NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report

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

FY 2015

Homeland Security

Contents

Welcome from the NCCIC and ICS-CERT IV

1. INTRODUCTION 1

2. SUMMARY FINDINGS 2

  2.1 Assessment Activity 2

  2.2 FY 2015 Top Vulnerabilities 3

3. DETAILED ASSESSMENT RESULTS AND ANALYSIS 5

  3.1 Top Six Discoveries: Risks and Recommended Mitigation 5

4. OVERARCHING STRATEGIC OBSERVATIONS FROM FY 2015 11

  4.1 Inadequate Access Security Controls for Virtual Machines 11

  4.2 Insecure Implementation of Remote Access 11

  4.3 Improper Use of VLAN 11

  4.4 Risk of Bring-Your-Own-Device Policies to ICS 12

  4.5 Cloud Services: Harden External Hosting Security for Critical Functions 12

  4.6 ICS Network Monitoring as a Core Defense-in-Depth Strategy 12

5. ABOUT ICS-CERT'S ASSESSMENT OFFERINGS 13

  5.1 Cyber Security Evaluation Tool Assessments 15

  5.2 Design Architecture Review 15

  5.3 Network Architecture Validation and Verification 16

6. CONCLUSION 17

Appendix A. NIST 800-53 Security Control Family Descriptions 18

Appendix B. FY 2015 Top 20 Subcategory Discoveries 20

FIGURES

Figure 1. ICS-CERT Onsite Assessments Geographical Distribution. 2

Figure 2. CI Sectors Assessed in FY 2015 (includes CSET, DAR, and NAVV Assessments). 13

Figure 3. CSET Assessment High-Level Process. 15

TABLES

Table 1. ICS assessments performed by the ICS CERT Assessment Program. 2

Table 2. Top Six Weaknesses Discovered in FY 2015. 3

Table 3. Comparison of 2014 and 2015 Top Six Weakness Categories. 4

Table 4. FY 2015 Top 20 Identified Weaknesses by Security Control Family Subcategory. 5

Table 5. Top Six Discoveries: Risks and Recommended Mitigation 6

Table B1. Descriptions of FY 2015 Top 20 Subcategory Discoveries. 20

Welcome from the NCCIC and ICS-CERT

The National Cybersecurity and Communications Integration Center (NCCIC) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) are pleased to provide our critical infrastructure (CI) partners with the FY 2015 NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report.

The NCCIC spearheads the Department of Homeland Security's (DHS) efforts to prevent, protect against, mitigate, and respond to cyber and communications disruptions to CI. The NCCIC serves as a national hub for cyber and communications information sharing, in near-real-time whenever possible, and provides assistance to respond to incidents on stakeholder assets. These activities fall under the "Information Sharing" and "Incident Response" lines of effort outlined in the Office of Cybersecurity and Communications (CS&C) Implementation Strategy for FY16-18. Within the NCCIC, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) leads DHS efforts to enhance the cybersecurity and resilience of the industrial control systems (ICSs) upon which much of the Nation's CI relies. In partnership with the ICS community, ICS-CERT provides unique analytical, technical, and information products to help CI owners and operators proactively enhance their control systems cybersecurity posture and incident response capabilities to limit the severity of incidents.

This report provides a year-end summary of the NCCIC/ICS-CERT security assessment activities. Security assessments are essential to helping CI owners and operators proactively understand their vulnerability to cyber threats and measure their ICS security posture against accepted industry standards. This work directly supports the "Leading Practices and Risk Management" line of effort reflected in the CS&C Implementation Strategy for FY16-18 which includes performing risk assessments with CI organizations to help organizations improve their own security, establish a relationship with companies, and provide DHS with a better understanding of sector-specific and national risk.

The report provides our partners with common cybersecurity findings and identifies weaknesses from assessments conducted in FY 2015. In addition, this report outlines risk mitigation actions that ICS users should consider when addressing control systems cybersecurity in their organizations.

ICS-CERT will continue to share analytical reports to assist CI owners and operators with managing control systems risk. We hope our partners find the information contained in this report useful.

Thank you.

John Felker, Director of Operations
NCCIC
Department of Homeland Security

Marty Edwards, Director
ICS-CERT
Department of Homeland Security

1. INTRODUCTION

The FY 2015 NCCIC/ICS-CERT Industrial Control Systems Assessment Summary Report identifies common control systems cyber-weaknesses, provides risk mitigation recommendations, and provides a broader strategic analysis of the evolving ICS cybersecurity landscape. Reporting periods for assessment data spans the Federal fiscal year (October-September).

As the cyber-threat landscape continues to evolve, control systems and their underlying architecture must be secured to withstand cyber attacks. It is important that organizations conduct both risk and vulnerability assessments for the systems that drive the critical automation and processes that support our Nation's CI. From the launch of the ICS-CERT assessment program in FY 2009 through the end of FY 2015, ICS-CERT conducted roughly 535 assessments for government and private sector CI owners and operators. Cybersecurity assessments help CI partners to understand their ICS security strengths and weaknesses and help guide decisions to enhance their cybersecurity posture.

The ICS-CERT Mission

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

In FY 2014, ICS-CERT issued the first ICS Assessment summary report. Many of the critical weaknesses identified in FY 2014 remained prominent in FY 2015. ICS-CERT draws the vulnerability-specific data contained in the summary report from its Design Architecture Review (DAR) and Network Architecture Validation and Verification (NAVV) assessments. These are deep dive ICS assessments conducted in close partnership with CI facility owners and operators. ICS-CERT also maintains the Cybersecurity Evaluation Tool (CSET®), available as both a facilitated assessment and a downloadable self-assessment product. ICS-CERT does not retain data from CSET assessments.

The discoveries and mitigation recommendations described in the summary report are not all-inclusive or prescriptive. Summary report information should be reviewed and applied to an organization's overall cybersecurity framework and program as appropriate to that organization. Addressing the best practices and recommendations in this report can improve a CI asset owner's overall security posture and heighten awareness of potential threats or cyber attacks targeting their operations.

2015 Assessment Snapshot

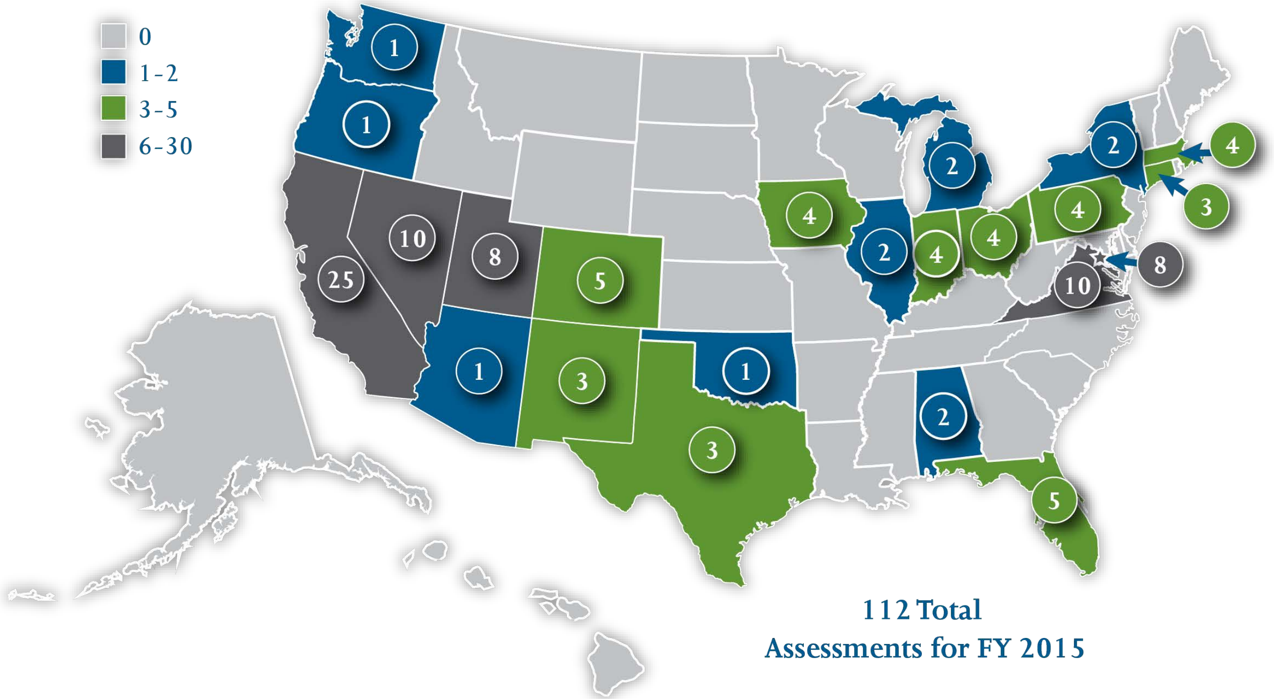
- ICS-CERT conducted 112 assessments in FY 2015, including 38 facilitated CSET®, 46 DAR, and 28 NAVV assessments.
- There were 638 weaknesses identified through DAR and NAVV assessments.
- The top six categories represented 36 percent of all weaknesses.
- Boundary protection was the most commonly identified area of weakness in both FY 2014 and FY 2015.
- Weaknesses related to boundary protection and least functionality represented 21 percent of all discovered weaknesses.
- Key trends included pervasive issues related to virtual machines, remote access, virtual local area network (VLAN) use, bring your own device (BYOD) risks, use of cloud services, and ICS network monitoring.

2. SUMMARY FINDINGS

2.1 Assessment Activity

As shown in Figure 1, ICS-CERT conducted 112 assessments in FY 2015. Demand for ICS-CERT assessment products continues to increase, particularly for in-depth assessment products: the DAR and NAVV assessments. This increase in demand is in part due to growing awareness of ICS-CERT's assessment capabilities and in part due to increased awareness among CI partners of the importance of understanding and improving their ICS cybersecurity posture.

FY 2015 Onsite Assessments by State



112 Total
Assessments for FY 2015

Figure 1. ICS-CERT Onsite Assessments Geographical Distribution.

Table 1 shows assessments by type from FY 2009 through FY 2015 and highlights increased demand for DAR and NAVV deep-dive assessments.

Table 1. ICS assessments performed by the ICS-CERT Assessment Program.

Assessment Type	FY 2009	FY 2010	FY 2011	FY 2012	FY 2013	FY 2014	FY 2015	Total
CSET	20	57	81	83	60	49	38	388
DAR	NA	NA	NA	2	10	35	46	93
NAVV	NA	NA	NA	4	2	20	28	54
Total	20	57	81	89	72	104	112	535

2.2 FY 2015 Top Vulnerabilities

ICS-CERT assessments uncovered 638 weaknesses in FY 2015. The top six areas of weakness accounted for approximately 36 percent of all weaknesses identified in FY 2015 assessments, as shown in Table 2.

Table 2. Top Six Weaknesses Discovered in FY 2015.

Area of Weakness	Consequence/Risk
Boundary Protection	· Cannot detect unauthorized activity in critical systems. · Increased risk to critical assets with weak boundaries between ICS and Enterprise networks.
Least Functionality	· Creates vectors for malicious party access to critical systems. · Rogue internal access could be established.
Authenticator Management	· Unsecured password communications can easily be compromised. · Password compromise could allow trusted unauthorized access to systems.
Identification and Authentication	· Results in lack of accountability and traceability for user actions if an account is compromised. · Increases difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access.
Least Privilege	· The more authorized users with elevated privileges, the larger the attack surface for an intruder to steal account credentials with elevated access rights to access and compromise critical systems.
Allocation of Resources	· Understaffing impedes organizational cybersecurity monitoring and response capability to a critical system cyber incident increasing the potential impact to the company.

The most common ICS cyber weakness in both FY 2014 and FY 2015 was insufficient network boundary protection. Monitoring and control of communications at the ICS network boundaries is a key tenet of the cybersecurity defense-in-depth concept. Boundary protection effectively slows attack processes and facilitates detection, analysis, and notification of unauthorized activity to support operational and incident response. Absent strong protection, attackers can more easily penetrate the network boundary around critical assets, access valuable information, and manipulate systems controlled by ICS. Vulnerabilities related to least functionality were the second most commonly identified concern. Specific issues include insufficient use of whitelisting; employing insecure, outdated, or otherwise vulnerable operating system services; and leaving communications ports accessible when not required for system operations. Shutting down all nonessential ports, services, and applications reduces the attack surface of the ICS and improves the ability to monitor and provide analysis of essential communications traffic.

Boundary Protection

- In both FY 2014 and FY 2015, Boundary Protection was the single most common ICS weakness discovered during assessments.
- Effective Boundary Protection is a pillar of the cybersecurity Defense-in-Depth concept.

Table 3 compares the top six weaknesses discovered in FY 2014 to those discovered in FY 2015 (***italics*** indicates that the weakness appeared in the top six for both years). Boundary protection continued to present the most common weakness discovered across both years, representing roughly 13 percent of all discovered weaknesses in FY 2015 and 11 percent in FY 2014. Boundary protection was identified as a weakness in 63 percent of the DAR assessments performed in 2015.

Table 3. Comparison of 2014 and 2015 Top Six Weakness Categories.

2014 Top Six Weaknesses	2015 Top Six Weaknesses
Boundary Protection	*Boundary Protection*
Information Flow Enforcement	Least Functionality
Remote Access	Authenticator Management
Least Privilege	Identification and Authentication
Physical Access Control	*Least Privilege*
Security Function Isolation	Allocation of Resources

3. DETAILED ASSESSMENT RESULTS AND ANALYSIS

In FY 2015, ICS-CERT provided mitigation recommendations for 638 weaknesses identified through 74 DAR and NAVV assessments. ICS-CERT's assessment methodology categorizes weaknesses based on the National Institute of Standards and Technology's (NIST) NIST 800-53 control family subcategories (See Appendix A for Control Family descriptions). The Top 20 categories of weaknesses make up 69.4 percent of the total weaknesses identified. Table 4 shows the Top 20 weakness categories discovered in 2015. Appendix B provides brief descriptions of each category.

Table 4. FY 2015 Top 20 Identified Weaknesses by Security Control Family Subcategory.

NIST 800-53 Control Family Sub-Category	Number of Discoveries
SC-7 Boundary Protection (13% of 638 Total DAR/NAVV discoveries)	85
CM-7 Least Functionality	46
IA-5 Authenticator Management	27
IA-2 Identification and Authentication	25
AC-6 Least Privilege	23
SA-2 Allocation of Resources	23
AU-6 Audit Review, Analysis, and Reporting	22
PE-3 Physical Access Control	19
SI-2 Flaw Remediation	19
CM-4 Security Impact Analysis	19
AT-2 Security Awareness Training	17
CP-9 Information System Backup	17
CM-6 Configuration Settings	16
AT-3 Role-Based Security Training	15
CM-3 Configuration Change Control	14
SA-8 Security Engineering Principles	13
AC-17 Remote Access	11
SC-8 Transmission Confidentiality and Integrity	11
AC-2 Account Management	10
SA-4 Acquisition Process	10

Top 6 Discoveries

3.1 Top Six Discoveries: Risks and Recommended Mitigation

While ICS-CERT assessments identified weaknesses across all control families, six categories were most prevalent, representing 35.8 percent of the total vulnerabilities discovered across assessed CI sectors. The top six categories were: Boundary Protection, Least Functionality, Authenticator Management, Identification and Authentication, Least Privilege, and Allocation of Resources. Table 5 summarizes the six most common vulnerabilities by security control family, subcategory, potential risk, and recommended mitigations.

Table 5. Top Six Discoveries: Risks and Recommended Mitigation.

1. System and Communications Protection: Boundary Protection (SC-7) 85 Discoveries
Description
• Controls associated with the monitoring and control of communications at the ICS external electronic boundaries and key internal boundaries, the implementation of subnetworks to separate critical systems, and the implementation of managed protective interfaces for external connectivity to critical systems.
Concerns if Not Mitigated
• Without adequate boundary protections for the ICS network, it becomes difficult to detect unauthorized activity. Weak boundary protection provides various vectors for unauthorized interfacing with devices and systems, which directly support the control process.
• The scope of threats and general risk to control systems operations increases significantly without logical separation of the ICS network from enterprise networks (or from untrusted systems, i.e., the Internet).
Recommended Mitigation
• Separate the enterprise network from the ICS network and establish a demilitarized zone (DMZ) between the two systems for ICS perimeter protection. Refer to NIST 800-SP 82 Chapter 5 for information on designing perimeter protections for an ICS.
• The DMZ should house a dedicated “jump” server that would permit systems on the enterprise network (or those accessing via a remote method, e.g., a virtual private network [VPN]) to access data elements derived from the ICS network.
• The jump server should be hardened, running only essential services. Credentials for this server should not be the same as those that are used for authentication to systems on the enterprise network.
• Ingress/Egress communication flows to this server should be restricted to the minimal subset of those that are required to support secure methods for accessing ICS systems (when needed to access from outside the standard ICS network).
• Logging and monitoring of information derived from this system should be incorporated with continued verification.
• Security devices and systems need to be resident in the DMZ to support ICS system network equipment patching and updates (antivirus update server, Windows Server Update Services [WSUS] patch update, etc.).

2. Configuration Management: Least Functionality (CM-7)

46 Discoveries

Description

- Controls associated with minimizing the computing resources of systems functions, ports, protocols, and services to only those required to support system essential operations.

Concerns if Not Mitigated

- Unnecessary services, ports, protocols, applications, and functions create vectors for malicious parties to gain access to the ICS.
- Unauthorized personnel could plug rogue devices into open ports (or unplug an authorized device and connect) to gain access to the network.

Recommended Mitigation

- Determine the necessary operational requirements, services, ports, protocols, and applications to complete the needed function of each system component. Restrict the component to allow only the use of the necessary requirements.
- Use available hardening guidelines and vendor operational requirements to determine the settings that allow the necessary system functionality and document exceptions.

3. Identification and Authentication: Authenticator Management (IA-5)

27 Discoveries

Description

- Controls associated with the management of system authenticators. Often ICSs or operations control centers either don’t support strong password management or operational implementation of individual passwords is not appropriate to the operating environment.

Concerns if Not Mitigated

- Passwords verify the authenticity of a user. If a password is compromised, the system assumes the user is an authorized party.
- Passwords can be easily compromised using techniques such as brute force (password guessing) or pass the hash techniques.
- If encryption is not enabled on authentication, meaning password data are transferred as clear text, attackers can simply listen to the traffic and pull the user name and passwords off the wire while in transit. Once compromised, persistent access is granted for the lifetime of the user accounts and passwords (i.e., account passwords that never expire or inactive/legacy accounts that are not disabled when not in use).

Recommended Mitigation

- Establish and enforce a password policy. Protect those passwords via encryption. This policy should require the use of strong passwords and the periodic change of those passwords.
- Implement additional requirements for remote access connections to verify the authenticity of parties requesting access remotely. Multi-factor authentication is typically seen as two or more of the following; something known (password), something possessed (RSA token or public key infrastructure [PKI] certificate), and something a user is (i.e., biometrics; such as a voice print).

4. Identification and Authentication: Identification and Authentication (IA-2)

25 Discoveries

Description

- Controls implemented for the identification and authentication of authorized organizational users (or processes acting on behalf of organizational users).

Concerns if Not Mitigated

- Lack of accountability for individual user actions.
- Shared accounts decrease nonrepudiation, which reduces accountability and traceability if an account is compromised.
- This practice also makes it more difficult to secure accounts when someone leaves the organization, especially if there are no policies and procedures to have accounts and passwords changed when an administrator leaves the organization.

Recommended Mitigation

- Establish individual user accounts where possible and document the use of shared accounts.
- All system administrators and users should have their own unique accounts. Where applicable, system administrator accounts should be integrated with active directory (AD).
- Where group user accounts are used, such as in an ICS control center environment, additional methods of accountability should be used, such as access key cards, log books, etc.

5. Access Control: Least Privilege (AC-6)

23 Discoveries

Description

- Controls established to limit access for authorized users and the processes used by them to only those that are necessary to accomplish their assigned tasks.

Concerns if Not Mitigated

- An attacker or malicious insider can leverage user and computer accounts to potentially gain access to the ICS.
- Assigning elevated or enhanced privileges to personnel above and beyond what they may require for their job functions introduces risk and provides a means for either intentional (malicious insider/outsider) or unintentional (accidental) consequences.
- Common vulnerabilities associated with the use of unnecessary privileges include the unauthorized installation of unapproved or untested software, the execution of malware or malicious application on a critical asset, or access rights to disable security features and controls (antivirus, host-based firewall) or modify application permissions or configuration settings.

Recommended Mitigation

- Enforce the concept of least privilege on all systems. Users that need elevated privileges should have accounts that allow privileges based on the work they are performing, using elevated privileges only when required.
- Work with the vendor to investigate methods to run and access supervisory control and data acquisition (SCADA) applications without the need of utilizing administrative/root level privileges on local systems.

6. System and Services Acquisition: Allocation of Resources (SA-2)

23 Discoveries

Description

- Organizational support for the sustainment of security resources, equipment, and personnel. Often the weakness was identified due to concerns by staff of having the right skills, training, and number of personnel needed to implement security measures and sustain the operational needs to maintain security operations.

Concerns if Not Mitigated

- Understaffing impedes the ability to respond to cybersecurity issues and events and impacts efficient maintenance of systems. Understaffed operations efforts are typically spent addressing day-to-day operational issues, and if time permits, the regular maintenance operations. Little time is generally available for staff to improve the systems security posture.

Recommended Mitigation

- As your organization establishes its risk appetite, evaluate the cost/benefit of hiring staff to allow for regular maintenance operations, and allow adequate time to implement proactive security measures (for example, reviewing logs, hardening networks, and testing upgrades and security patches).

4. OVERARCHING STRATEGIC OBSERVATIONS FROM FY 2015

Meeting with industry and government organizations provides the opportunity to not only share what ICS-CERT found at specific facilities, but also to see shifts in technology use in control systems operational and security environments. In FY 2015, ICS-CERT saw significant changes in the application of various technologies and corresponding challenges in implementing them securely. These include challenges related to use of virtual machines, remote access, VLANs, BYOD policies, cloud services, and network monitoring.

4.1 Inadequate Access Security Controls for Virtual Machines

Increasingly, CI asset owners are implementing and leveraging virtual machine (VM) technologies as a method of reducing capital equipment, managing device recovery, and running multiple disparate guest operating systems on a single physical host machine. ICS-CERT continues to see inadequate user access security controls to the hypervisor (VM monitor) host management interface with many of these implementations. This provides a single point of failure and entry that adversaries could use to control every guest VM on the host computer. These interfaces should be placed within management networks with strict and logged zone access control. This ensures that network, host, and VMs are provided with adequate security controls. When CI owners and operators configure the physical host to contain both DMZ and ICS servers, the networks and network interface controls (NIC) should be hardened, and all others deleted to prevent the possibility of opening up a bridged scenario. It is also imperative that operational technology (OT) and information technology (IT) departments coordinate regular patching of the hypervisors to minimize impact to ICS processors.

4.2 Insecure Implementation of Remote Access

Use of remote access — while not a new concept — raises a number of issues that managers should consider prior to documenting a policy and implementing a process. Whether access is from the corporate network to the ICS or from the Internet to the ICS, this access provides a serious risk to the system. Attackers can gain access to user accounts at the users' home or corporate office and obtain the user credentials and connection to access critical ICS assets or allow an infected computer an access channel into the networks via a VPN connection. The organization must therefore decide what, if any, access it will require from these remote locations, who needs that access, and how to harden the access process to reduce the risk to an acceptable level. The use of multi-factor authentication and limiting VPN access to hardened and monitored jump servers can reduce these risks.

4.3 Improper Use of VLAN

VLAN technology has been around for a long time; in fact, implementing VLANs as security mechanisms is a standard practice in many configurations. While VLANs can logically segment networks, if users do not follow best practices of the hardware vendors, network activity can traverse to other VLAN segments. Default and native VLANs that remain unchanged on trunk ports provide an avenue where jumping from one VLAN to another is possible.

4.4 Risk of Bring-Your-Own-Device Policies to ICS

Operations, maintenance, and engineering personnel are increasingly implementing portable computing devices—such as tablets, smart phones, and laptops—in ICS environments. A number of organizations are actively promoting their use because of their popularity and convenience of mobility while maintaining access. However, such devices are not typically managed by the organization and security policies implemented by the organization are often not also implemented on the portable devices. Use of BYODs to access personal email, web pages, and social media applications, are inherently high risk to ICS. This risk must be considered by the organization and appropriate measures, such as mobile device management systems, should be put into place to mitigate the risk to acceptable levels.

4.5 Cloud Services: Harden External Hosting Security for Critical Functions

ICS-CERT is seeing some organizations utilizing cloud services for data storage and considering methods of utilizing them for additional services to support their ICS architectures. Organizations must ensure that the parts of any ICS architecture hosted externally have a level of security consistent with the criticality of the functions of the ICS operation. Organizations must also consider ICS operational information integrity, security, and confidentiality, as well as functional and operational details associated with recovery, event/incident management, failover, forensic support, monitoring, and other operational sequences that require special support by the cloud-hosting service provider. Legal instruments, such as service level agreements, are important because all operational support should be explicitly identified. This ensures that support by cloud service providers — and Internet service provider (ISP) availability and bandwidth capacity — are sufficient to manage any operational issues that may surface. Issues that are sometime overlooked when shifting resources to the cloud include reliance on ISP connections on premise and the corresponding potential of bandwidth increases. The effects of load balancing and effects associated with an upsurge in data usage by other ISP customers should also be considered.

4.6 ICS Network Monitoring as a Core Defense-in-Depth Strategy

The concept of Defense-in-Depth (DiD) is premised on early detection and alerts of an intrusion to ensure defensive action can be taken before the breach of critical assets. Network monitoring is an absolute requirement for any critical system. Having an electronic boundary around the ICS is not sufficient to protect critical assets from unauthorized access. For each protection in a network environment, attackers can find a method to overcome that protection. Most CI organizations have some level of monitoring at the corporate level, but this is rarely implemented within the ICS networks. Network monitoring can be done and collected in many ways, such as using free centralized syslog servers for Linux and network devices to centrally collect Windows Events using winrm and wevtutil utilities, but these events (logs) must also be reviewed. Solutions such as security information and event management (SIEM) products exist that can collect, log, and correlate information from multiple sources and alert on anomalous or specified activity and provide real-time analysis. Technologies for monitoring include log collection and management to windows hosts with free utilities such as the Microsoft wevtutil utility and local logs on firewalls. Canaries and honeypots/honeynets are other concepts that flag any unauthorized intrusion to sophisticated SIEM products and services, combining security information management and security event management.

5. ABOUT ICS-CERT'S ASSESSMENT OFFERINGS

ICS-CERT offers cybersecurity assessments of ICS to government and private sector CI organizations across all 16 CI sectors. In FY 2015, ICS-CERT conducted assessments (including CSET, DAR, and NAVV assessments) in the Chemical, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Information Technology, Transportation, and Water Sectors. Figure 2 provides a percentage breakout of all FY 2015 assessments by CI sector.

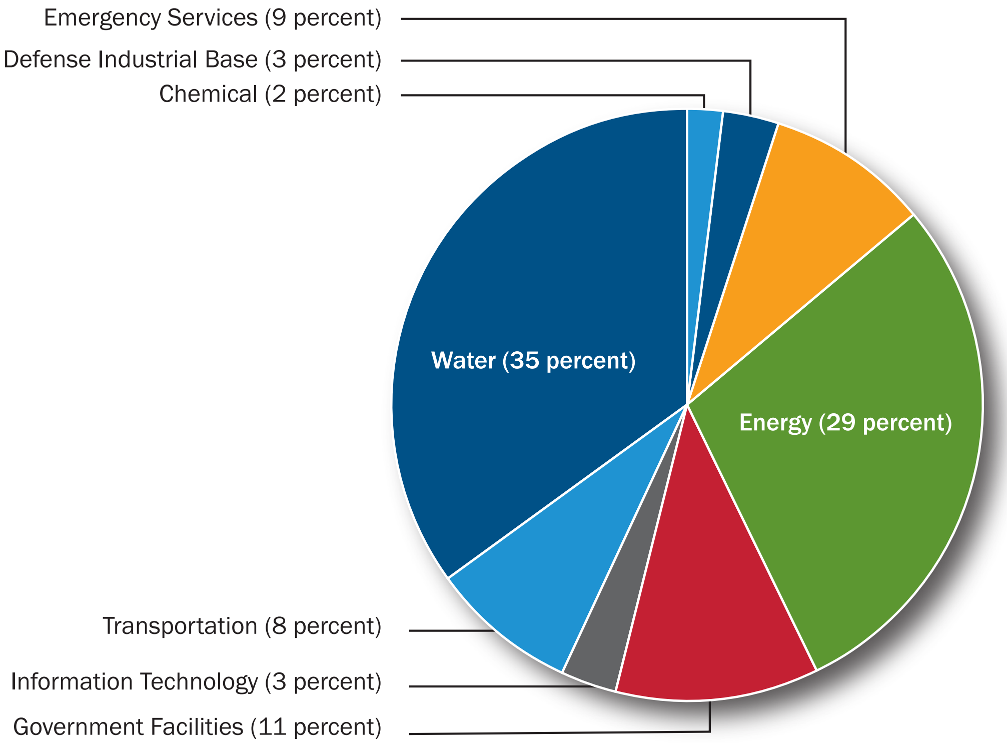


Figure 2. CI Sectors Assessed in FY 2015 (includes CSET, DAR, and NAVV Assessments).

The types of organizations for which ICS-CERT conducts assessments vary greatly, ranging from small organizations that have never completed a cybersecurity evaluation of their control systems to large multinational corporations. Data collected during assessments is anonymized and used for trend and other analyses.

Working with CI Partners

- CI owners and operators request ICS cybersecurity assessments on a voluntary basis.
- ICS-CERT prioritizes assessments resources based on factors such as CI sector risk profile, specific threat information, and the dependence of specific CI sectors on control systems.
- The number of assessments in any given sector and geographic region fluctuate from year to year, based on the current threat landscape and other factors.

ICS-CERT provides three primary assessment services:

1. Cybersecurity Evaluation using CSET
2. DAR
3. NAVV.

ICS-CERT uses NIST's Recommended Security Controls for Federal Information Systems (NIST 800-53) to group and analyze weaknesses discovered during assessments. NIST 800-53 control family mappings provide a consistent and repeatable methodology for collecting and correlating data to analyze and trend key discoveries at a holistic level.

NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," implements an ICS overlay to NIST 800-53, tailoring security guidance to the unique ICS operational and system characteristics. While NIST Special Publication 800-82 applies generally to all CI control systems, ICS-CERT can work with sector stakeholders to provide additional tailoring to unique aspects of individual sectors, as necessary. Appendix A shows the top-level NIST 800-53 Security Control Families.[a]

Requesting An Assessment

- ICS-CERT assessments are available at no cost to CI asset owners and operators.
- ICS-CERT provides an in-depth post-assessment report to the asset owner, describing key discoveries and risk mitigation options for enhancing ICS cybersecurity.
- Information shared with ICS-CERT can be protected by DHS as Protected Critical Infrastructure Information (PCII).

[a] Additional information on NIST 800-53 Security Control Families and subcategories can be found http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

5.1 Cyber Security Evaluation Tool Assessments

DHS developed CSET to support a basic evaluation of cybersecurity posture based on standards and practices best suited to their sector. CSET is available as a downloadable software product to support user self-assessments as well as a facilitated assessment service. Figure 3 shows the high-level CSET process.

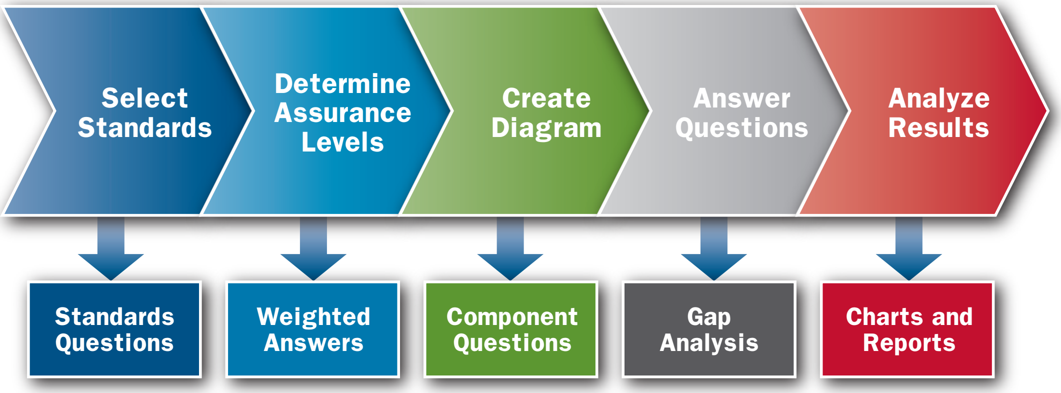


Figure 3. CSET Assessment High-Level Process.

To maximize the effectiveness of the CSET evaluation process, the asset owner should include subject matter experts from various disciplines to conduct the guided discovery-oriented evaluation of the entity's underlying control processes, procedures, policies, methodologies, and protective and detective security controls.

5.2 Design Architecture Review

A DAR is an assessment facilitated by ICS-CERT assessment personnel. ICS-CERT works with the system owners and operators to perform a deep-dive manual assessment and analysis of the operational process. The assessment focus is of the underlying ICS network architecture, integration of IT and OT teams, vendor support, monitoring, cybersecurity controls, and a review of internal and external connections utilized within the control systems environment. The DAR focuses heavily on ICS network architecture, asset inventory, and protective and detective security controls.

A DAR provides the asset owner with a thorough evaluation of system interdependencies, vulnerabilities, and mitigation options. It examines information related to key ICS external connections and includes an in-depth review of control systems design documents, drawings, and architectures. ICS-CERT provides a detailed final report to the user that captures the key discoveries identified by the team and provides potential impact and recommended mitigations for each.

2015 CI Cyber Risk Mitigation Status

- ICS-CERT conducts follow-up meetings with each asset owner to review the impact of the assessment findings.
- Follow-up meetings identify each site's plans and progress in mitigating identified areas of weakness.
- Asset owners make risk management decisions based on a variety of factors, including risk appetite, cost of mitigation strategies, feasibility, and ease of implementation.

5.3 Network Architecture Validation and Verification

The NAVV assessment entails the analysis of network traffic (passively captured) within the ICS network. ICS-CERT visualizes and performs analysis on the network traffic and device-to-device communications occurring within various ICS network segments to identify potential unauthorized or suspect communications. Threat data analysis of the traffic evaluates for indicators of known unauthorized attacks in the user's network. NAVV assessments enable asset owners to:

- Verify the accuracy of ICS network diagrams.
- Identify potentially rogue/misconfigured devices or malicious data communications.
- Analyze data flows to ensure boundary protection devices work as designed.
- Identify opportunities or areas to improve zoning and perimeter protections.
- Baseline the ICS network (including a protocol hierarchy and organization of network traffic).
- Gain practical knowledge of how to passively monitor and verify the communications occurring within their ICS networks.

The NAVV provides organizations with a view of network communication occurring within the ICS network infrastructure, in addition to those communications sourced from or destined to ICS network segments. ICS-CERT typically provides NAVV reviews as an extension to DARs, although this service is also offered independently.

6. CONCLUSION

The protection of the Nation's CI is essential for ensuring public confidence and safeguarding the Nation's safety, prosperity, and well-being. Much of our CI depends on automated control systems to manage industrial processes efficiently and securely, so it is essential that organizations conduct security assessments, so that they can understand how best to secure this architecture against cyber threats.

ICS-CERT will continue to improve its cybersecurity assessment services to meet the evolving needs of its CI customer base. ICS-CERT's assessment capabilities are a key part of a holistic cyber risk management program that helps CI stakeholders to better prepare for, protect against, mitigate, respond to, and recover from cyber incidents affecting ICS.

Over the coming years ICS-CERT will launch a number of new initiatives to expand access to assessment products and services, while continuously improving the quality of service offerings and the utility of mitigation recommendations. Future initiatives include, for example, launching train-the-trainer programs to enable DHS regional personnel to conduct CSET assessments for local customers. In addition, ICS-CERT will be instrumental in supporting assessments focused on federal facility building and access control systems. Understanding cyber risk is the first step in mitigating it. ICS-CERT remains committed to helping its partners gain a clearer comprehension of the threats and vulnerabilities they face and the actions they can take to secure their ICS.

Appendix A

NIST 800-53 Security Control Family Descriptions

ICS-CERT uses NIST's "Recommended Security Controls for Federal Information Systems" (NIST 800-53) to categorize the discoveries found during assessments. Using NIST 800-53 provides a consistent and repeatable methodology for collecting and correlating data.

The NIST 800-53 controls are organized into 18 families; each family contains subcategories related to the general security topic of the family. Subcategories include, for example, policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by system technologies. Descriptions of the 18 security control families follow:

Access Control (AC). The security controls governing the mechanisms, principles, processes, and other controls used to facilitate access to the information system.

Awareness and Training (AT). The security controls facilitating general and role-based security training of users in regard to the information system and the corresponding records of training.

Audit and Accountability (AU). The security controls used to define, record, analyze, and report on the actions of the information system.

Security Assessment and Authorization (CA). Security controls that define and establish how the information system will authorize for use, how the information system is checked to ensure that security controls are in place and deficiencies are tracked and corrected, and how the system is connected to external systems as well as its internal connections.

Configuration Management (CM). Security controls to manage the installation and configuration of the information system as a whole and per device. These controls establish documentation, planning, configuration, testing, and analysis of the hardware and software changes made to the information system.

Contingency Planning (CP). Security controls to define and aid in the recovery/restoration processes of an information system.

Identification and Authentication (IA). The controls to verify the identity of a user, process, or device through the use of specific credentials (e.g., passwords, tokens, biometrics) as a prerequisite for granting access to resources in an IT system.

Incident Response (IR). Security controls pertaining to incident response training, testing, handling, monitoring, reporting, and support services.

Maintenance (MA). Security controls governing the maintenance processes and tools.

Media Protection (MP). Security controls ensuring access to, marking, storage, and sanitization of media both electronic and physical.

Physical and Environmental Protection (PE). Security controls addressing the physical security and needs of an information system including environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, and fire protection).

Planning (PL). Security Controls comprising the security plan, security architecture, rules of behavior, and operations of the information system.

Personnel Security (PS). Security controls dealing with the security implications of information system personnel.

Risk Assessment (RA). Security controls to determine the risk of the information system. The control family includes the assessment of risk and scanning the system for vulnerabilities.

System and Services Acquisition (SA). Security controls that pertain to the establishment and operations of the information system, including its resources, development, and life cycle.

System and Communications Protection (SC). Security controls to protect the information system and its data as they are dispersed through the various channels of communication.

System and Information Integrity (SI). Security controls to ensure information system data are valid and authentic. Control family includes controls to address flaws in the system, malicious code, and error handling.

Program Management (PM). Provides enterprise-level security controls reaching across an entire organization.

Appendix B

FY 2015 Top 20 Subcategory Discoveries

Table B1 provides a summary overview of the top 20 discoveries and their percentage in the overall subcategory metric set of weaknesses identified in FY 2015 assessments.

Table B1. Descriptions of FY 2015 Top 20 Subcategory Discoveries.

#	Subcategory Discovery	Areas Where Weakness Discovered	% of Total Findings
1	SC-7 Boundary Protection	Network segmentation, network monitoring, and isolation of critical or sensitive network components	13.3%
2	CM-7 Least Functionality	Hardening systems and the use of whitelisting	7.2%
3	IA-5 Authenticator Management	Password protection and management	4.2%
4	IA-2 Identification and Authentication (Organizational Users)	Shared accounts, use of two factor authentication for remote access	3.9%
5	AC-6 Least Privilege	Administrative accounts, accounts with unnecessary privileges	3.6%
6	SA-2 Allocation of Resources	Staffing, lack of resources, excessive overtime of existing staff	3.6%
7	AU-6 Audit Review, Analysis, and Reporting	Logging and analysis	3.5%
8	PE-3 Physical Access Control	Securing physical sites	3.0%
9	SI-2 Flaw Remediation	Patching	3.0%
10	CM-4 Security Impact Analysis	Risk and Impact Analysis	3.0%
11	AT-2 Security Awareness Training	General cybersecurity awareness training	2.7%
12	CP-9 Information System Backup	System Backups	2.7%
13	CM-6 Configuration Settings	Baseline configurations, documentation of network	2.5%
14	AT-3 Role-Based Security Training	Role-based training of cybersecurity	2.4%
15	CM-3 Configuration Change Control	Change management processes, ensuring the right staff are included in change processes	2.2%
16	SA-8 Security Engineering Principles	Addressing obsolete systems, system life-cycle plans	2.0%
17	AC-17 Remote Access	Remote access policies and plans	1.7%
18	SC-8 Transmission Confidentiality and Integrity	Plain-text transmissions of sensitive material	1.7%
19	AC-2 Account Management	Centralized account management in moderate to large systems, processes to handle/ manage user accounts	1.6%
20	SA-4 Acquisition Process	Contract language that doesn't include security provisions.	1.6%

Department of Homeland Security

Office of Cybersecurity and Communications

National Cybersecurity and Communications Integration Center

NCCICCustomerService@hq.dhs.gov

1-888-282-0870

Industrial Control Systems Cyber Emergency Response Team

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