ICS-CERT Year in Review

Industrial Control Systems Cyber Emergency Response Team

2014

Homeland Security

National Cybersecurity and Communications Integration Center

What's Inside

Homeland Security

Welcome

As industrial control systems (ICSs) grow more advanced and interconnected, the threat of cyber attack against our Nation's critical infrastructure (CI) grows even greater. Since its inception, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has stayed true to its mission to assist CI asset owners in reducing the risk of cyber attack. Throughout the last 10 years, ICS-CERT has continued to expand and improve its capacity to provide these vital services.

In 2014, the increasing trend of ICS devices connecting directly to the Internet (intentionally or unintentionally) was a serious concern. Shodan, Google, and other search engines have enabled threat actors to easily discover and identify a variety of Internet facing ICS devices. Adding to the threat landscape is the continued scanning and cataloguing of devices known to be susceptible to emerging vulnerabilities such as the "Heartbleed" OpenSSL vulnerability. The search terms needed to identify ICS devices are widely available because of an increasing public body of knowledge with detailed ICS-specific terminology. The availability of this information, coupled with the aforementioned tools, lowers the level of knowledge required to successfully locate Internet facing control systems. In many cases, these devices have not been configured with adequate authentication mechanisms, thereby further increasing the chances of both opportunistic and targeted attempts to directly access these components. As these tools and the capabilities of adversaries advance, we expect that exposed systems will be more effectively discovered and targeted by adversaries.

2014 demonstrated ICS-CERT's ability to grow and evolve to meet the public and private sector needs of CI asset owners. ICS-CERT experienced an increase in onsite assessments, information products released, copies of the Cyber Security Evaluation Tool (CSET®) distributed or downloaded, Industrial Control Systems Joint Working Group (ICSJWG) memberships, speaking engagements, number of training sessions, and professionals trained.

The hard work and dedication of ICS-CERT's personnel resulted in many impressive achievements and highlights over the course of the past year. ICS-CERT conducted an intensive "action campaign" providing classified briefings to the critical infrastructure community on the Havex and BlackEnergy malware threats to ICS. The Vulnerability Coordination and Incident Response Teams released detailed and timely advisories, conducted briefings in 15 cities, and hosted two webinars on the Heartbleed OpenSSL vulnerability and one webinar on the BlackEnergy/Havex threats. The Assessments Team deployed to 21 different states to conduct 104 onsite cybersecurity assessments. The Training Team launched new online training modules incorporating a new blended learning approach. The CSET Development Team released two new versions of CSET, 6.0 in February and 6.1 in August.

While 2015 is sure to bring additional and evolving cybersecurity threats, ICS-CERT is prepared to meet the challenge and support the CI community as we combine efforts to reduce cyber risks that threaten our Nation's CI.

Regards,

Marty Edwards
Director
Industrial Control Systems Cyber Emergency Response Team
Department of Homeland Security
ICSJWG Government Coordinating Council (GCC) Chair

ICS-CERT Introduction

America's economic and national security relies on the resilience and reliability of the Nation's critical infrastructure (CI). Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," identifies 16 CI sectors (see table below).

The Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) mission is to assist owners of CI in the 16 sectors to improve the overall cybersecurity posture of their industrial control systems (ICSs). In addition to working with ICS owners, operators, and vendors, ICS-CERT coordinates its efforts with Federal, state, local, and tribal governments. ICS-CERT operates within the National Cybersecurity and Communications Integration Center (NCCIC), a division of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD).

NCCIC's mission is to operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains.

ICS-CERT's activities are composed of four operations functions and four risk reduction functions. Operations functions include incident response, vulnerability coordination, situational awareness, and technical analysis. Risk reduction functions include cybersecurity assessments, the Cyber Security Evaluation Tool (CSET), training, and the Industrial Control Systems Joint Working Group (ICSJWG).

CI asset owners benefit from ICS-CERT's cybersecurity services in many ways, including an increased awareness of emerging threats, state-of-the-art analysis, incident response support, established partnerships, and collaboration with other agencies and partners. By extension, Americans benefit from ICS-CERT's work with access to a more secure and resilient CI, which undergirds our economy and provides many of the critical services we rely on every day.

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

ICS-CERT 2014 Highlights

- **Havex and BlackEnergy Activities:** The ICS-CERT Team conducted an action campaign to provide classified briefings with contextual and detailed information about Havex and BlackEnergy malware for private sector CI asset owners. These briefings covered 15 cities, from November 25 through December 11. ICS-CERT also hosted a webinar and released multiple alerts and advisories with detailed actionable information related to the malware characteristics as well as methods for detecting compromise and improving cyber defenses. ICS-CERT reached nearly 1,400 participants across all 16 CI sectors with these briefings.
- **Heartbleed OpenSSL Activities:** The Vulnerability Coordination Team released detailed and timely advisories, conducted briefings, and hosted two webinars featuring the original researchers who discovered the Heartbleed OpenSSL vulnerability. The team acted quickly to identify affected ICS products and developed multiple alerts in coordination with the vendor community to prevent any major incidents.
- **Onsite Assessments:** The ICS-CERT Assessments Team deployed to 21 different states, conducting 104 onsite cybersecurity assessments to assist CI asset owners in strengthening the overall cybersecurity posture of their ICSs.
- **"Safeguard" Assessments:** ICS-CERT and the Federal Energy Regulatory Commission's (FERC) Office of Energy Infrastructure Security (OEIS) introduced a new technical service offering entitled "Safeguard." This engagement provided select asset owners with proactive and customized cyber assessment services based on their specific interest and area of focus.
- **Online Training:** The ICS-CERT Training Team launched new online training modules with a blended learning approach, which makes accessing course material easier and more efficient, reduces redundancy in training materials, and eliminates the need to travel to participate in ICS-CERT training.
- **CSET Tool:** The CSET Development Team released two new versions of CSET in 2014, CSET 6.0 in February and CSET 6.1 in August. The latest version includes the National Institute of Standards and Technology (NIST) Framework, which allows asset owners to create their own question sets and provides industry organizations the ability to collaborate in creating and sharing question sets.

Photo credit: Stephen Barrett / DHS OPA

ICS-CERT Watch Floor Operations

Information Sharing and Situational Awareness

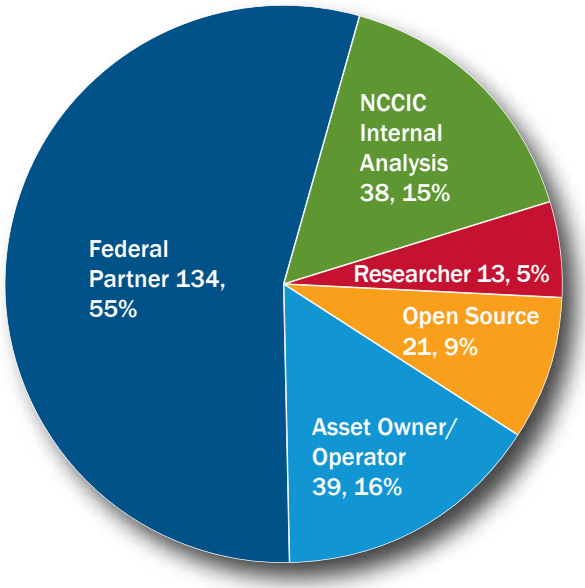
The ICS-CERT watch floor is staffed by approximately two dozen analysts and incident handlers across two geographically separate watch floor locations. These watch floors handled numerous operational activities, which include responding to reported cyber incidents, providing recovery and mitigation support, vulnerability coordination and analysis, interfacing with law enforcement and the Intelligence Community, and providing situational awareness alerts and advisories to warn of cyber threats affecting the Nation's critical infrastructure. In 2014, ICS-CERT expanded its information sharing initiatives through webinars and teleconferences with public and private sector partners. ICS-CERT also works closely with Information Sharing Analysis Centers (ISACs), researchers, vendors, sector specific agencies, 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.

In 2014, ICS-CERT tracked and responded to multiple newly discovered cyber campaigns that had been ongoing for several years. The delayed time to discovery, coupled with the tactics of the threat actors, was of great concern to ICS-CERT, particularly when considering the potential for a large victim footprint across the Nation's CI sectors. Accordingly, ICS-CERT leveraged well-established relationships to encourage asset owners to be more proactive in reporting incidents, which then provided a better understanding of the depth and breadth of these campaigns by sophisticated threat actors. Asset owners

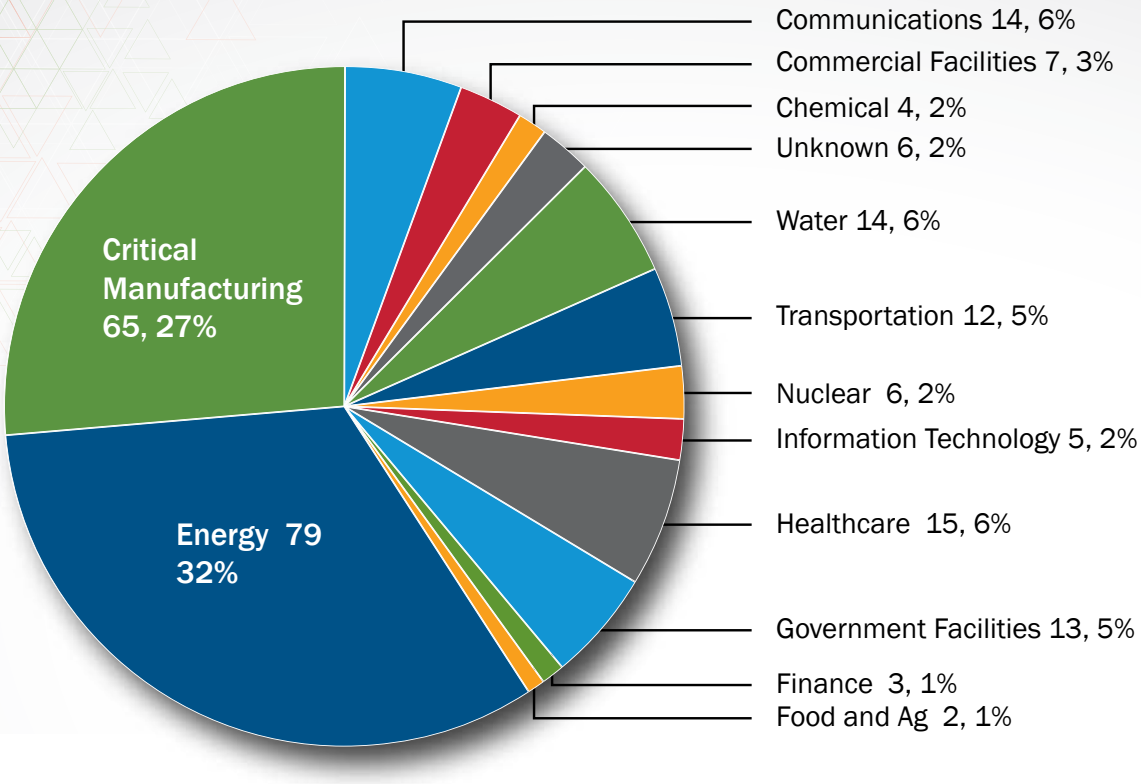
from across all CI sectors responded by engaging in briefings, webinars, and teleconferences and by reporting cyber activity to ICS-CERT. In 2014, ICS-CERT continued to strengthen its trusted relationships with asset owners as they reported cyber incidents impacting their networks and utilized situational awareness information to detect intrusions and improve their defensive posture. The number of returning customers also increased in 2014 as partners shared information on observed threat activity, which was then used, anonymously, to develop alerts and warn the entire community. The frequent reporting, information exchanges, and situational awareness updates have all helped lower the overall risk to CI.

The watch floors also coordinated with other sections of the ICS-CERT to provide all aspects of incident response services, including digital media analysis, onsite response, and recommendations for improving cyber defenses.

Who is Reporting Cyber Incidents



FY 2014 incidents reported by reporting entity (245 total).



FY 2014 incidents reported by sector (245 total).

Incident Response

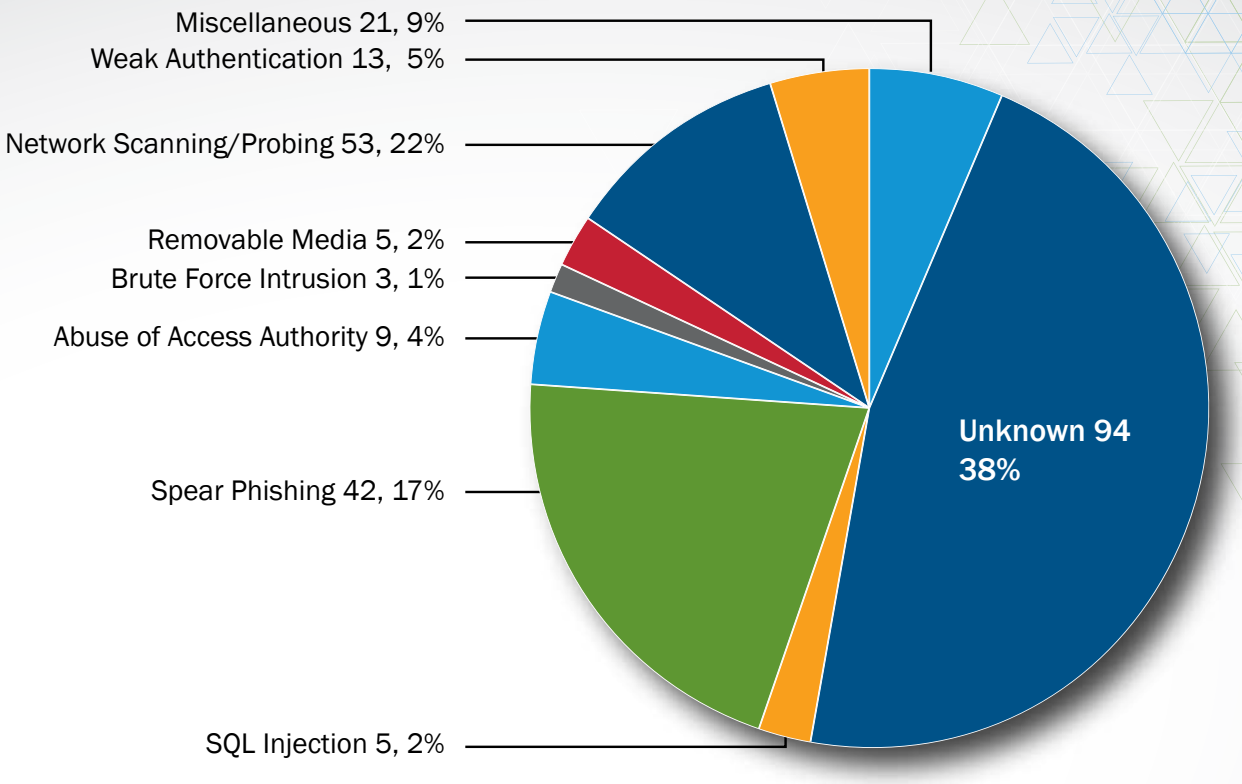
ICS-CERT supports CI asset owners by responding to cyber incidents, emerging threats, and vulnerabilities impacting organizations that operate ICSs. An essential element of our mission success is the coordination effort with partners across all 16 CI sectors.

In addition, ICS-CERT 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.

Incident response is fundamental to ICS-CERT's mission to assist CI asset owners in reducing cyber risks to critical infrastructure. 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. These mitigations are specific to the cyber threat and needs of the organization.

In FY 2014, ICS-CERT received and responded to 245 incidents as reported by asset owners and industry partners. The scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure, including but not limited to the following:

- Unauthorized access and exploitation of Internet facing ICS/Supervisory Control and Data Acquisition (SCADA) devices,
- Exploitation of zero-day vulnerabilities in control system devices and software,
- Malware infections within air-gapped control system networks,
- Structured Query Language (SQL) injection and application vulnerability exploitation,
- Network scanning and probing,
- Lateral movement between network zones,
- Targeted spear-phishing campaigns, and
- Strategic web site compromises (a.k.a., watering hole attacks).



FY 2014 incidents reported by access vector (245 total).

In FY 2014, ICS-CERT observed greater variety in the characteristics of the reported incidents. Whereas spear phishing is still a popular infection vector because of its effectiveness, a wider variety of techniques was reported this year. While ICS-CERT has previously observed strategic watering hole attacks, a new technique uses trojanized software installers at various vendors' sites to install malware on the unsuspecting user's network along with the software update. Many of the victims were unaware they were compromised. As expected, social engineering continued to be a popular attack method, enhanced by the use of social media. In some cases, this yielded greater success for attackers.

The year also saw multiple malware families targeting ICS-specific functionality, underscoring the evolving landscape and the recognition by adversaries of high-stakes ICS targets. In response to these and other threats, ICS-CERT provided remote and onsite incident response support, conducted technical analysis of artifacts and malware, and developed mitigation strategies for owners and operators. In coordination with the Federal Bureau of Investigation (FBI), ICS-CERT launched a call to action campaign providing classified briefings in 15 cities, a secret-level secure video teleconference, and an unclassified webinar. The purpose of this campaign was to inform private sector CI stakeholders of the threat and to provide mitigation strategies for detecting and defending against malicious activity. ICS-CERT issued several alerts with detailed information regarding the malware, as well as detection signatures to aid in identifying if the malware files are present on a given system.

Sharing information about cyber incidents is essential to improving the overall security posture of our Nation's CI. We encourage CI asset owners to contact ICS-CERT for assistance with responding to a cyber incident affecting the control systems environment. ICS-CERT is able to leverage the breadth of knowledge available through our government and community partnerships to improve awareness and provide actionable information to the entire community, without disclosing the identity or sensitive information about the reporting organization.

Vulnerability Coordination

ICS-CERT coordinates vulnerability activities with ICS owners, operators, and vendors and with Federal, state, local, and tribal governments to reduce the likelihood of a successful cyber attack against CI control systems.

The ICS-CERT vulnerability handling process involves five basic steps: 1) detection and collection, 2) analysis, 3) mitigation coordination, 4) application of mitigation, and 5) disclosure. ICS-CERT attempts to coordinate all reported vulnerabilities with the associated vendor and works to publicly disclose the vulnerabilities in a timely manner.

In November 2014, the Vulnerability Coordination team released a Vulnerability Coordination report detailing its activities from 2010–2013. This report provides trend analysis for all vulnerabilities reported to ICS-CERT and gives descriptions, details, and metrics for the most commonly identified vulnerabilities. The report shows that improper input validation, at 61 percent of reported vulnerabilities, is by far the most common.

Heartbleed Vulnerability

The Vulnerability Coordination team devoted a significant amount of time and effort to combating the Heartbleed OpenSSL vulnerability in 2014. These efforts resulted in the release of several advisories, briefings, and two webinars on the topic. The advisories listed vendors and products reported to be vulnerable and announced vendor patches as soon as they became available. The advisories also included methods for asset owners to determine whether they were running vulnerable products. To defend against exploitation, Snort signatures and other signatures suggested by the FBI were provided to asset owners for use in determining if they were actively being exploited. ICS-CERT's first webinar on the Heartbleed OpenSSL vulnerability was aimed at a more limited audience of vendors and some asset owners. The second webinar was open to a wider audience. Each webinar featured an explanation of Heartbleed from the original researchers who discovered the vulnerability.

Technical Analysis

The Advanced Analytical Laboratory (AAL) 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 perform forensic analysis on digital media, reverse engineer malware, and 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. In 2014, the AAL focused on automating and streamlining the lab's analytical capabilities. Improvements for the year included the following:

- Completion of a remote incident response network (RIRN). The RIRN allows analysts to remotely and securely perform an incident response engagement with an asset owner. After an initial equipment installation, AAL analysts can remotely sweep the asset owner's network for indications of compromise. This allows analysts to spend multiple weeks on an engagement and provides a thorough, in-depth examination of the company's network.
- 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 companies responding to a compromise.
- Development of a custom application, called the Correlating Extensive Incident Response (CEIR) tool, to analyze data collected during an incident response. The CEIR tool allows the user to consolidate the many types of data collected into a single, user-friendly database and helps identify known and unknown threats. The AAL uses the CEIR tool in both onsite and remote incident response engagements.

With these improved analytical capabilities, the AAL performed in-depth analysis of numerous malware samples associated with multiple watering hole and ICS-focused threat campaigns. These efforts helped uncover sophisticated threat actor techniques and tactics, which allowed ICS-CERT to publish multiple alerts warning the community of the threat and providing information for detecting and mitigating intrusion activity.

Assessments

In FY 2014, ICS-CERT conducted 104 onsite cybersecurity assessments. These assessments, which are based on standards, guidelines, and best practices, assist the Nation's CI asset owners to strengthen the cybersecurity posture of their ICSs. 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.

ICS-CERT's onsite cybersecurity assessment services include the following assessment types:

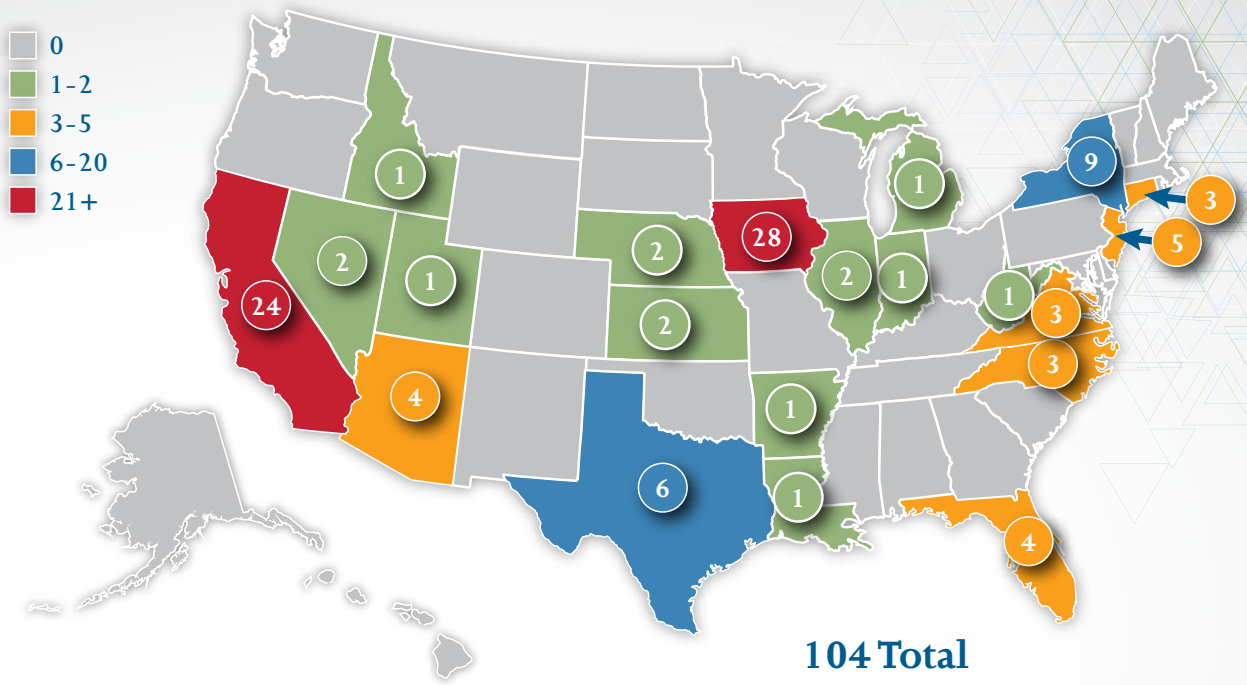
- Onsite guided Cyber Security Evaluation Tool (CSET) Assessment
- Design Architecture Review (DAR)
- Network Architecture Verification and Validation (NAVV).

CSET is a stand-alone software tool that enables users to assess their network and cybersecurity methodology against recognized industry and government standards, guidelines, and best practices. ICS-CERT released two new versions of the CSET tool in 2014: CSET 6.0, released in February, included the ability to trend, compare, and merge assessments; and CSET 6.1, released in August, included the NIST Framework, which allows asset owners to create their own question sets and provides industry organizations the ability to collaborate in creating and sharing question sets.

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 guidance, 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 owner 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

FY 2014 Onsite Assessments



104 Total Assessments for FY 2014

Total FY 2014 ICS-CERT onsite assessments by state.

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.

In addition to these assessment offerings, in FY 2014, ICS-CERT and FERC's OEIS introduced a new proactive technical service offering entitled "Safeguard." These one-week engagements provide select asset owners with a menu of various proactive service offerings, which are tailored and customized based on the asset owner's specific interest and area of focus. Some common examples of services performed for these engagements include the following:

- Facilitated control systems security assessments and network architecture reviews,
- Passive network-based validation and detailed analysis of control system network traffic,
- Active host-based scanning for indicators of compromise and anomalous behavior (within an organization's enterprise environment).

In FY 2014, ICS-CERT completed six Safeguard assessments. These services provide enhanced value for asset owners during a week-long engagement, including the following:

- Verification and validation of security controls, based on the current threat landscape and an understanding of adversarial capabilities and tactics
- Relationship building and collaboration with DHS
- Tailored and prioritized recommendations and guidance based on an organization's existing architecture, security controls, and security posture.

Total FY 2014 onsite assessments by type.

Type of Assessment	Fiscal Year 2014
CSET	49
DAR	35
NAVV	18
Enterprise Host-Based Analysis	2
FY 2014 Totals	104

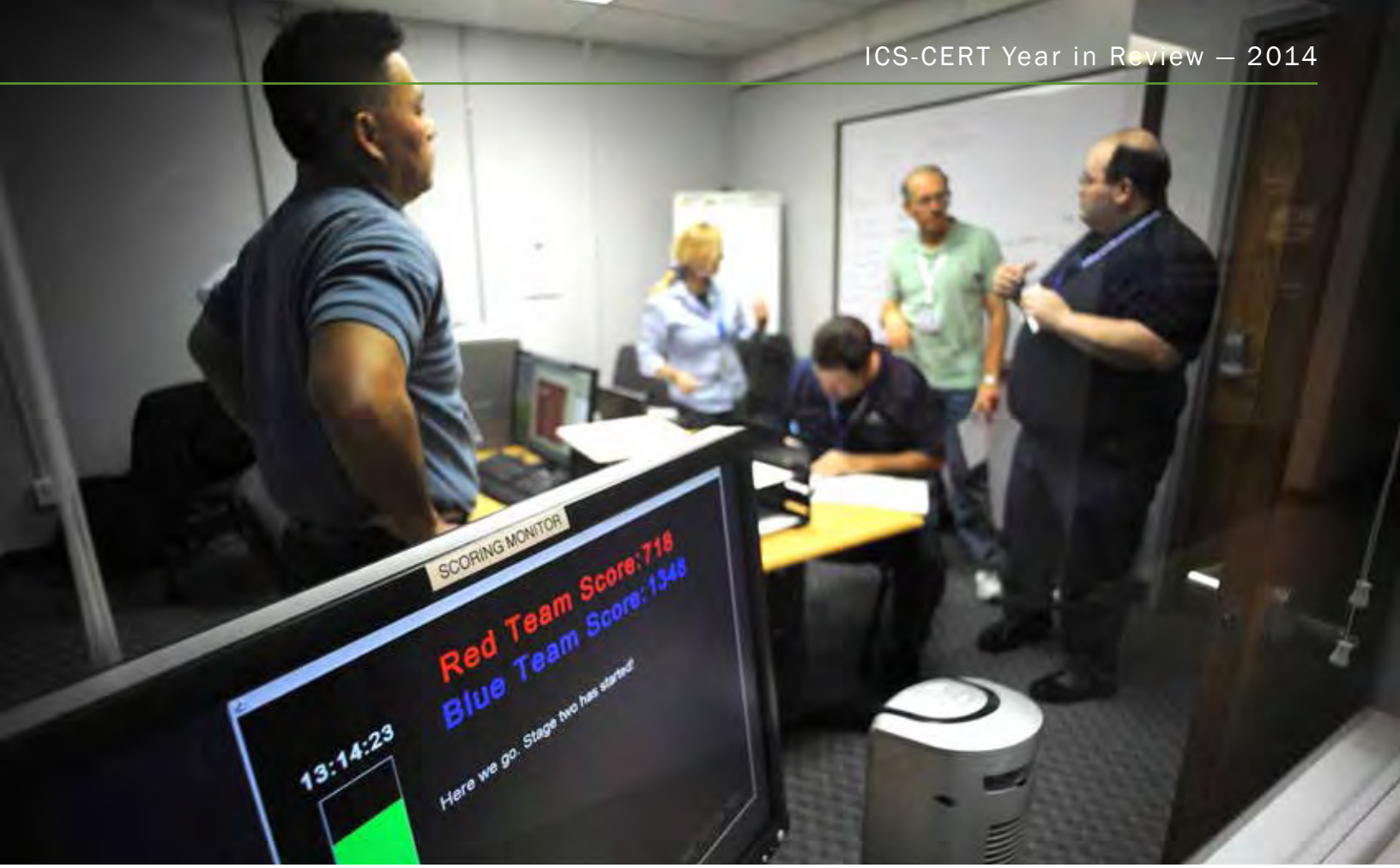
Training

Training is a critical component of the ICS-CERT program. ICS-CERT performs outreach activities through training and education programs to help CI sectors and the control systems community better understand the cybersecurity risks associated with ICSs. In 2014, the program adopted a blended learning approach to enhance training opportunities. A new course, Introduction to ICS Cybersecurity, blends web-based and instructor-led methods. The curriculum is made up of ten modules and is available online at no cost.

The challenges solved by the blended learning approach are three-fold. First, trainees have asked for materials in a format that is more efficient and easier to access. Web-based training allows trainees to access the course on their own time in a setting that allows for asynchronous interaction, and it is self-paced to better fit trainees' work schedules.

The second challenge was to reduce redundancy in the training materials. As the ICS-CERT Cybersecurity Training Program has matured and developed new course materials to support its growth, the courses were designed to build on each other. Ideally, a trainee would complete the Introduction to ICS Cybersecurity course, followed by Intermediate Level courses, and eventually complete the 5-day, hands-on Technical Level ICS Cybersecurity Training. These courses have no prerequisites for enrolling and include a test-out option. As a result, trainees can begin courses at the level appropriate to their cybersecurity experience and knowledge with the confidence that they are prepared for the more technical course work. To further streamline the online training process and eliminate redundancy, ICS-CERT has removed remedial material from the more technical courses.

The third challenge for some people is the travel required to participate in training. Web-based courses alleviate the time, cost, and inconvenience of traveling to attend multiple in-person sessions.



In addition to blending methods and creating web-based modules, the program employs a learning management system (LMS). The LMS is a software application for the administration, documentation, tracking, reporting, and delivery of training courses. The benefits of this service are as follows:

- Creates a unique user ID and provides credit for course completion.
- Provides training courses using varied multimedia approaches (video, audio, PowerPoint, Flash).
- Facilitates interoperability between eLearning software products through compliance with Sharable Content Object Reference Model (SCORM) web-based training courses.
- Enables live training events, training invitations, self-registration, and attendance tracking.
- Assists in tracking, analyzing, and reporting course statistics.
- Ensures course availability on desktop or mobile device (iPads, iPhones, or Android devices).

Over 4,760 trainees have initiated online training and have accessed the courses from multiple states and countries.

Additional ICS-CERT Training highlights for 2014 include the following:

- Initiated online introductory and intermediate courses in 10 modules.
- Resumed quarterly regional training, which takes introductory and intermediate classroom training to trainees in their own region. In 2014, regional classroom training was held in Alabama and Houston. Five regional classroom training sessions are planned for 2015.
- Provided 11 technical-level cybersecurity training sessions to 436 participants. These 5-day courses provide intensive hands-on training and a 12-hour, red team/blue team exercise that simulates a corporate espionage scenario.

Industrial Control Systems Joint Working Group

The 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 goal of the ICSJWG is to secure CI by accelerating the design, development, and deployment of secure ICS.

2014 Spring Meeting

The ICSJWG 2014 Spring Meeting was held in Indianapolis, Indiana, and was attended by approximately 220 people, including asset owners and operators, government professionals, vendors, systems integrators, and academic professionals from around the globe. Key highlights from the meeting were an opening keynote presentation by Indiana Governor Mike Pence as well as two more keynote presentations from CS&C Deputy Assistant Secretary Gregory Touhill and NCCIC Director Larry Zelvin. Presentations also included demos and lightning round talks that offered the opportunity for attendees to discuss the latest initiatives impacting the security of ICSs and the risk of threats and vulnerabilities to these systems.

2014 Fall Meeting

The ICSJWG 2014 Fall Meeting was held in Idaho Falls, Idaho, hosting approximately 175 attendees from the worldwide community. This meeting included a classified briefing and tours of the Idaho National Laboratory facilities. Further highlights include keynote remarks by the DHS Assistant Secretary for CS&C, Dr. Andy Ozment. Because of the positive reception of demonstrations and lightning round talks in previous meetings, those venues were expanded to allow more opportunity for participation.

The ICSJWG Steering Team

The ICSJWG Steering Team (IST) held its first face-to-face meeting in Indianapolis and discussed a variety of topics, including ways to improve the ICSJWG bi-annual meetings and the overall working group moving forward. The IST is made up of members representing roles such as asset owners; vendors; state, local, and tribal governments; industry associations; university/academia; consultants/integrators; and the international community. By bringing this diverse group together, the ICSJWG hopes to improve the partnership between the public and private sectors in working together to secure our Nation's CI.

ICSJWG Webinars

Another outreach opportunity the ICSJWG has offered to the community is a series of webinars that focus on specific topics related to ICS cybersecurity. During FY 2014, ICSJWG webinars covered various topics, including the following:

- I Think, Therefore I Fuzz—demonstration explaining the fuzzing process and how fuzzing can help users find their systems' vulnerabilities before attackers.
- Online Real Time Monitoring for Change Identification—introduction to the Sophia software tool that assists control system owners in learning how their systems communicate and quickly identify new and unexpected connections.
- The New Paradigm for Information Security: Assumption of Breach—review and discussion of the change from a defined perimeter defense to an assumption of breach of critical systems and suggestions on how to respond.

The ICSJWG is looking forward to offering a flexible and resilient approach as well as a substantial platform for the public and private sectors to collaborate on cybersecurity for the global infrastructure in FY 2015.

Moving Forward

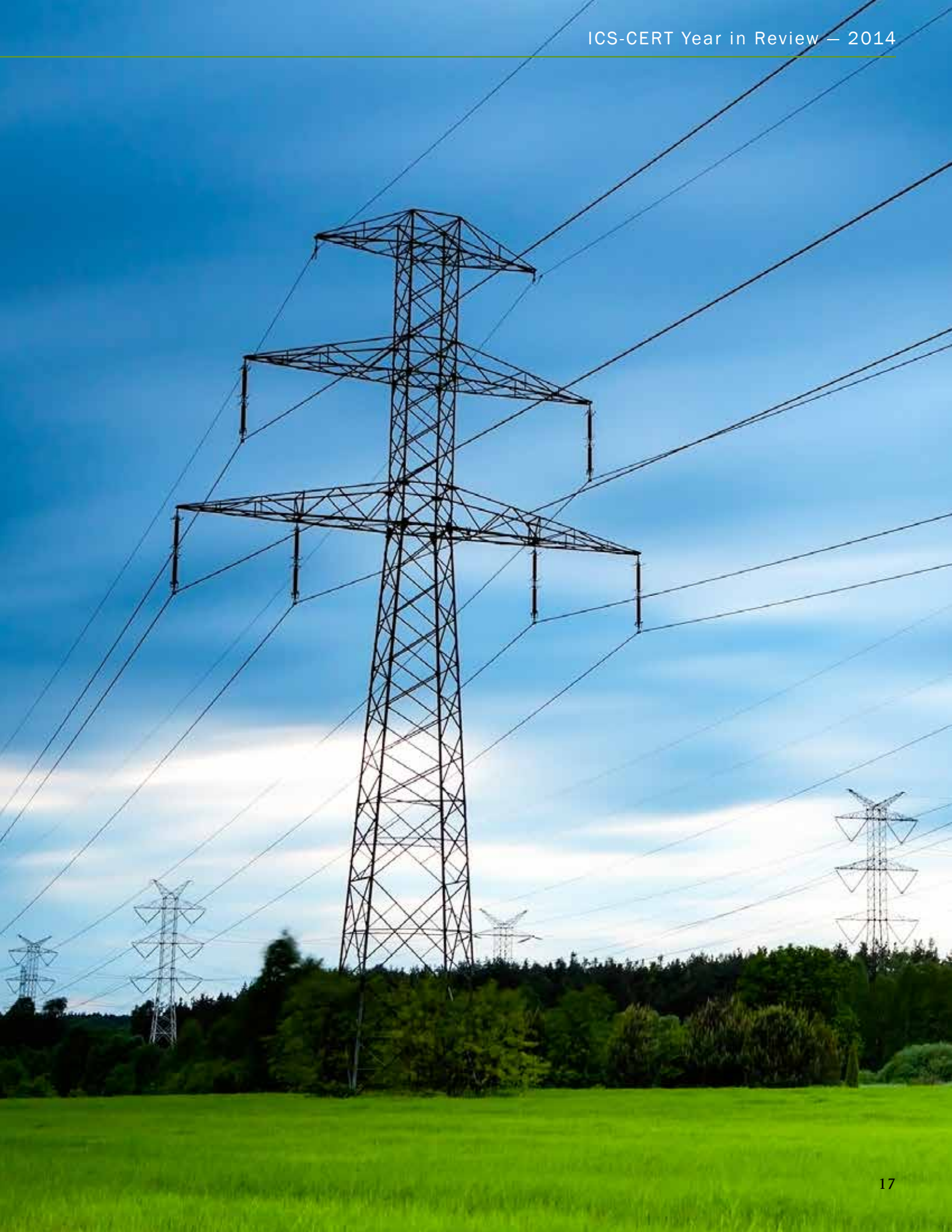
In 2015, ICS-CERT will continue to improve cybersecurity capabilities and extend services in support of all ICS stakeholders in the 16 CI sectors. ICS-CERT will continue coordination efforts with industry and government partners to mitigate cyber risks to CI through timely and effective sharing of situational awareness information and mitigation strategies.

To further improve onsite assessments, ICS-CERT will pursue more one-on-one engagements with CI asset owners on the use of CSET and assist them in identifying gaps and developing strategies for improving their defensive posture. The Assessment team's SafeGuard Initiative will also further aid asset owners in the Energy industry to assess critical assets for intrusion and security gaps.

In addition to extending onsite assessments, ICS-CERT will develop and publish control system specific technical guidance related to recommended practices and defensive strategies for protecting against ever-evolving threats. These guidance documents will send a clear message about what ICS-CERT finds important and which threats are of greatest concern.

Other goals for 2015 include improving and expanding ICS-CERT technical teams and tools, which will provide greater value during incident response and assessment activities. We will also continue to improve training offerings and expanded training curriculum, which will allow CI asset owners to better meet the demands of challenging and evolving technical issues in control system security.

It is uncertain what new cybersecurity threats will emerge in 2015, but ICS-CERT stands prepared to meet the challenge and help CI asset owners prevent attacks or mitigate their harmful effects.



Sector Specific Onsite Support FY 2014

This table compares the overall sector support statistics for onsite assessments in Fiscal Years 2012, 2013, and 2014.

Sector	FY 2012	FY 2013	FY 2014
Chemical Sector	4	0	1
Commercial Facilities Sector	2	0	2
Communications Sector	0	2	0
Critical Manufacturing Sector	1	0	0
Dams Sector	0	0	0
Defense Industrial Base Sector	12	1	0
Emergency Services Sector	3	0	0
Energy Sector	7	18	43
Financial Services Sector	6	0	0
Food and Agricultural Sector	0	0	0
Government Facilities Sector	3	2	5
Healthcare and Public Health Sector	1	5	0
Information Technology Sector	5	2	0
Nuclear Reactors, Materials, and Waste Sector	8	8	5
Transportation Systems Sector	10	10	10
Water and Wastewater Systems Sector	25	24	38
Totals	87	72	104
Number of Sectors Assessed	13/16	9/16	7/16

ICS-CERT FY 2014 Metrics

This table compares the overall incident, vulnerability, onsite event, and information product statistics for Fiscal Years 2012, 2013, and 2014, indicating control system cyber events and activity.

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

ICS-CERT CY 2014 Metrics

This table compares the overall incident, vulnerability, onsite event, and information product statistics for Calendar Years 2012, 2013, and 2014, indicating control system cyber events and activity.

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

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

National Cybersecurity and Communications Integration Center

14-50426

Homeland Security

ICS CYBERSECURITY FOR THE C-LEVEL

Cyber threats against Industrial Control Systems (ICS) continue to increase in intensity, frequency, and complexity. Yet, basic cybersecurity practices within many ICS organizations continue to be an afterthought or significantly less than needed. This document was developed as a tool to help facilitate the communication of strong, basic cybersecurity principles to the leadership of ICS organizations.

Through conversation with various stakeholders, the need for a document that conveys concise cybersecurity concepts and strategies to organizational leadership became apparent. Thus, the U.S. Department of Homeland Security's (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT), with direction from the Industrial Control System Joint Working Group (ICSJWG), developed this document to support communication and improve cybersecurity practices across the Nation's critical infrastructure (CI).

ICS ATTACKS - GROWING SOPHISTICATION

Attacks that target ICS infrastructure continue to evolve and mature. Through a variety of methods, malicious threat actors are introducing sophisticated malware into control systems at growing rates. The following case studies, Havex and BlackEnergy, represent sophisticated, global malware campaigns against ICS that went unnoticed for years. These examples evidence the ability of threat actors to remotely issue command functions via malicious code.

HAVEX

Sophisticated threat actors using Havex malware have targeted and compromised control systems worldwide since 2013. Spear phishing along with infected ICS software downloads from legitimate websites have been the main attack vectors. The Havex malware operates as a Remote Access Trojan (RAT) with the ability to inject unauthorized control commands as well as cause a denial of service effect on certain applications.

BLACKENERGY

The BlackEnergy campaign used previously unknown software vulnerabilities in multiple common Human Machine Interface (HMI) software products to gain direct access to control system operating screens. Since 2011, BlackEnergy has infected dozens of control systems in the U.S. and hundreds globally. The malicious code could potentially be used to manipulate control processes and cause physical damage. No interaction with the target was required as BlackEnergy targeted systems connected **directly to the internet.**

LONG-TERM THREAT

These two campaigns illustrate a concerted effort by sophisticated threat actors for at least four years to understand critical ICS, discover unknown/ unpatched vulnerabilities for exploitation, and use differing techniques to gain access to the operational environment.

SIX QUESTIONS EVERY C-LEVEL EXECUTIVE SHOULD BE ASKING

1) What's at Risk – have we prioritized our assets and identified the potential consequences if our control system was compromised? Can we sustain operations of critical processes following a cyber incident?

2) Who is the manager ultimately responsible for cybersecurity or do we rely on third-party support?

3) Is our ICS environment protected from the Internet and how have we validated that?

4) Do we have remote access to our ICS network? If so, why do we need it, and how is it protected and monitored?

5) Do we have an ICS-CERT Portal Account to receive alerts and advisories?

6) Are we reading available resources and applying the recommended cybersecurity best practices?

Homeland Security

KEY RISK MANAGEMENT CONCEPTS

Identify Critical Assets – Assess the Risk
Complete a risk assessment to ascertain areas of greatest vulnerability, identify critical assets, and define the parameters for your security plan. Perform a baseline cybersecurity assessment via NIST's "Guide to Industrial Control Systems (ICS) Security" or DHS' Cyber Security Evaluation Tool (CSET).

Assign a Manager Responsible for Cybersecurity
Every organization needs a trained and qualified individual whose primary responsibility is cyber-security. A cybersecurity manager should set policies and implement procedures, enforce monitoring and protective/detective controls, train employees, perform regular assessments, and implement patching and configuration practices.

Protect Your Networks from the Internet
Do NOT allow direct connectivity from the internet to your ICS network. Protect your network from remote access via defensive measures, monitoring, and strong authentication requirements. Isolate, protect, and monitor your key assets.

Limit the Use of Remote Access to Your ICS
If remote access is required, protect your ICS with multiple defensive layers. Consider using different levels of access and appropriate controls for remote access, coupled with strong detection/ monitoring capabilities. Implement a control system demilitarized zone (DMZ) with two-factor authentication and a virtual private network (VPN) connection.

Join the ICS-CERT Portal
Joining the ICS-CERT Portal allows access to alerts and advisories, indicators of compromise, and a secure method of reporting cyber incidents and requesting incident response services.

Take Advantage of Available Resources
Participate in your sector's Information Sharing and Analysis Center (ISAC) information sharing programs, know your Sector Specific Agency (SSA), and visit the ICS-CERT website.

ICS-CERT RESOURCES AND ASSISTANCE

ICS-CERT operates within the National Cybersecurity and Communications Integration Center (NCCIC), a division of the DHS Office of Cybersecurity and Communications (CS&C). NCCIC/ICS-CERT is an integral component of the DHS Strategy for Securing Control Systems and strives to reduce risks and threats to CI by collaborating with other government and private sector partners.

ICS-CERT provides or sponsors the following services and activities to improve CI security:

- **OUTREACH AND TRAINING** – ICS-CERT performs outreach activities to help CI sectors understand cybersecurity risks and offers training opportunities to assist the control systems community in improving their cybersecurity preparedness.
- **ICSJWG** – The ICSJWG facilitates partnerships between the Federal government and private sector owners and operators in all CI sectors through biannual face-to-face meetings, webinars, and newsletters.
- **CSET** – CSET is a desktop software tool that enables users to self-assess their network and ICS security practices against recognized standards, guidelines, and recommended practices.
- **SITE ASSISTANCE AND EVALUATIONS** – ICS-CERT offers onsite field assessments, network design architectural reviews, and network traffic analysis and verification.

CONTACT ICS-CERT

For more information about ICS-CERT, please visit our web site: https://ics-cert.us-cert.gov/.

To contact ICS-CERT with a question, or to report a cyber incident, please send email to: ics-cert@hq.dhs.gov, or call: (877) 776-7585.