ICS-CERT Year in Review

Industrial Control Systems Cyber Emergency Response Team

2013

Homeland Security

National Cybersecurity and Communications Integration Center

What's Inside

The metrics information or numbers included in the text are Fiscal Year (FY) numbers. Calendar Year (CY) metrics are only available in the chart on page 16.

Homeland Security

Welcome NCCIC

National security has become interconnected with our Nation's cybersecurity. The National Cybersecurity and Communications Integration Center (NCCIC) provides critical national capabilities. The NCCIC's primary focus areas include conducting daily analysis and situational awareness, incident management, and information sharing in the cybersecurity and communications domains.

The NCCIC organization supports a holistic approach at home and abroad to prevention, protection, mitigation, response, and recovery efforts. The NCCIC is a 24/7 Communications Operations and Integration Center.

NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities.

In 2013, the NCCIC as a whole received over 220,000 reports of cybersecurity and communications incidents. These reports originated from both public and private partners sharing what they discovered on their information technology systems. The outreach facilitated gaining insights on the latest prevention and mitigation measures from the broader national cybersecurity community. In the coming years, an even greater number of cyber incidents are likely with a renewed need to solve cybersecurity and communications-related challenges as expeditiously as possible.

I am proud of the hard work and dedication illustrated by the NCCIC team.

Sincerely,

Larry Zelvin, Director
National Cybersecurity and Communications
Integration Center (NCCIC)

Department of Homeland Security

Welcome ICS-CERT

This year, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) briefed asset owners and developed tools and capabilities to enhance cybersecurity incident handling and response efforts.

ICS-CERT correlated emerging cyber incidents with previous events and tracked known threat actors based on their techniques and tactics. The information these tools and capabilities yielded was leveraged to provide situational awareness information to federal law enforcement agencies and the greater industrial control system community.

ICS-CERT initiatives accomplished in 2013 included:

- Providing briefings, including classified briefings, on industrial control systems threats and defense-in-depth to critical infrastructure owners, operators, and vendors as well as other industry and government partners.
- Hosting meetings and presenting event information and mitigations across all 16 critical infrastructure sectors.
- Triaging over 250 cybersecurity incidents by providing analytic support and guidance to asset owners.
- Delivering expert guidance and consultation to asset owners and operators on the self-assessment Cyber Security Evaluation Tool (CSET®) or Architecture Reviews.
- Engaging in one Industrial Control System Joint Working Group meeting bringing together the industrial control system community to share its best cybersecurity practices, create new relationships, and leverage knowledge from ICS-CERT.

Best regards,

Marty Edwards, Director
Industrial Control Systems Cyber
Emergency Response Team

Department of Homeland Security
ICSJWG GCC Chair

National Preparedness

The economic welfare and safety of the American people relies on the resilience and reliability of the Nation's critical infrastructure. The National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team (NCCIC/ICS-CERT) provides a variety of operational capabilities to ensure that critical infrastructure across the nation continues to operate as designed and is well secured. These efforts require continual vigilance and innovative responses to address emerging challenges at a global level. ICS-CERT brings together a community of critical infrastructure stakeholders who work together to improve our national cybersecurity posture and address future needs.

The Department of Homeland Security (DHS) applies guidance from Presidential Policy Directive 8: National Preparedness to enable operational programs like ICS-CERT to align key roles and responsibilities in its national cybersecurity response and mitigation efforts.

The critical principles establish a fundamental doctrine for ICS-CERT response capabilities that include: engaged partnership; tiered response; scalable, flexible, and adaptable operational capabilities; unity of effort through unified command; and readiness to act.

ICS-CERT employs an adaptable and repeatable process to ensure that ICS-CERT vendors, operators, and owners across the country can organize response efforts to address a variety of cybersecurity risks based on their unique needs and capabilities. This framework is not based on a one-size-fits-all organizational construct. Instead, it acknowledges the concept of tiered response, which emphasizes that response to cybersecurity incidents, and should be handled at the right level to support the critical infrastructure sector owner, operator, or vendor.

ICS-CERT operations in this brochure are described by the attributes that support its scalable, flexible, and adaptable coordinating structures. The program has roles and responsibilities which include integrating capabilities across the whole community, local, state, tribal, territorial, and federal governments in support of response to actual and potential cybersecurity incidents.

National Preparedness

I. Prevention – Engaged Partnership

WHAT The capabilities necessary to avoid, prevent, or stop a threatened or actual act or terrorism

HOW
- Industrial Control Systems Joint Working Group
- Outreach

II. Protection – Tiered Protection

WHAT The capabilities necessary to secure critical infrastructure in the homeland against acts of terrorism and manmade or natural disasters

HOW
- Training
- Cyber Security Evaluation Tool (CSET®)

III. Mitigation – Scalable, Flexible and Adaptable Capabilities

WHAT The capabilities necessary to reduce loss of life and property by lessoning the impact of the cyber attack

HOW
- Incident Response, Vulnerability Handling
- Advanced Analytical Laboratory

IV. Response – Unity of Effort Through Unified Command

WHAT The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after a cyber incident has occurred

HOW
- US Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- National Coordinating Center for Telecommunications (NCC)
- National Cybersecurity and Communications Integration Center (NCCIC) Operations
- Industrial Control System Consequence and Effects Analysis (ICS-CEA)

V. Recovery – Applies Advanced Capabilities to Support Recovery

WHAT The capabilities necessary to assist communities affected by an incident to recovery effectively

HOW
- Cybersecurity Assessments
- Evaluations and Architecture Reviews

Prevention

Outreach Across Critical Infrastructure Sectors

ICS-CERT supports prevention through the deployment of operational capabilities to avoid, or stop a cybersecurity threat. Prevention in this context relies on an engaged partnership with the industrial control system community of owners, operators, and vendors.

DHS ICS-CERT, in coordination with the Federal Bureau of Investigation (FBI), Department of Energy, the Electricity Sector Information Sharing and Analysis Center, Transportation Security Administration (TSA), and the Oil and Natural Gas and Pipelines Sector Coordinating Councils' Cybersecurity Working Group, conducted a series of Action Campaign Briefings throughout Fiscal Year 2013 in response to the growing number of cyber incidents related to U.S. critical infrastructure. The 14 briefings were given to over 750 attendees in various cities throughout the country to assist asset owners and operators in detecting intrusions and developing mitigation strategies. Briefings were held at both the classified and unclassified levels, and covered a wide range of topics. This included the latest threats against industrial control systems, adversary tactics, lessons learned from current activities, best practices for detecting and preventing intrusion, and methods for securing networks.

Important sector-specific briefings:

- The American Fuel & Petrochemical Manufacturers (AFPM) Quality and Assurance and Technology Forum/ AFPM Plant Automation and Decision Support Conference,
- Nuclear Sector Joint Cyber Subcouncil - Sponsored by Nuclear Energy Institute,
- 7th Annual American Petroleum Institute Cybersecurity Conference for the Oil & Natural Gas Industry,
- Chemical Classified Briefing for Chief Information Officers,
- Nuclear Fuel Cycle Facility Conference,
- 2013 Chemical Sector Security Summit, and
- Cybersecurity for Oil and Natural Gas Forum.

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, mitigation, and recovery strategies.

Prevention

Engaged Partnership with the ICSJWG

Partnership relies on engagement of the entire control systems community by developing shared goals and aligning capabilities to reduce the risks associated with successful cyber attacks. Building a cohesive industrial control system community includes supporting ongoing, clear, consistent, and effective communications and shared situational awareness about cybersecurity incidents, mitigations, and recovery. ICS-CERT recognizes that outreach plays a critical role in those coordination efforts.

ICS-CERT's outreach strategy continues to leverage the Industrial Control Systems Joint Working Group, engaging an increasingly broad range of partners, including critical infrastructure sector-specific agencies; other federal, state, local, and tribal government agencies; national groups and councils; fusion centers; vendors; researchers and academia; infrastructure owners and operators; and international partners, including various CERTs.

The Industrial Control Systems Joint Working Group 2013 Fall Meeting took place in Rockville, Maryland, at the Institute for Bioscience and Biotechnology Research/National Institute of Standards and Technology (NIST) facility on the grounds of the University of Maryland, Shady Grove campus. The conference provided for two days of presentations consisting of topics of interest to the Industrial Control Systems Joint Working Group community.

Highlights included:

- Presentations on a variety of topics such as Information Technology Integration, Cyber Intelligence Analysis, NIST ICS Standards, Fuzzing, and Industrial Control Systems Security in the Healthcare sector.
- Discussions on the path forward for the Industrial Control Systems Joint Working Group, including a detailed explanation of new working activities and the associated activity plan, as well as an overview of the outstanding products developed by previous subgroup structures.
- An unclassified threat briefing from NCCIC/ICS-CERT detailing the current threat landscape to the nation's critical infrastructure.
- Two Lunch & Learn sessions educating the audience on new technology to replace firewalls and the way ahead for the Department of Defense as it relates to industrial control systems cybersecurity.

Protection

Tiered Protection Through Cybersecurity Training

ICS-CERT aligns training to further develop the skills necessary to secure and protect critical infrastructure from cyber threats. ICS-CERT offers cybersecurity training at no cost to industrial control system professionals and managers across all 16 critical infrastructure sectors in order to transfer knowledge on securing and protecting infrastructure to reduce cyber risk. These training courses include Introduction to Control Systems Cybersecurity, Intermediate Cybersecurity for Industrial Control Systems, and Industrial Control Systems Advanced Cybersecurity. In 2013, nearly 700 infrastructure professionals and law enforcement agents were trained. ICS-CERT training programs offer a foundation for cybersecurity professionals to attain the necessary skills to approach cybersecurity challenges.

2013 Training Highlights included the following:

- Provided 11 Advanced Training Sessions to 442 participants, 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.
- Trained law enforcement professional in Control Systems Forensics for Law Enforcement course. This course educates law enforcement agents on performing forensics on industrial control systems versus normal corporate enterprise network forensics.
- Delivered five 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).
- Conducted our first regional trainings.
- Supported international training courses that reached 65 students from around the world.

Protection

Tiered Support with the CSET

The ICS-CERT foundation tool to baseline cybersecurity relative to cybersecurity standards is our Cyber Security Evaluation Tool (CSET). In 2013, over 5,000 CSETs were distributed and downloaded. As a significant piece of the ICS-CERT proactive portfolio, CSET continues to support, educate, and guide critical infrastructure asset owners. By combining the use of recognized standards and a step-by-step wizard style, CSET has become an accepted practice for critical infrastructure asset owners in establishing their own cybersecurity baselines and processes.

CSET educates asset owners through an assessment process. During this process, cybersecurity implementers and management personnel are taken step by step through a series of concepts and ideas. While considering each concept, the assessment team reviews its individual processes from a cybersecurity perspective. The team discovers its own unique vulnerabilities while being introduced to new concepts and principles of cybersecurity.

To accommodate more mature cybersecurity processes, CSET now provides the capability for current CSET users to use their past and current assessments to evaluate their investment in an established cybersecurity process. The release of CSET 6.0, helps users to establish a baseline assessment and then incorporate following assessments to trend and compare overall improvement. Users will be able to drill down into specific areas to view trending in areas such as account management, password-management, defense-in-depth, or least user privileges. Users can use this information to justify spending on particular areas of vulnerability, prioritize work and investment, and determine return on investment for cybersecurity-related spending.

New functionality CSET 6.0 includes:

- Video tutorials available on demand from YouTube.
- Component questions reflect the latest concerns and issues in control system-related cybersecurity.
- High-level concept questions help the user to better understand and navigate questions.
- Ability to assign different portions and sections of an assessment and then merge all the pieces back together to create a single assessment.
- Capability to combine assessments to compare cybersecurity between divisions, find common problems, or illustrate the distinctive needs for each department.

Mitigation

Incident Response relies on a Scalable, Flexible, and Adaptable Operational Capabilities

ICS-CERT operations rely on an adaptable and repeatable approach to mitigate cyber attacks. The repeatable process delivers core cybersecurity capabilities to industrial control system owners, operators, and vendors. The number, type, and mitigation resources ICS-CERT is able to provide are directly proportional to the requirement of the cybersecurity incident. As needs of an incident escalate and change, the program remains scalable, flexible, and adaptable in their incident response.

ICS-CERT's suite of mobilized capabilities is associated with those actions that may protect property and the environment, stabilize communities and support basic human needs after a significant cybersecurity incident.

ICS-CERT works with critical infrastructure asset owners and operators to respond to cyber incidents that have the potential to impact any of the 16 critical infrastructure sectors. ICS-CERT works with the potentially affected organizations to offer mitigations and subject matter expertise for immediate actions. The mitigations are specific to the cyber threat and needs of the organizations.

In 2013, ICS-CERT applied capabilities to a number of cyber incidents, coordinated researcher discovered industrial control system 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 257 incidents as voluntarily reported by asset owners and industry partners. In 2013, attacks against the Energy sector represented over 56 percent of all incidents reported to ICS-CERT. 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:

- Unauthorized access and exploitation of Internet-facing ICS/SCADA devices
- Malware infections within air-gapped control system networks (impacting operations)
- SQL Injection and application vulnerability exploitation

- Lateral movement between network zones
- Targeted spear phishing campaigns
- Watering hole attacks (one of which utilized a zero-day vulnerability)

Mitigation

Preparation Focuses Scalable, Flexible, and Adaptable Approach to Incident and Vulnerability Analysis

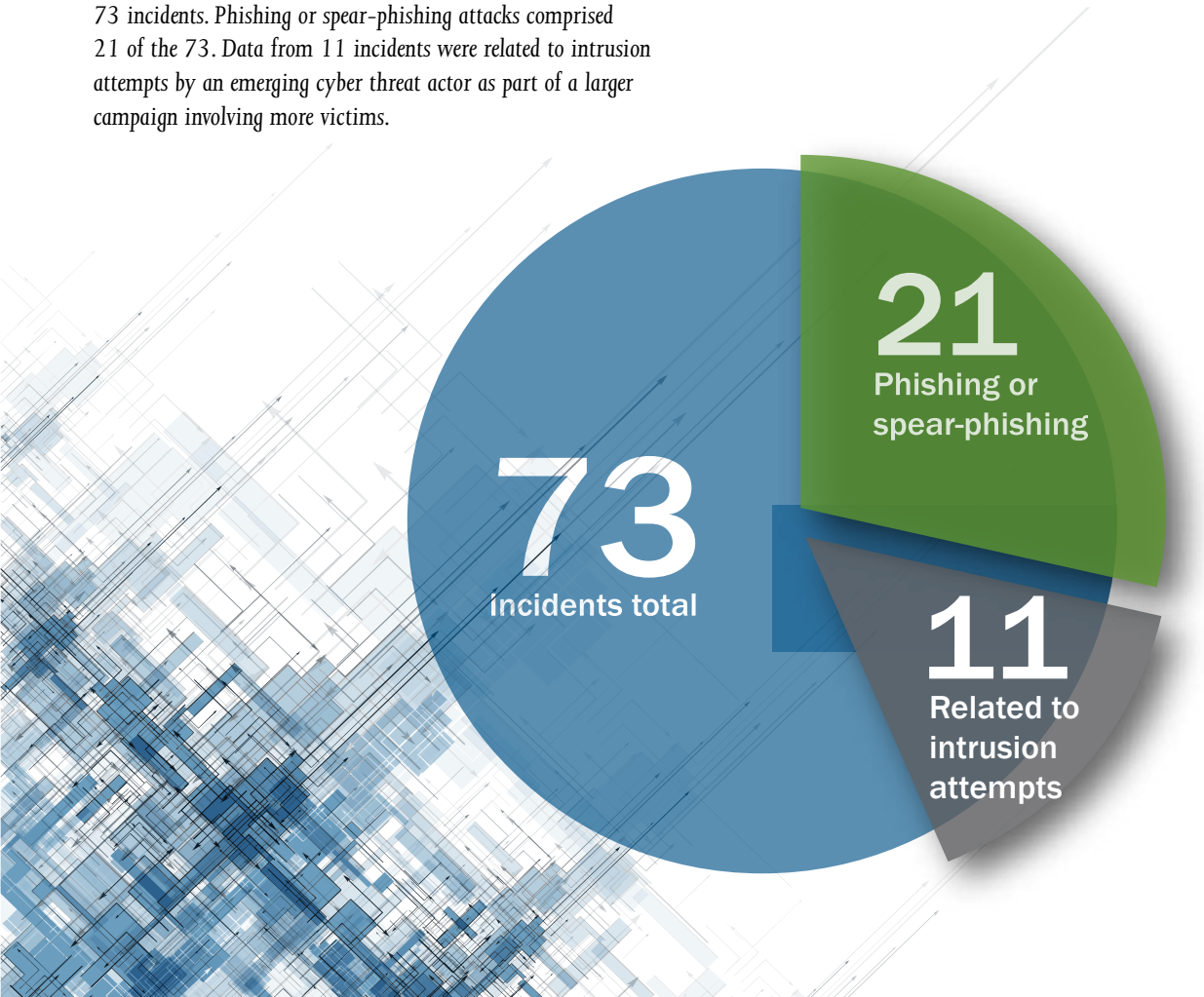
ICS-CERT employs analysis to improve the security posture and identify cybersecurity mitigation measures for industrial control systems. Vulnerability coordination, incident response, and mitigation services provided by ICS-CERT rely on advanced analysis provided through our Advanced Analytical Laboratory. The program cultivates skills, tools, and personnel to meet the demands of traditional industrial control systems security and today's threat landscape and evolving exploitation techniques.

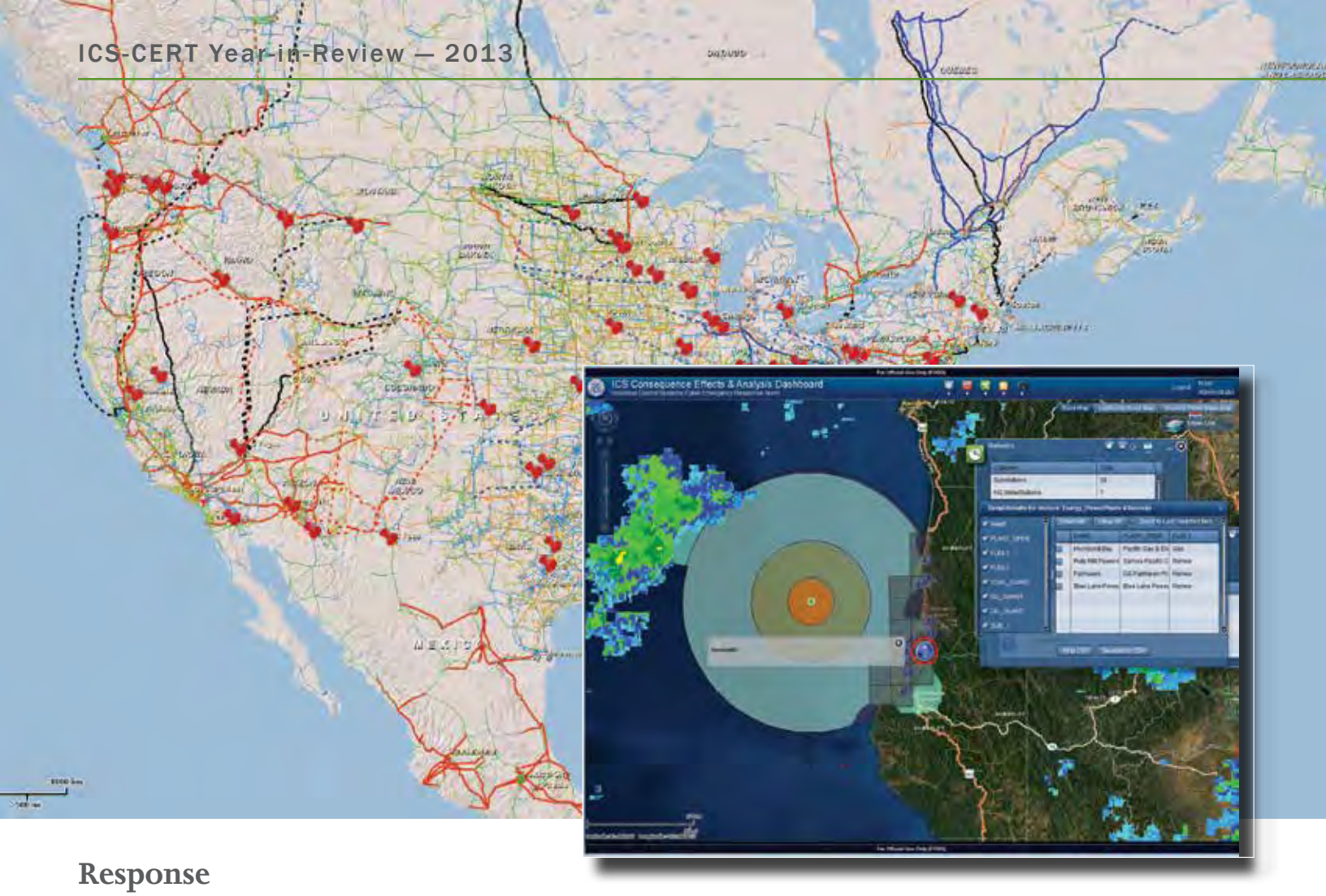
The Advanced Analytical Laboratory conducted vulnerability analysis and provided feedback and guidance to the ICS-CERT Vulnerability Team. The ICS-CERT prepared alerts and advisories using the vulnerability information and working closely with the industrial control system vendor. These alerts and advisories are posted to the US-CERT secure portal and on the public Web site. In total, the ICS-CERT Vulnerability Team received 187 reports from researchers and vendors that required coordination, testing, analysis, and the publication of information products.

This year, the Advanced Analytical Laboratory focused on improving ICS-CERT's incident response capabilities and tools to include rapid, enterprise scanning of systems to look for known indicators of compromise for sophisticated intrusions. At the request of asset owners, these new capabilities as well as traditional incident response techniques were deployed for seven onsite incident response activations.

The Advanced Analytical Laboratory also made significant improvements in its ability to handle and process digital media. Advanced Analytical Laboratory developed additional automation tools and techniques that have shortened the turn-around time and increased the thoroughness of the analysis.

In FY-13, ICS-CERT's Advanced Analytical Laboratory analyzed data from 73 incidents. Phishing or spear-phishing attacks comprised 21 of the 73. Data from 11 incidents were related to intrusion attempts by an emerging cyber threat actor as part of a larger campaign involving more victims.





Response

NCCIC Provides Unified Response

DHS provides analysis and support through the Office of Cybersecurity & Communications, within the National Protection and Programs Directorate, to an advanced network of cybersecurity professionals who work to protect critical infrastructure from cybersecurity threats.

The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity for critical infrastructure are coordinated and integrated with ICS-CERT.

The NCCIC is composed of four branches:

United States Computer Emergency Readiness Team (US-CERT) employs analysis techniques and expertise to address malicious cyber activity targeting our nation's networks. US-CERT develops and deploys timely and actionable information to federal departments and agencies, state and local governments, private sector organizations, and over 200 international partners. US-CERT operates the National Cybersecurity Protection System, providing federal departments and agencies with intrusion detection and prevention capabilities.

ICS-CERT strengthens control systems cybersecurity through public-private partnerships. ICS-CERT has four focus areas: 1) situational awareness for stakeholders, 2) control systems incident response and technical analysis, 3) control systems vulnerability coordination, and 4) strengthening cybersecurity partnerships with government departments and agencies.

National Coordinating Center (NCC) for Telecommunications leads and coordinates the initiation, restoration, and reconstitution of telecommunications services or facilities under all conditions. The NCC leverages partnerships with government, industry, and international partners to obtain situational awareness and determine priorities for protection and response.

NCCIC Operations and Integration engages in planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts across all NCCIC branches and activities. This includes coordinating the continuity of operations responsibilities for alternate site operations to support minimal disruption to NCCIC mission essential functions. It acts as a 24-hour clearinghouse for critical cyber and communications

information and tracks and initiates critical information requirements that guide the dissemination of critical information.

The NCCIC operational activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation, and recovery actions. As the incident stabilizes, each organizational response effort is able to support the transition from response to recovery.

As mutually supporting, fully integrated elements of the NCCIC, these branches provide the authorities, capabilities, and partnerships necessary to lead a national approach to addressing cybersecurity and communications issues at the operational level.

The NCCIC organization works closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems and actively engages with private sector companies and institutions; state, local, tribal, and territorial governments; and international counterparts. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology with which they own, operate, manage, or interact.

Response

Unity of Effort Through Unified Command Supported with ICS-CEA

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 several critical infrastructures and their related sectors.

In 2013, ICS-CEA has been used for responding to multiple requests by the NCCIC regarding the identification of potentially affected critical infrastructure sectors because of natural and potential man-made threats.

Recovery

ICS-CERT Applies Advanced Capabilities to Support Recovery

ICS-CERT works with critical infrastructure asset owners and operators to respond to cyber incidents that impact any of the 16 critical infrastructure sectors. ICS-CERT supports recovery of the affected organization by providing adequate interim and long-term solutions and subject matter expertise for immediate actions. The response and recovery are specific to the incident and needs of the organizations.

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 2013, ICS-CERT conducted 72 onsite assessments across the US critical infrastructure sectors. 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 and systems are similar. This year has seen increased partnering with the commercial nuclear industry and the energy sector with regard to performing onsite cybersecurity assessments.

Cybersecurity assessments and recovery plans are tailored to each individual organization depending on the level of complexity in the systems. Asset owners can now request CSET evaluations and/or Architecture Reviews, which is a more in-depth comprehensive evaluation of specific control systems networks, architectures, and components, to support system analysis and future recovery actions.

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

Future

ICS-CERT will advance and ensure the resilience and reliability of the Nation's critical infrastructure and protect key resources. ICS-CERT's mission is essential to the economic welfare and safety of the American people.

ICS-CERT will engage and work with critical infrastructure vendors, operators, and asset owners across the country to enable response efforts to address a variety of cybersecurity risks. A computer based training course is being developed to engage a larger number vendor owner and operators. This training will allow the program to reach more critical infrastructure professionals across the country. The program will further enable a framework that acknowledges the concept of tiered response, which emphasizes enabling the best possible support to meet the unique challenges of each critical infrastructure sector.

ICS-CERT is committed to supporting a community of critical infrastructure stakeholders to address future needs and continue to improve cybersecurity capabilities. The Industrial Control System Joint Working Group (ICSJWG) will support membership groups to align activities and more effectively employ member expertise. Going forward, the governing body of ICSJWG will focus on development of working group meetings, webinars, product review and approval, socialization and marketing of deliverables. This approach will deliver on a flexible and resilient approach to partner engagement, as well as provide a substantial platform for the public and private sectors to collaborate on the cybersecurity of the critical infrastructure in FY-14.

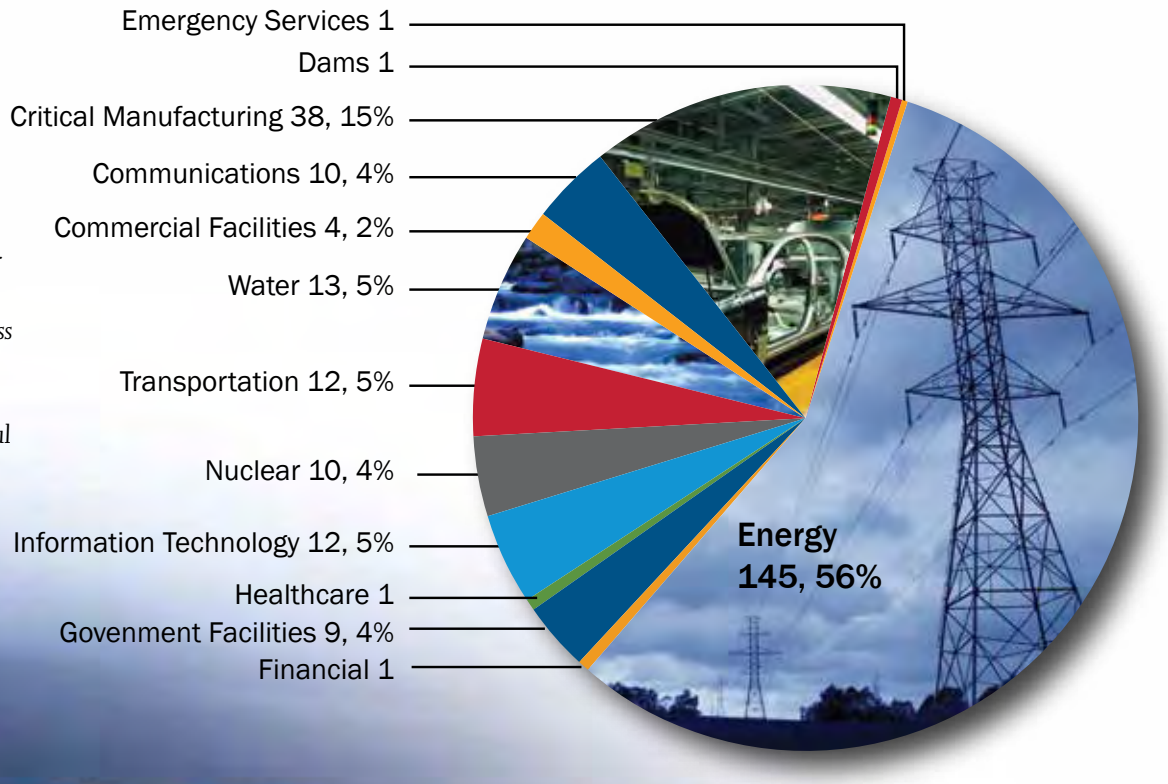
The program will continue to support: engaged partnership; tiered response; scalable, flexible, and adaptable operational capabilities; unity of effort through unified command; and readiness to actively engage the public and private sectors, as well as international partners to prepare for, prevent, and respond to cybersecurity incidents that could impair strategic assets. The rollout of CSET 6.0 will provide an unprecedented level of organizational interaction with the tool to baseline and track cybersecurity. ICS-CERT continually improves the program's 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 all aspect of preparedness and capabilities based on the specific needs and requirements of the requesting customer. This tailored approach provides scalable response to cybersecurity challenges across critical infrastructures.

Critical Infrastructure Sectors

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

ICS-CERT Responses



This chart illustrates the number of ICS-CERT responses to sector specific cybersecurity threat across the critical infrastructure sectors. Any percentage noted is the percentage as it relates to the total response for FY-13.

Sector Specific On Site Support Fiscal Year (FY)

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7. The sectors changes include redistribution of the Postal & Shipping and National Monuments & Icons on the sector breakout. Table 1 compares the overall sector support statistics for on site assessments in fiscal years 2011, 2012, and 2013. PPD-21 identifies 16 critical infrastructure sectors:

Table 1.

Sector	FY-11	FY-12	FY-13	Cumulative
Chemical Sector	0	4	0	4
Commercial Facilities Sector	10	2	0	12
Communications Sector	1	0	2	3
Critical Manufacturing Sector	2	1	0	3
Dams Sector	0	0	0	0
Defense Industrial Base Sector	0	12	1	13
Emergency Services Sector	2	3	0	5
Energy Sector	11	7	18	27
Financial Services Sector	1	6	0	7
Food and Agricultural Sector	5	0	0	5
Government Facilities Sector	5	3	2	10
Healthcare and Public Health Sector	6	1	5	12
Information Technology Sector	3	5	2	10
Nuclear Reactors, Materials, and Waste Sector	2	8	8	18
Transportation Systems Sector	7	10	10	27
Water and Wastewater Systems Sector	21	25	24	70
Totals	**76**	**87**	**72**	**235**
Number of Sectors Assessed	13/16	13/16	9/16	15/16

NCCIC/ICS-CERT Metrics Fiscal Year (FY)

Table 2: Compares the overall incident, vulnerability, onsite event, and information product statistics for fiscal years 2011, 2012, and 2013, indicating control system cyber events and activity.

Table 2.

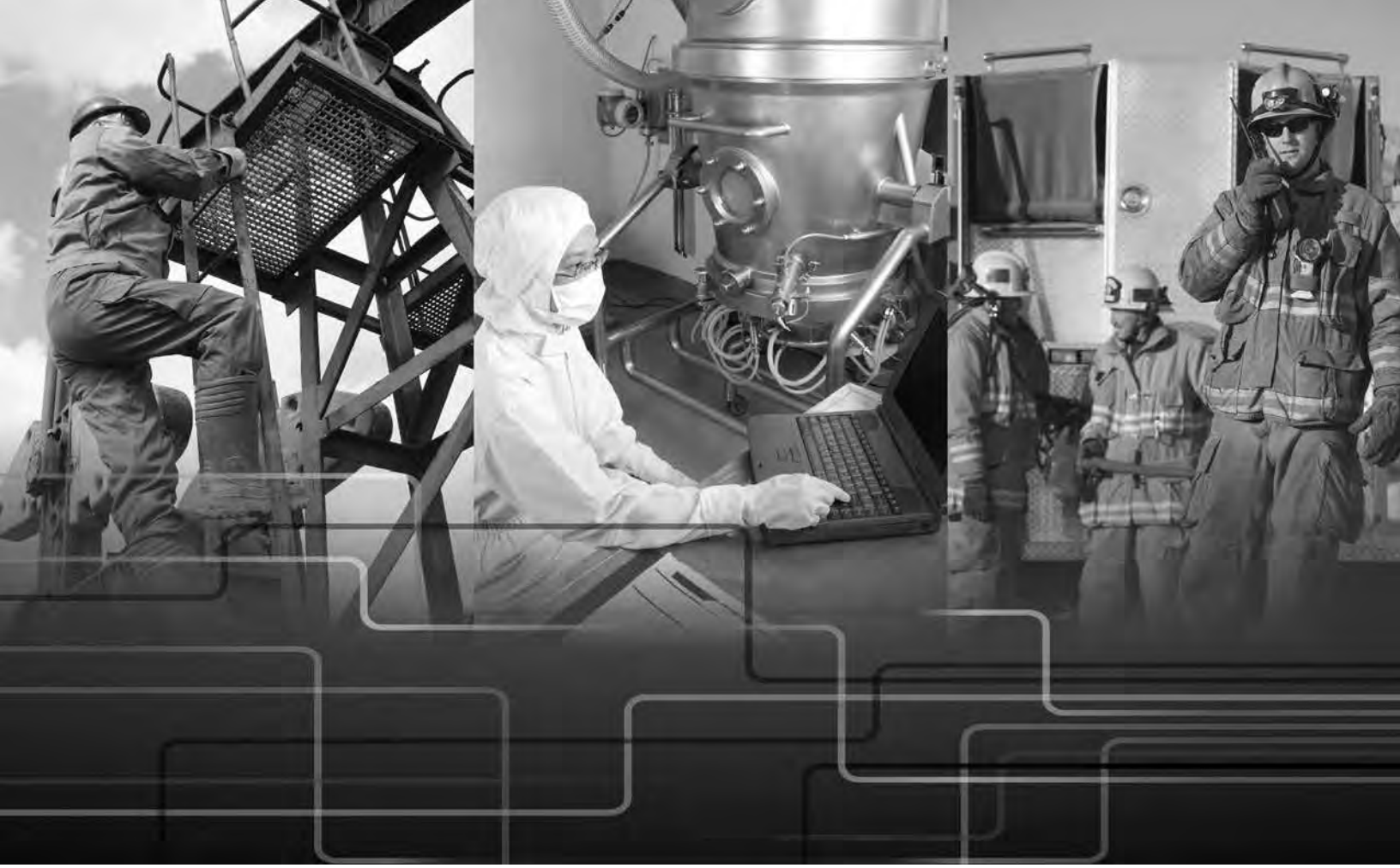
NCCIC/ICS-CERT FY Metrics	2011 Totals	2012 Totals	2013 Totals
ICS Incident Reported - Tickets	140	197	257
ICS Incident Response Onsite Deployments	7	6	7
ICS-Related Vulnerability Report - Tickets	139	137	187
NCCIC/ICS-CERT Information Products	243	347	295
Distributed or Downloaded CSET	5,100	6,631	5,085
Onsite Assessments	81	89	72
Professionals Trained	1,686	2,327	693
Number of Training Sessions	47	56	17
ICSJWG Membership	1,012	1,371	1,476
Speaking Engagements	137	205	162
Conference Exhibitions	20	22	2

NCCIC/ICS-CERT Metrics Calendar Year (CY)

Table 3: Compares the overall incident, vulnerability, onsite event, and information product statistics for calendar years 2011, 2012, and 2013, indicating control system cyber events and activity.

Table 3.

NCCIC/ICS-CERT Metrics	2011 Totals	2012 Totals	2013 Totals
ICS Incident Reported - Tickets	204	138	256
ICS Incident Response Onsite Deployments	7	6	5
ICS-Related Vulnerability Report - Tickets	141	147	181
NCCIC/ICS-CERT Information Products	283	343	285
Distributed or Downloaded CSET	7,448	5,584	4,175
Onsite Assessments	70	89	76
Professionals Trained	1,658	2,241	445
Number of Training Sessions	47	52	12
ICSJWG Membership	1040	1,416	1,544
Speaking Engagements	164	200	147
Conference Exhibitions	20	19	1



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:

Toll Free: 1-877-776-7585

International Callers: (208) 526-0900

Email: *ics-cert@hq.dhs.gov*

For industrial control systems security information and incident reporting: *http://ics-cert.us-cert.gov*

For more information about the ICS-CERT program visit: *https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team*

Homeland Security

National Cybersecurity and Communications Integration Center

13-50369