The team designed the 210W series of courses to cover a broad range of topics related to cybersecurity for ICS. For the most comprehensive training, trainees should take the courses in order, 210W-01 through 210W-10.

ICS-CERT classroom training courses are as follows:

- Introduction to Control Systems Cybersecurity (101);
- Intermediate Cybersecurity for Industrial Control Systems—Part 1 (201), lecture only;
- Intermediate Cybersecurity for Industrial Control Systems—Part 2 (202), with lab/exercises; and
- Advanced Cybersecurity for Industrial Control Systems (301), with lab/exercises.

The 101, 201, and 202 courses are available in combination at various locations, multiple times per year. Accompanying hardware and software demonstration systems show exploits and mitigation tactics in the numerous exercises. ICS-CERT Training offers the 301 course in Idaho Falls, Idaho. This course 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.

Training in FY 2016

In FY 2016, 24,350 students registered and 17,773 students completed at least one of the online courses offered. The team hosted regional training sessions for 1,076 attendees in Pittsburgh, Pennsylvania; Baton Rouge, Louisiana; Boston, Massachusetts; and Lisbon, Portugal. ICS-CERT Training presented the Red Team / Blue Team exercise 12 times in FY 2016 and hosted 506 students. In early April, the Training team conducted the pilot of an Incident Responder course and developed a new instructional course for CSET. The team completed a major systems upgrade to the CSAC, integrating additional control system hardware and software into the Red Team/Blue Team exercise networks.

DHS NPPD Under Secretary Suzanne Spaulding presents ICS-CERT's Training team with a DHS NPPD appreciation award.

Feedback from Training attendees:
"Excellent management of the educational balance."
"This is one of the best organized and most effective training courses I have ever attended."

Pittsburgh, Pennsylvania ICS-CERT Regional Training, October 2015

Feedback from Training attendees:
"This is an excellent course. I have paid a lot of money in the past for courses that were not 1/10th as good."

Baton Rouge, Louisiana ICS-CERT Regional Training, February 2016

Feedback from Training attendees:
"The best part of this exercise is the IT/OT joint participation."
"The amount of hands-on is invaluable. Awesome week. Loved it."

Boston, Massachusetts ICS-CERT Regional Training, June 2016

Attendee on what he liked the least about the training:
"That it is over already."

Lisbon, Portugal ICS-CERT Regional Training, September 2016

Scottsdale, Arizona ICS-CERT ICSJWG 2016 Spring Meeting

Industrial Control Systems Joint Working Group

ICS-CERT established the Industrial Control Systems Joint Working Group (ICSJWG) in 2009 to enhance collaboration between ICS stakeholders and to facilitate partnerships between the Federal Government and private sector in all CI sectors. The ICSJWG is a principle 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 provides a vehicle for the ICS community to network, collaborate, and share information freely.

ICSJWG Biannual Face-to-Face Meetings

The focal point of the ICSJWG is the biannual face-to-face meetings. These meetings provide the opportunity for anyone in the ICS community, newcomers and industry veterans alike, to network and share information formally or informally through presentations, panels, training sessions, demonstrations, and ad hoc discussions among peers. The face-to-face meetings are unique in that they target the ICS community and include all sectors, with subject matter experts from private industry, trade associations, information sharing groups, academia, and governmental agencies.

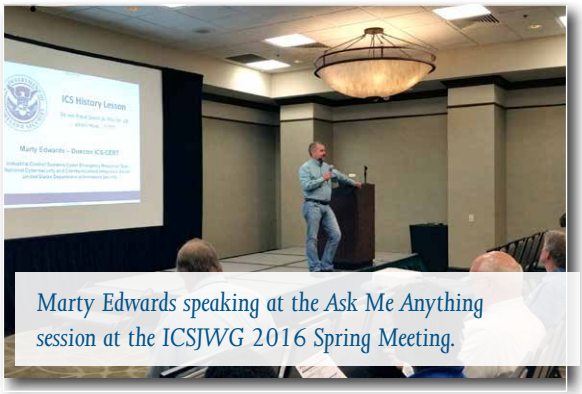
The focus on networking and collaboration is what sets the ICSJWG meetings apart from a mere conference with presentations. ICSJWG members consistently give the face-to-face meetings high ratings for their relevancy and value to their professional lives. ICSJWG meetings are direct reflection of the ICS community, and the ICSJWG Program Management Office (PMO) strives to continuously improve the meetings based on stakeholder feedback.

2016 Spring Meeting

The ICSJWG hosted the 2016 Spring Meeting at Chaparral Suites in Scottsdale, Arizona, from May 3–5. This meeting was the largest to date, bringing together 306 stakeholders from the ICS community. Over the course of three days, attendees had the opportunity to network and interact through demonstrations, presentations, panels, and lightning round talks.

Highlights of the 2016 Spring Meeting:

- Keynote presentations from:
  - Gregory Touhill, Deputy Assistant Secretary for Cybersecurity and Communications, DHS;
  - Frank Grimmelmann, President and CEO of Arizona Cyber Threat Response Alliance (ACTRA);
  - Mark Fabro, President and Chief Scientist of Lofty Perch; and
  - Marty Edwards, Director of ICS-CERT, DHS.
- A hands-on forensics technical workshop that allowed attendees to learn recommended best practices for performing hard drive and memory captures on a live system.
- The ICSJWG's second Vendor Expo, which allowed the ICS vendor community to share its literature, experience, and insight with participants in a booth-type arrangement.
- An Ask Me Anything session with Marty Edwards.



Marty Edwards speaking at the Ask Me Anything session at the ICSJWG 2016 Spring Meeting.

2016 Fall Meeting

The ICSJWG hosted the 2016 Fall Meeting in Fort Lauderdale, Florida, from September 13-15, at the Embassy Suites Fort Lauderdale 17th Street hotel. This meeting brought together over 288 stakeholders from the ICS community and over half of the stakeholders were first-time attendees.

Highlights of the 2016 Fall Meeting:

- Keynote presentations from:
  - Billy Rios, Founder of WhiteScope;
  - Joel Langill, ICS Cybersecurity Subject Matter Expert at AECOM Management Services Group;
  - John Felker, Director of Operations, NCCIC, DHS; and
  - Marty Edwards, Director of ICS-CERT, DHS.
- A hands-on technical workshop and training focused on Network Monitoring of ICS and Google Hacking/ Shodan.
- Plenary panel sessions focused on Vulnerability Coordination and Research.
- An Ask Me Anything session with Marty Edwards.

ICSJWG Webinars

In addition to the biannual meetings, the ICSJWG sponsors ad-hoc webinars to address issues that are of concern to ICS stakeholders. These issues range from technical solutions to problems to newly found vulnerabilities with corresponding mitigation techniques. ICS-CERT has also used ICSJWG resources to produce more technically specific webinars about relevant and high profile issues that affect the entire community. As an example, ICS-CERT representatives conducted a webinar campaign in the aftermath of the Ukraine infrastructure cyber attacks to elucidate some of the findings of the group and explain mitigation techniques and strategies. The ICSJWG PMO will also look to explore methods of turning the most popular presentations from ICSJWG meetings into webinars, so those who are unable to attend meetings in person could enjoy and benefit from the highest-rated presentations.

Other ICSJWG Activities

The ICSJWG also provides informational products to the broader ICS community to raise awareness regarding a particular issue or to address a specific need. In addition, the ICSJWG acts as a vehicle for community members to distribute and receive relevant information from other stakeholders. The ICSJWG Quarterly Newsletter includes relevant information from ICS-CERT along with articles and whitepapers submitted by the community.

The ICSJWG Steering Team

The ICSJWG Steering Team (IST) is composed of the ICSJWG PMO and select volunteers from the ICSJWG community. The IST provides guidance for the ICSJWG and all associated initiatives, with the overall objective of enhancing and growing the collaborative efforts of the ICSJWG, thereby leading to an improved security posture among ICS stakeholders.

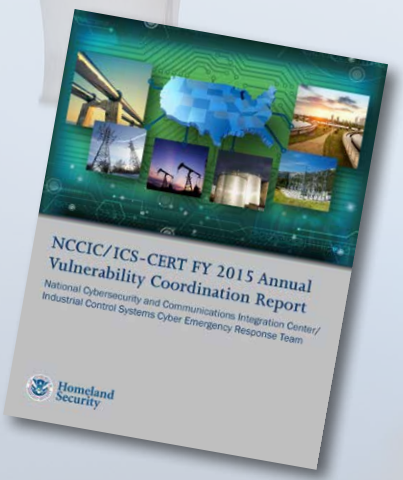
IST representatives are drawn from a variety of different areas in the ICS community, including asset owners, vendors, state/local government officials, consultants/ integrators, and representatives from industry associations, academia, and international organizations. These representatives act as resources and liaisons to the broader ICS community and bring a wealth of knowledge and experience to the effort to continuously improve the ICSJWG and related activities.

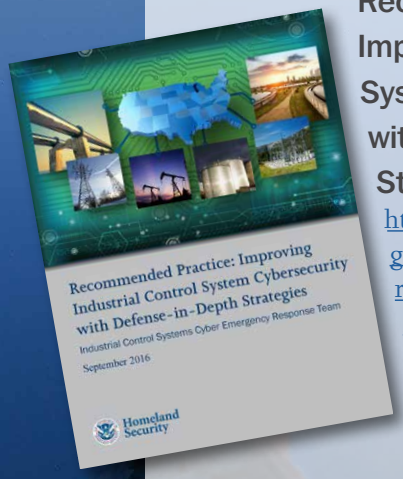
Ft. Lauderdale, Florida ICS-CERT ICSJWG 2016 Fall Meeting

ICS-CERT Information Products Released in 2016

NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report, 8-4-2016
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report, 9-28-2016
https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf





Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, 9-13-2016
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Malware Trends White Paper 11-2-16
https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf

ICS-CERT Monitor

ICS-CERT publishes the Monitor Newsletter bimonthly, six times a year, as a service to personnel actively engaged in the protection of critical infrastructure assets. The Monitor offers a means of promoting preparedness, information sharing, and collaboration with the 16 critical infrastructure sectors. This newsletter highlights recent activities and information products affecting control systems and provides a look ahead at upcoming ICS-CERT events.

The current issue of the Monitor, along with past issues, is available at the following URL: https://ics-cert.us-cert.gov/monitors. If you have questions or comments about the content of the Monitor or if there are topics you would like to see covered, please contact ICS-CERT at ics-cert@hq.dhs.gov.

ICS-CERT MONITOR

Moving Forward

Moving into 2017, ICS-CERT's activities will continue unabated as ICS-CERT looks to improve cybersecurity capabilities and extend services in support of the Nation's 16 CI sectors. ICS-CERT will continue to share timely and focused cybersecurity information with ICS stakeholders, and it stands prepared to meet each new challenge as it comes.

In 2017, the ICS-CERT private sector Assessment team's services will continue transitioning from individual CSET, DAR, and NAVV assessments toward an integrated process including all the assessment offerings along with more advanced analytics to provide improved actionable feedback to asset owners. The team will work with asset owners to determine which set of assessment services best fits the needs of that particular organization. ICS-CERT is actively exploring additional resources that would provide facilitated CSET assessments so that ICS-CERT can focus on the more comprehensive integrated assessment activity mentioned. The team is also working to include log analysis to the overall assessment services.

The CSET team is planning two new releases of CSET again next year. These releases will include new standards such as NIST 800-53 Revision 4, for Information Technology, and the NERC CIP Version 6 standard for the Energy Sector. In addition, a new "discoveries" feature based on ICS-CERT Assessment team onsite visits will provide immediate vulnerability mitigation recommendations for selected issues as part of the analysis process. The Vulnerability Coordination team will be adding additional staff in 2017 to address an increasing ticket workload, and they will be revising the format for alerts and advisories to be more concise and easier to interpret.

Because of high demand, the Training team is planning on a significant increase in the number of Red/Blue (301) training sessions next year and will be conducting a session approximately every three weeks beginning in the spring of 2017. In addition, the number of online training courses will be increased and enhanced with additional graphics and exercises. The Training team will continue to conduct offsite sessions including new venues in the United States and Europe. They are also working to become an accredited provider (AP) of continuing education units (CEU) through the International Association of Continuing Education and Training (IACET), and they expect to complete the process in 2017.

The ICSJWG team will be focusing on improving leadership, coordination, and strategic direction by utilizing the IST to help expand membership and promote additional engagement across all critical infrastructure sectors. ICS-CERT is also looking into additional IST liaison roles, including representation from the Information Sharing and Analysis Center (ISAC) community. ICS-CERT is actively working to identify venues in all 10 designated Federal Emergency Management Agency (FEMA) regions (given the diffuse nature of the ICS community) for ICSJWG biannual meetings to increase awareness of ICS security as a whole.

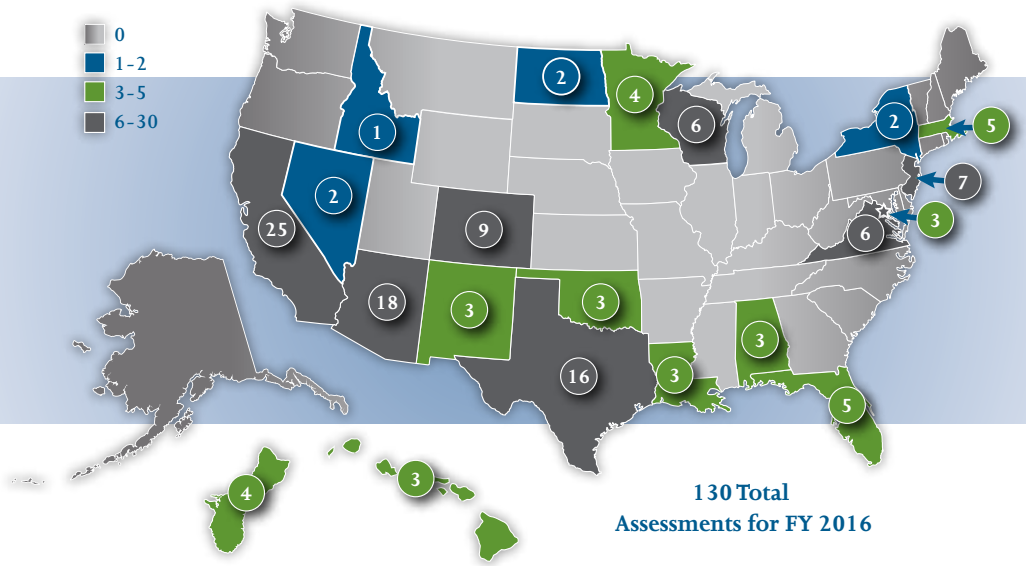
There is no way to know what cybersecurity threats 2017 will bring, but we do know that new threats will emerge. ICS-CERT will continue into 2017 working tirelessly toward its mission to reduce risk to the Nation's CI by strengthening control systems security and resilience through public-private partnerships. To stay apprised of what ICS-CERT is doing in 2017, sign up for our GovDelivery service to be notified of ICS-CERT alerts, advisories, Monitor newsletter, and other product releases. Users can also sign up for a HSIN account for access to NCCIC Portal releases and can follow ICS-CERT on Twitter at the following URL: https://twitter.com/icscert.

ICS-CERT Assessments FY 2016 Metrics

Total FY 2014–2016 onsite assessments by sector.

Sector	FY 2014	FY 2015	FY 2016
Chemical Sector	1	3	7
Commercial Facilities Sector	2	0	4
Communications Sector	0	0	5
Critical Manufacturing Sector	0	0	5
Dams Sector	0	0	2
Defense Industrial Base Sector	0	3	0
Emergency Services Sector	0	10	3
Energy Sector	43	33	22
Financial Services Sector	0	0	0
Food and Agricultural Sector	0	0	3
Government Facilities Sector	5	12	10
Healthcare and Public Health Sector	0	0	0
Information Technology Sector	0	3	3
Nuclear Reactors, Materials, and Waste Sector	5	0	0
Transportation Systems Sector	10	9	10
Water and Wastewater Systems Sector	38	39	56
Totals	**104**	**112**	**130**
Number of Sectors Assessed	**7/16**	**8/16**	**11/16**

FY 2016 Assessments by State



130 Total
Assessments for FY 2016

ICS-CERT Fiscal Year and Calendar Year 2016 Metrics

NCCIC/ICS-CERT FY Metrics	2014	2015	2016
ICS Incident Reports - Tickets	245	295	290
ICS Incident Response Onsite Deployments	4	5	3
ICS Related Vulnerability Reports - Tickets	159	189	187
ICS-CERT Information Products	339	332	274
ICS-CERT Portal Accounts	1,654	1,667	2,360
Distributed or Downloaded CSET®	5,132	7,565	10,249
Onsite Assessments	104	112	130
Professionals Trained	800	1,330	1,622
Number of Training Sessions	21	29	29
ICSJWG Membership	1,726	1,912	2,476
Speaking Engagements	168	342	343

NCCIC/ICS-CERT CY Metrics	2014	2015	2016
ICS Incident Reports - Tickets	232	303	222
ICS Incident Response Onsite Deployments	6	4	2
ICS Related Vulnerability Reports - Tickets	167	177	257
ICS-CERT Information Products	362	316	287
ICS-CERT Portal Accounts	1,944	1,710	1,444
Distributed or Downloaded CSET®	6,364	7,800	10,461
Onsite Assessments	106	130	121
Professionals Trained	1,048	1,542	1,292
Number of Training Sessions	27	29	26
ICSJWG Membership	1,733	2,000	2,491
Speaking Engagements	188	380	323

Contact ICS-CERT

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

U.S. Toll Free: 1-877-776-7585

International: (208) 526-0900

Email: ics-cert@hq.dhs.gov

Web site: https://ics-cert.us-cert.gov

ICS-CERT Report an Incident page: https://ics-cert.us-cert.gov/Report-Incident?

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

Contact NCCIC

NCCIC encourages you to report suspicious cyber activity and vulnerabilities affecting government or critical infrastructure enterprise IT systems.

NCCIC Service Desk and Customer Service

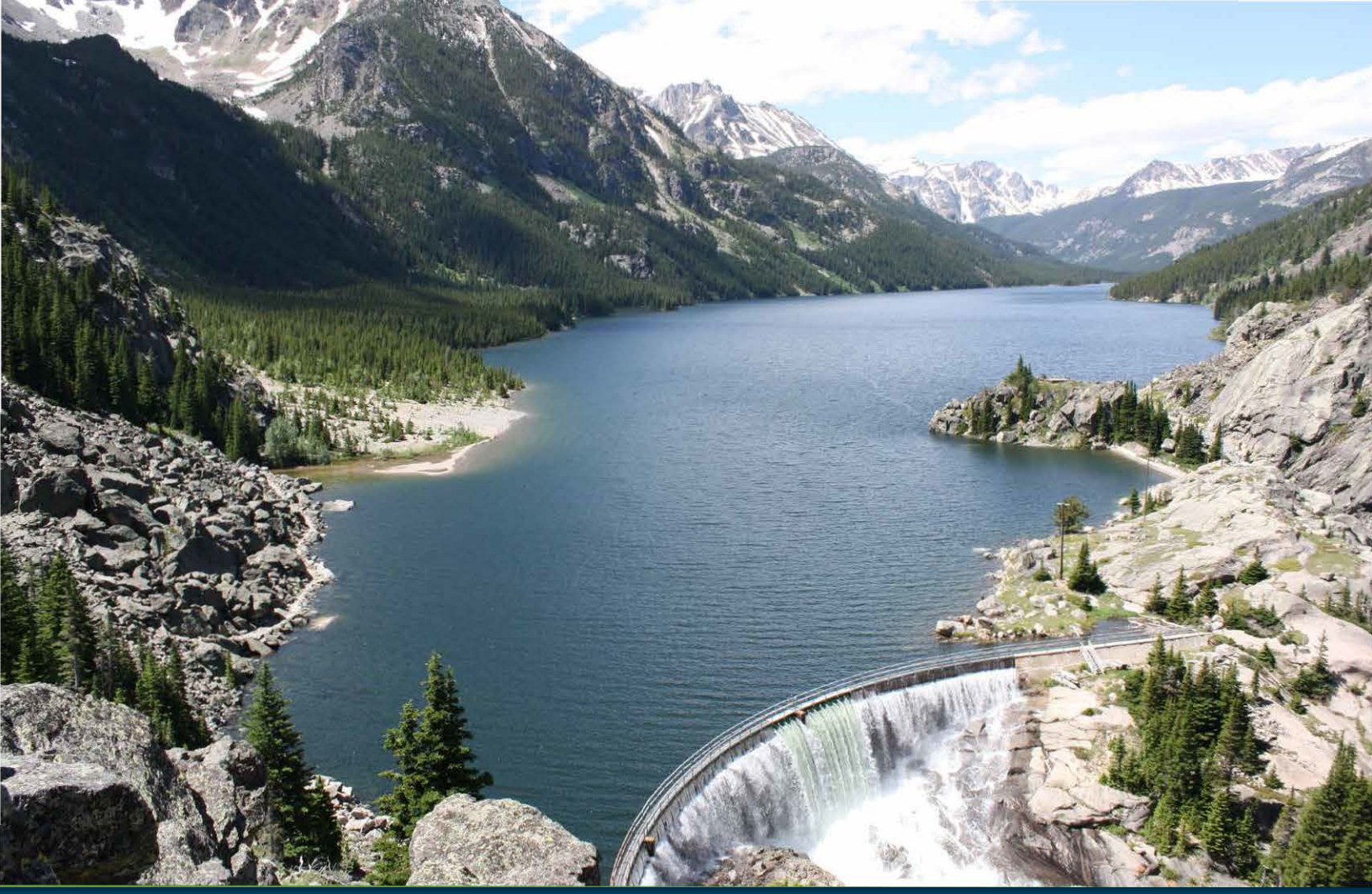
Phone: (888) 282-0870

Email: NCCICCustomerService@hq.dhs.gov

To speak with or to contact the NCCIC Duty officer (24x7)

Phone: (703) 235-5273

Email: NCCIC@hq.dhs.gov



16-50418