ICS-CERT Year in Review

Industrial Control Systems Cyber Emergency Response Team

2012

Homeland Security

What's Inside

Homeland Security

Welcome

This year, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) developed tools and capabilities to assist asset owners with incident handling and response efforts. ICS-CERT correlates emerging cyber incidents with previous events and tracks known threat actors based on their techniques and tactics. The information these tools and capabilities yield is leveraged to provide situational awareness information for the greater industrial control system community.

Our team accomplished several key initiatives in 2012 including:

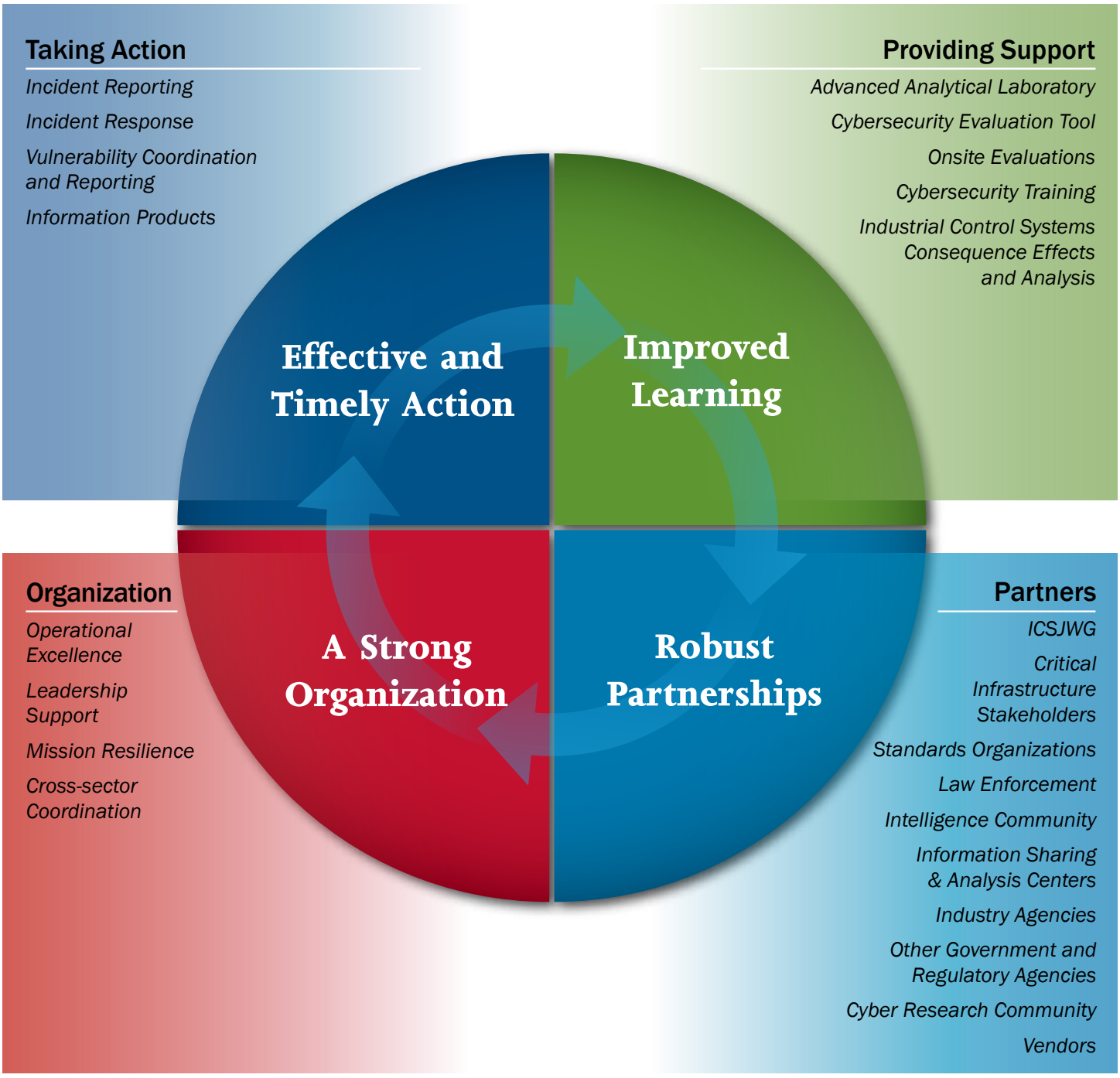
- Developed incident handling and response guidance/ training for asset owners, including tools to assist in forensic data gathering and analysis;
- Improved watch floor operational capabilities, data fusion, and data analysis capabilities to correlate events and disseminate data;
- Developed a hands-on Control Systems Forensics for Law Enforcement course to train personnel in gathering, handling, and preserving forensic data;
- Published relevant information products and cybersecurity guidance for protecting against emerging threats, mitigating common vulnerabilities, and implementing best recommended practices;
- Improved relationships with the critical infrastructure and key resources (CIKR) community to share critical information and raise awareness by leveraging knowledge of new vulnerabilities to reduce risk across all sectors; and
- Updated policy related to researcher attribution in alerts and advisories to support coordinated disclosures.

Cybersecurity is a journey, not a destination. ICS-CERT will continue to enhance our ability to identify weaknesses and emerging vulnerabilities, take the necessary steps to implement change, and maintain adequate security measures to defend against the continuously evolving threats.

As we move into 2013, we are anxious to hear from you. Establishing a strong posture of continuous information exchange is essential to reducing cybersecurity incidents and improving the overall security posture of our Nation's critical infrastructure.

Regards,

Marty Edwards
Director
Industrial Control Systems Cyber Emergency Response Team
Department of Homeland Security
ICSJWG GCC Chair


Taking Action
Incident Reporting
Incident Response
Vulnerability Coordination and Reporting
Information Products
Providing Support
Advanced Analytical Laboratory
Cybersecurity Evaluation Tool
Onsite Evaluations
Cybersecurity Training
Industrial Control Systems Consequence Effects and Analysis
Effective and Timely Action
Improved Learning
A Strong Organization
Robust Partnerships
Organization
Operational Excellence
Leadership Support
Mission Resilience
Cross-sector Coordination
Partners
ICSJWG
Critical Infrastructure Stakeholders
Standards Organizations
Law Enforcement
Intelligence Community
Information Sharing & Analysis Centers
Industry Agencies
Other Government and Regulatory Agencies
Cyber Research Community
Vendors

Organization

Recognizing the importance of control systems to our critical infrastructure, the Department of Homeland Security (DHS) supported the Control System Security Program's (CSSP) mission to reduce risk to the Nation's critical infrastructure by strengthening control systems cybersecurity through public-private partnerships.

The ICS-CERT is aligning to facilitate the expansion of those essential capabilities in support of Cybersecurity & Communications (CS&C). CS&C will provide guidance to promote operational efficiencies and transition of responsibilities and mission objectives to ICS-CERT. ICS-CERT will continue to provide the same essential products, services, and support to critical infrastructure asset owners and operators, vendors, government agencies, and others.

In 2012, ICS-CERT served as a primary component of the National Cybersecurity and Communication Integration Center (NCCIC) and contributed to the NCCIC's growing mission and capabilities.

ICS-CERT continues to accomplish its mission to reduce cybersecurity risks to the Nation's critical infrastructure by establishing and operating under its four core functional areas:

1. Providing situational awareness through alerts and advisories to warn of cyber-based threats and vulnerabilities affecting critical infrastructure assets;
2. Conducting technical analysis of malware, digital media, system vulnerabilities, and emerging exploits;
3. Performing incident response to support asset owners with discovery, analysis, and recovery efforts; and
4. Coordinating and monitoring control system vulnerabilities in collaboration with the cyber research and vendor communities.

These four core functions are supported by a foundation of partnering with the control system stakeholder community to facilitate cyber risk mitigation activities.

Outreach

The ICS-CERT is organized to support the Strategy for Securing Control Systems, which outlines a longterm, common vision where effective risk management of control systems security can be realized through successful coordination efforts. ICS-CERT recognizes that outreach plays an important role in those coordination efforts.

In 2012, ICS-CERT provided nearly 60 briefings to 500 industry partners across the 18 critical infrastructure sectors, including multiple classified threat briefings to industry organizations that have developed programs for security-cleared personnel. The following is a sampling of the sector briefings:

- Electrical Sector Information Sharing and Acquisition Centers (ISAC),
- Combined Chemical and Oil and Natural Gas ISACs,
- Water ISAC,
- Cyber Threat Intelligence Coordination Working Group (CTICG),
- Transportation Security Sector Cyber Working Group (TSSCWG), and
- Nuclear Sector Specific Agency (NSSA).

In addition, ICS-CERT attended over 200 events to promote awareness among critical infrastructure owners, operators, and vendors. This level of engagement supports the continuous development of resources to help industry understand and prepare for ongoing and emerging control systems cybersecurity issues, vulnerabilities, and mitigation strategies.

Industrial Control Systems Joint Working Group

ICS-CERT's outreach strategy has leveraged the Industrial Control Systems Joint Working Group (ICSJWG) to engage a broad range of partners, including critical infrastructure sector specific agencies; other federal, state, local, and tribal government agencies; national, trans and subnational groups and councils; fusion centers; vendors; researchers and academia; infrastructure owners and operators; and international partners, including various CERTs.

In 2012, ICSJWG had one of the most successful years to date with membership expanding to more than 1,400 industrial control systems (ICS) professionals. The increased coordination between various ICS professionals and cybersecurity organizations was mirrored at the Spring and Fall 2012 ICSJWG meetings.

Highlights include the following.

- The ICS-CERT participated in panels fostering open dialog about control systems vulnerabilities and how the community can work together to mitigate these issues.
- The subgroup meetings allowed participants to discuss in depth the current status of subgroup activities and report accomplishments to the community.
- The Introduction to Control Systems Cybersecurity training course was taught to more than 115 meeting attendees at the Spring meeting and the Intermediate Cybersecurity Industrial Control Systems Training was taught to over 65 participants at the Fall meeting.
- ICS-CERT hosted its first International Day featuring information sharing sessions, goal discussions, and conversations about a possible path forward for creating a new ICSJWG international subgroup.
- Marty Edwards provided an ICS threat brief and overview to meeting attendees at the Fall meeting.
- International attendees were invited to attend the world renowned "hands-on" Industrial Control Systems Cybersecurity Advanced Training held at the ICS-CERT training facility in Idaho Falls, Idaho.

Moving forward, we will continue to promote growth and collaboration in the ICSJWG community through public-private partnership.

Advanced Analytical Laboratory

ICS-CERT provides expertise for response and analysis of cyber incidents affecting the ICS community through the Advanced Analytical Laboratory (AAL). One such example in 2012 was the spear-phishing campaign against the oil and natural gas sector. AAL worked directly with a dozen energy and manufacturing companies affected by the campaign, providing digital media and log file analyses to identify compromised hosts. During the course of this response effort, AAL analyzed over 50 malware samples and malicious files, 20 emails, and 38 hard drive images to determine the extent of the compromise and identify the techniques and tactics used by the threat actors. By analyzing malicious emails and malware samples, AAL was able to provide indicators of compromise through alerts and advisories to the ICS community to aid in detection efforts. AAL provided onsite support to two affected companies, helping determine the extent of the compromise and providing mitigation recommendations.

The chemical sector was also the victim of targeted spear-phishing attacks in 2012. AAL worked directly with companies affected by this campaign, providing onsite support, analyzing drive images and malware samples and disseminating indicators back to the community. AAL provided onsite support to one of the affected companies.

AAL also provides vulnerability verification and patch validation for ICS products. AAL's verification and validation reports assist ICS-CERT Vulnerability Handlers with developing product advisories for the ICS community.

In 2012, AAL enhanced its analysis capabilities with a core information storage system. This system maintains forensic information for all analysis activities and is integrated with the AAL automated analysis environment. AAL also developed a tool to scan whole drives for malware using multiple antivirus engines. This tool greatly reduced the time needed to scan multiple drive images with commercial antivirus products.

ICS-CERT will continue to support AAL's development of tools and techniques available to ICS community members affected by cyber incidents.

Cybersecurity Training

ICS-CERT offers cybersecurity training at no cost to ICS professionals and managers across all sectors of CIKR in order to support risk reduction efforts. These training courses include Introduction to Control Systems Cybersecurity, Intermediate Cybersecurity for Industrial Control Systems, ICS Advanced Cybersecurity, and ICS Security for Management. In 2012, over 2,200 ICS professionals were trained.

2012 Training Highlights included the following.

- Provided 12 Advanced Training sessions, which are week-long events that provide intensive hands-on training and a 12-hour, red team/blue team exercise that simulates a corporate espionage scenario.
- Developed a Control Systems Forensics for Law Enforcement course. This course helps law enforcement agents to understand the differences in performing forensics on ICSs versus normal corporate enterprise network forensics.
- Delivered 52 training sessions across the country, including Introduction to Control Systems Cybersecurity (101), Intermediate Cybersecurity for Industrial Control Systems lecture (201), and Intermediate Cybersecurity for Industrial Control Systems with lab (202).
- Provided demonstrations of how an ICS attack could progress for high ranking government officials and congressional staffers.
- Conducted our first regional training event in Atlanta, Georgia. This event was so successful that ICS-CERT will now conduct regional training on a regular basis.

Cybersecurity Evaluations

ICS-CERT provides cybersecurity evaluations to support the reliability and resiliency of the systems that comprise and interconnect critical infrastructures. ICS-CERT develops and implements coordinated security measures in collaboration with partners from across public, private, and international communities.

In 2012, ICS-CERT conducted 89 onsite assessments across all CIKR. The objective of the assessment is to establish a "baseline of performance" with regard to cybersecurity maturity as defined within a suite of cybersecurity standards and guidelines. Although the results may differ from sector to sector, many of the vulnerabilities and weaknesses within the networks are similar. This year has seen considerable partnering with the Nuclear Industry, Oil and Gas Industry, and Department of Defense with regard to performing onsite cybersecurity assessments.

Cybersecurity assessments are now tailored to each individual assessment depending on the level of complexity in the system(s). Asset owners can now request Cybersecurity Evaluation Tool (CSET®) evaluations and/or Architecture Reviews, which is a more in-depth comprehensive evaluation of specific control systems networks, architectures, and components.

Cybersecurity Evaluation Tool

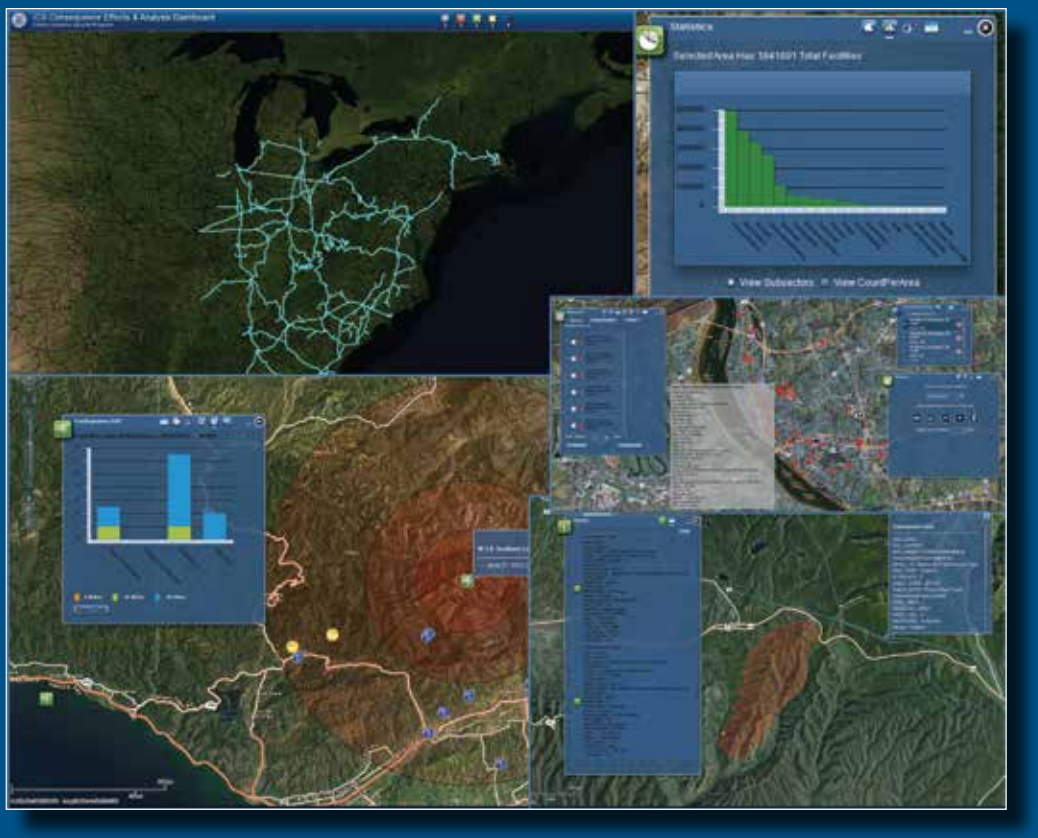
The ICS-CERT foundation tool for onsite assessments is our CSET®. In 2012, over 5,500 CSETs® were distributed and downloaded. Version 4.1 was released in January 2012 and incorporated integration with Microsoft Visio. This functionality allows users to develop a diagram in Visio and then map and export it to CSET® where component questions are generated. It also allows for a diagram created in CSET® to be imported into Visio with all the CSET® metadata preserved. A new stencil of CSET® components for Visio was also included as part of the installation package.

ICS-CERT released CSET® 5.0, in January 2013, this version represents the most significant upgrade in the underlying technical architecture of the tool. This upgrade involves conversion to the Microsoft.NET framework environment as well as utilization of component pieces from Syncfusion. In addition, Section 508 of the Americans with Disabilities Act (ADA) was incorporated into the new version to allow those with disabilities a way to interact with and use the CSET®.

Standards Support

A broad range of standards exists to support the CSET® tool across CIKR. ICS-CERT executes a comprehensive approach to standards by providing assistance to standards bodies, promoting awareness of accepted standards and providing tools, like CSET® to asset owners, to evaluate compliance. The ICS-CERT continues to engage with cross-sector industry partners to develop new cybersecurity standards and enhancement of existing standards. The ICS-CERT provides key support to:

- the ISA-99 Working Groups,
- International Standard Organization (ISO)/ International Electrotechnical Committee (IEC),
- the National Institute of Standards (NIST),
- Technology Smart Grid Interoperability Panel (SGIP),
- American Public Transportation Association (APTA), and
- ICSJWG Roadmap Subgroup.



Industrial Control Systems Consequence Effects and Analysis

ICS-CERT supports the development of leading edge tools to foster an environment of collaboration and provide unique forensic capabilities to address cybersecurity challenges specific to ICS.

The Industrial Control Systems Consequence Effects and Analysis (ICS-CEA) framework is a collaboration tool. ICS-CEA provides a critical infrastructure modeling and simulation capability. The tool also provides a means for users to model, analyze, and share information related to potential consequences of naturally occurring or man-made threats on our Nation's critical infrastructure. The ICS-CEA system provides the NCCIC a capability for daily use of modeling, simulation, analysis, and information sharing related to potential cross-sector "consequence" effects to ICS and their related CIKR sectors.

In 2012, ICS-CEA has been used for responding to multiple requests by the NCCIC regarding the identification of potentially affected CIKR because of natural and potential man-made threats. These events have included analysis support for the Super Bowl, national level exercises, and others related on our Nation's energy, water, and transportation infrastructure.

ICS-CERT's suite of tools provides analysis to improve security posture as well as identify the appropriate cybersecurity mitigation measures. ICS-CERT continues to cultivate capabilities in collaboration and forensics to span the gap between ICS, information technology, and the user interface to provide advanced industrial analysis to enhance cybersecurity.

Taking Action

ICS-CERT works with critical infrastructure asset owners and operators to respond to cyber incidents that have the potential to impact ICS. ICS-CERT works with the affected organizations to offer subject matter expertise for immediate actions to mitigate the compromise and develop strategies for recovery and future defenses. The mitigation strategies are specific to the incident and individual needs of the organizations.

ICS-CERT is a component of the NCCIC, bringing ICS security technical and response capabilities to the partnership. The work is performed in conjunction with the NCCIC and furthers its overall mission to coordinate defense against and response to cyber attacks across the Nation.

In 2012, ICS-CERT responded to a steady stream of cyber incidents, coordinated researcher-discovered ICS vulnerabilities with vendors, and produced alerts and advisories to notify the ICS community. These situational awareness products provide actionable information about mitigation and protection strategies for implementing sound security practices.

This year, ICS-CERT received and responded to 138 incidents as reported by asset owners and industry partners. In 2012, attacks against the energy sector represented over 40 percent of all incidents reported to ICS-CERT. In roughly half of these incidents, information pertaining to the ICS/SCADA environment, including data that could facilitate remote unauthorized operations, was targeted in these incidents. ICS-CERT also deployed on site incident response teams to assist various critical infrastructure operators with efforts to mitigate cyber intrusions. The on site teams were able to help identify the extent of the intrusion and develop strategies for recovery and improving the operator's defensive posture and future detection capabilities. The AAL played a key role in the response; providing support for analysis of hard drives, log files, and malware artifacts. The AAL also developed the guidelines found in the paper on Cyber Intrusion Mitigation Strategies.[a]

Vulnerability analysis and coordination activities continued to increase with more researchers using ICS-CERT as a conduit for coordination with ICS vendors. The ICS-CERT AAL also provided analytic support to vendors to perform proof-of-concept testing and patch validation. Many of those vulnerabilities resulted in ICS-CERT alerts and advisories on the US-CERT secure portal and on the public Web site.

In 2012, ICS-CERT published 342 information products warning the ICS community about various vulnerabilities and threats that could potentially impact control systems. ICS-CERT also published the Incident Summary Report[b] to summarize cyber incidents, onsite deployments, and associated findings from 2009 through 2011.

a. http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01.pdf
b. http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

ICS-CERT by the Numbers "Calendar Years"

Table 1 compares the overall incident, vulnerability, onsite event, and information product statistics for calendar years 2010, 2011, and 2012, indicating control system cyber events and activity.

*Table 1. ICS-CERT activity trend by *Calendar Year*

ICS-CERT Metrics	2010 Totals	2011 Totals	2012 Totals
ICS Incident Reported — tickets	39	204	138
ICS Incident Response Onsite Deployments	8	7	6
ICS Related Vulnerability Report — tickets	41	141	147
ICS-CERT Information Products	138	283	343
Distributed or Downloaded CSET®	2,394	7,448	5,584
Onsite Assessments	57	70	89
Professionals Trained	2,499	1,658	2,241
Number of Training Sessions	55	47	52
ICSJWG Membership	N/A	1,040	1,416
Speaking Engagements	47	164	200
Conference Exhibitions	11	20	19

*Calendar Year accounts for the time period between Jan 1 of a given year and Dec. 31 of the same year.

ICS-CERT by the Numbers "Fiscal Years"

Table 2 compares the overall incident, vulnerability, onsite event, and information product statistics for fiscal years 2010, 2011, and 2012, indicating control system cyber events and activity.

*Table 2. ICS-CERT activity trend by *Fiscal Year*

ICS-CERT FY Metrics	2010 Totals	2011 Totals	2012 Totals
ICS Incident Reported — tickets	39	140	197
ICS Incident Response Onsite Deployments	6	7	6
ICS Related Vulnerability Report — tickets	18	139	137
ICS-CERT Information Products	110	243	347
Distributed or Downloaded CSET®	2,400	5,100	6,631
Onsite Assessments	57	81	89
Professionals Trained	2,463	1,686	2,327
Number of Training Sessions	54	47	56
ICSJWG Membership	600	1,012	1,423
Speaking Engagements	26	137	205
Conference Exhibitions	11	20	22

*Fiscal Year 2010 represents the time period of October 1, 2009–September 30, 2010, 2011 represents the time period of October 1, 2010–September 30, 2011, and 2012 represents the time period of October 1, 2011–September 30, 2012.

Sector Support by the Numbers "Fiscal Years"

Table 3 compares number of onsite assessments provided to the control systems community in each of the 18 critical infrastructure sectors in fiscal years 2010, 2011, and 2012.

The last row on the table compares the number of sector requesting support in each fiscal year with the total number of critical infrastructure sectors.

Table 3. Fiscal Year onsite assessments by Sector

Sector	FY-10	FY-11	FY-12	Cumulative Assessments
Agriculture & Food	0	5	0	5
Banking & Finance	2	1	6	9
Chemical	0	0	4	4
Commercial Facilities	3	10	2	15
Dams	1	0	0	1
Defense Industrial Base	1	0	12	13
Emergency Services	0	2	3	5
Energy	13	11	7	31
Government Facilities	6	5	3	14
Information Technology	0	3	5	8
National Monuments & Icons	0	5	1	6
Nuclear Reactors, Materials, & Waste	0	2	8	10
Postal & Shipping	0	0	1	1
Public Health & Healthcare	5	6	1	12
Telecommunication	0	1	0	1
Transportation	5	7	10	22
Water	19	21	25	65
Critical Manufacturing	2	2	1	5
Totals	57	81	89	227
Number of Sectors Assessed	11/18	14/18	15/18	N/A

*Fiscal Year 2010 represents the time period of October 1, 2009–September 30, 2010, 2011 represents the time period of October 1, 2010–September 30, 2011, and 2012 represents the time period of October 1, 2011–September 30, 2012.

Future

ICS-CERT will continue to actively engage the public and private sectors as well as international partners to prepare for, prevent, and respond to cybersecurity incidents that could impair strategic assets. The ICS-CERT provides resources to enhance the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

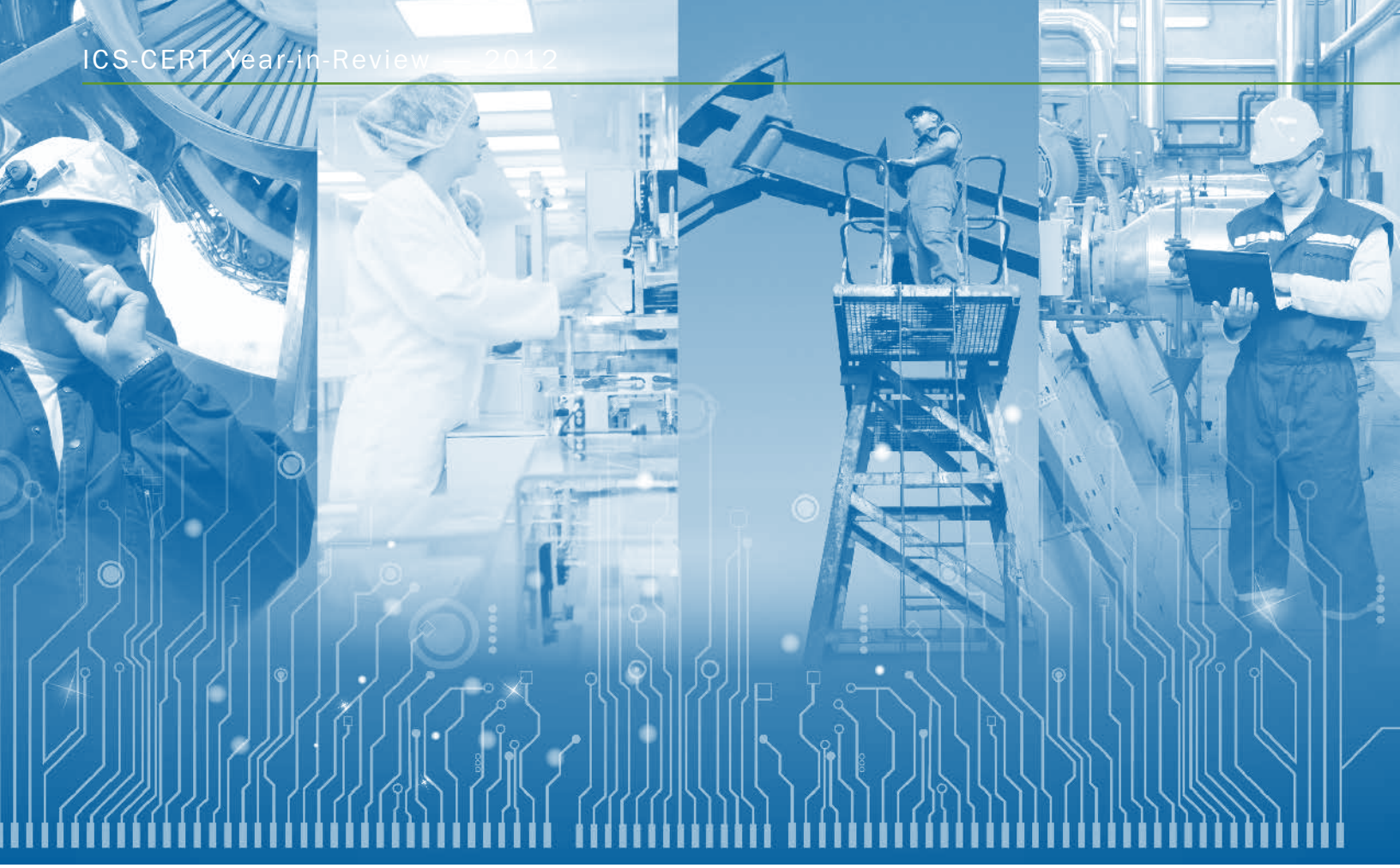
In order to provide integrated capabilities ICS-CERT enhances response capabilities based on the specific needs and requirements of the requesting customer. This tailored approach provides scalable response to cybersecurity challenges across critical infrastructures. ICS-CERT works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, economy, government services, and the overall security of the United States. This is accomplished through a series of continuous efforts designed to further safeguard systems by reducing potential vulnerabilities, protecting against cybersecurity and communications intrusions or disruptions, and anticipating future threats.

Under ICS-CERT, AAL's future development plans include automated tools for registry analysis, timelining, and pdf analysis.

The ICS-CERT will continue to pursue five strategic goals.

- Goal 1: Foster public-private partnerships to plan, coordinate, and support ICS cybersecurity initiatives.
- Goal 2: Serve as a global clearinghouse for information associated with the security of ICS.
- Goal 3: Support robust preparedness planning and facilitate effective incident response capabilities.
- Goal 4: Support increased awareness of control systems security issues and improved technical expertise for stakeholders.
- Goal 5: Ensure that ICS-CERT is an adaptive and prepared organization that effectively plans for, anticipates, and manages future risks and disruptions.

In 2012, ICS-CERT served as a primary component of the NCCIC and contributed to the NCCIC's growing mission and capabilities.



Assistance from ICS-CERT is only a phone call away

The 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 the ICS-CERT:

ics-cert@dhs.gov
(877) 776-7585

www.us-cert.gov/control_systems/ics-cert

For more information on the ICS-CERT Program visit:

http://www.us-cert.gov/control_systems/

Homeland Security

13-50012