ICS-CERT Annual Assessment Report

Industrial Control Systems Cyber Emergency Response Team

FY 2016

NCCIC

NCCIC

Table of Contents

Welcome from the NCCIC and ICS-CERT

The past year was an eventful one for both the National Cybersecurity and Communications Integration Center (NCCIC) and the Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) Assessment program.

Cyber incidents at home and abroad in FY 2016 highlighted the continued and significant risks associated with cyber-attacks on industrial control systems (ICS). To meet both new and existing cybersecurity challenges, ICS-CERT redoubled efforts to provide its customers with comprehensive assessments of their ICS cybersecurity posture, arming them with both understanding of their cyber vulnerabilities and with the expert guidance they need to mitigate ICS cyber threats.

The third ICS-CERT Annual Assessment Report captures the Assessment team's consolidated discoveries and activities throughout the year. The report summarizes our key discoveries (including the most common vulnerabilities across our customer base), provides year-over-year vulnerability comparisons across critical infrastructure (CI) sectors, shows where we focused our activity in FY2016, describes how customers can request an assessment, and provides our customers with recommendations for enhancing their ICS cybersecurity posture.

The report also highlights some of the changes we are making to our assessment program to better serve our customers. For example, in FY 2016 we launched Version 8.0 of our Cybersecurity Evaluation Tool (CSET), adding new functionality to the tool. We began an extended hiring initiative to expand the number of assessment teams, enabling us to conduct more assessments for more customers each year. We also stood up the ICS Federal Critical Infrastructure Assessments (ICSFCIA) program, which focuses exclusively on providing assessments to Federal Government partners. The data and lessons we glean from this effort will, in turn, inform and support our continued focus on CI owned by the private sector and by state and local governments. Additionally, ICS-CERT is transitioning its assessment model from individual products to an integrated assessment process that includes all assessment offerings as well as more advanced analytics to provide improved actionable feedback to asset owners.

We hope our partners find the information contained in this report useful. We continue to look for ways to improve service to our customers and we hope that the changes to our assessment program, along with the discoveries and continued feedback that we provide our customers through our assessment team, will mitigate existing threats to control systems, help our customers stay ahead of the cyber-threat curve, and minimize the duration and severity of incidents if they do occur.

Thank you.

John Felker
Director of Operations, NCCIC

Marty Edwards
Director, ICS-CERT

1. Introduction

Fiscal Year 2016 marks the third publishing year for the ICS-CERT Annual Assessment Report.

As in previous years, the report provides our stakeholders with important information they can use to help secure their control systems and associated CI. This includes descriptions of the most common vulnerabilities found by our assessment teams in FY 2016 and the cybersecurity actions we recommend ICS owners and operators take to improve their cybersecurity posture.

Now more than ever, vital operational processes depend on secure and reliable control systems. In addition to traditional industrial processes, rapid increases in the connectivity of operational technology through the Internet of Things raise new challenges for control systems security. ICS-CERT continues to work with its government and private sector partners to identify, understand, and mitigate cyber threats to control systems and the CI they support.

1.1 Our 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.

We pursue this mission through a comprehensive cybersecurity program that helps our government and private sector partners improve ICS security across the entire risk management spectrum. For example, our Assessment team offers CI partners a suite of products and services that include in-depth facilitated assessments — our Network Validation and Verification (NAVV) and Design Architecture Review (DAR) assessments — as well as our Cybersecurity Evaluation Tool (CSET), a downloadable software product that enables CI partners to conduct their own assessments against a range of cybersecurity standards. Section 4 provides more detailed descriptions of our assessment program as well as instructions for requesting an assessment.

In addition to our cybersecurity assessment program, we offer our partners a wide variety of platforms through which to share technical information about new and existing ICS threats and vulnerabilities within a global partnership network. We also help our partners through technical malware and vulnerability analysis in our dedicated laboratory, provide cybersecurity training for all levels of knowledge and technical skill, and help our partners to respond to cybersecurity incidents focused on control systems.

Through ICS-CERT, our partners can also request services available through other NCCIC components. Examples of available services include machine-to-machine threat information exchange through the NCCIC's Automated Indicator Sharing program; enterprise network penetration testing, malware analysis, and incident response services; and cybersecurity exercises. ICS-CERT works closely with the NCCIC components that provide these services to ensure that our government and private sector partners can access the full range of NCCIC services and capabilities. Other NCCIC components include the United States Computer Emergency Readiness Team (US-CERT), National Coordinating Center for Communications (NCC), National Cyber Exercise and Planning Program (NCEPP), and National Cybersecurity Assessment and Technical Services (NCATS) team.

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.

2. FY 2016 Assessment Summary

We conducted 130 assessments in FY 2016, more than in any previous year. We also began a multi-year initiative to expand the number of Assessment teams we can field and to provide dedicated teams to support our Federal Government and CI customers, respectively. Figure 1 provides a quick snapshot of our FY 2016 activities.

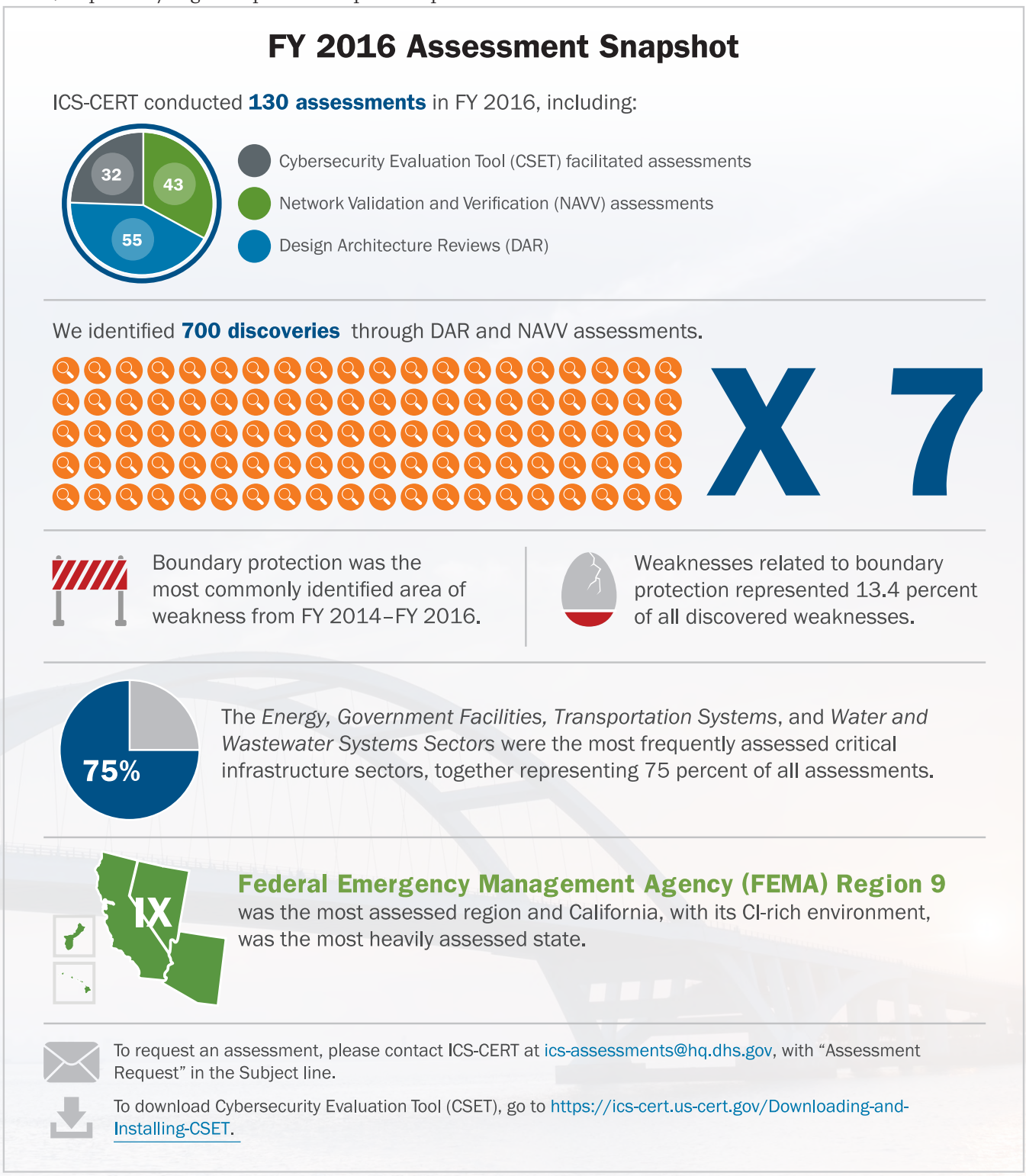

Figure 1: FY 2016 Assessment Snapshot

2.1 Overarching Discoveries

For the third consecutive year, ICS-CERT assessment teams found weaknesses related to boundary protection to be the most prevalent. Weaknesses related to the principal of least functionality were the second most commonly discovered issues, as was the case in FY 2015. Table 1 shows year-over-year comparisons of discovered weaknesses, in order of prevalence, from FY 2014-16. Of note, while least privilege and allocation of resources categories fell out of the top six weaknesses (they were fourth and fifth in FY 2015), in FY 2016 they were ranked seventh and eighth, respectively. These changes may be due to the year-over-year variances in the types of assets assessed rather than to shifts in the overarching ICS cybersecurity posture. Table 2 describes the potential consequences that may result from exploitation of these weaknesses.

FY 2014-2016 TOP SIX WEAKNESS CATEGORIES IN ORDER OF PREVALENCE		
FY 2014	**FY 2015**	**FY 2016**
1. Boundary Protection	1. Boundary Protection	1. Boundary Protection
2. Information Flow Enforcement	2. Least Functionality	2. Least Functionality
3. Remote Access	3. Authenticator Management	3. Identification and Authentication
4. Least Privilege	4. Identification and Authentication	4. Physical Access Control
5. Physical Access Control	5. Least Privilege	5. Audit Review, Analysis and Reporting
6. Security Function Isolation	6. Allocation of Resources	6. Authenticator Management

Table 1: FY 2014-2016 Top Six Weaknesses

FY 2016 MOST PREVALENT WEAKNESSES		
Area of Weakness	**Rank**	**Risk**
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Least Functionality	2	• Increased vectors for malicious party access to critical systems • Rogue internal access established
Identification and Authentication	3	• Lack of accountability and traceability for user actions if an account is compromised • Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
Physical Access Control	4	• Unauthorized physical access to field equipment and locations provides increased opportunity to ○ Maliciously modify, delete, or copy device programs and firmware ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Audit Review, Analysis and Reporting	5	• Without formalized review and validation of logs, unauthorized users, applications, or other unauthorized events may operate in the ICS network undetected detection
Authenticator Management	6	• Compromised unsecured password communications. • Password compromise could allow trusted unauthorized access to systems

Table 2: Risk Associated with FY2016 Most Prevalent Weaknesses

2.2 FY 2016 Assessment Coverage

The number of security assessments conducted in FY 2016 represents a 16 percent increase from FY 2015 and an increase of 25 percent from FY 2014. There were also changes to the mix of assessments conducted in FY 2016, with the number of facilitated CSET assessments declining — an ongoing trend since FY 2012 — as ICS-CERT's other assessment services evolve and customer demand for DAR and NAVV assessments increases.

Table 3 shows the number of facilitated assessments conducted by ICS-CERT since the program's inception in 2009. ICS-CERT began offering DAR and NAVV assessments in 2012.

ICS ASSESSMENTS BY FISCAL YEAR									
Assessment Type	**FY 2009**	**FY 2010**	**FY 2011**	**FY 2012**	**FY 2013**	**FY 2014**	**FY 2015**	**FY 2016**	**Total**
Facilitated Cybersecurity Assessment Tool (CSET)	20	57	81	83	60	49	38	32	420
Design Architecture Review(DAR)	NA	NA	NA	2	10	35	46	55	148
Network Architecture Validation and Verification (NAVV)	NA	NA	NA	4	2	20	28	43	97
Total	20	57	81	87	72	104	112	130	665

Table 3: Number of Assessments by Year and Type

ICS-CERT offers cybersecurity assessments of ICS to both government and private sector organizations across all 16 CI sectors. ICS-CERT conducts all private sector assessments in response to voluntary requests from CI owners and operators. As a result, year-to-year fluctuations in assessments for a given CI sector are generally demand driven (based on customer requests). However, ICS-CERT prioritizes scheduling of assessments using a variety of factors, including sector or facility risk profile, the reliance of the CI asset on control systems, and geographic clustering of CI to ensure the most effective and efficient use of existing resources (it is generally more efficient to conduct assessments on multiple facilities of geographic proximity to one another).

In FY 2016, ICS-CERT conducted assessments in 12 of the 16 CI sectors. These include the Chemical (7 assessments), Commercial Facilities (4), Communications (5), Critical Manufacturing (5), Dams (2), Emergency Services (3), Energy (22), Food and Agriculture (3), Government Facilities (10), Information Technology (3), Transportation Systems (10), and Water and Wastewater Systems (56). The Water and Wastewater Systems and Energy Sectors, which together represented 60 percent of all assessments, are both heavily dependent on control systems to manage operational processes. The Defense Industrial Base, Financial Services, Healthcare and Public Health, and Nuclear Reactors, Materials and Waste

WORKING TO SUPPORT REGIONAL CI RESILIENCE

In conjunction with DHS's Office of Infrastructure Protection and DHS Protective Security Advisors, ICS-CERT participates in the Regional Resiliency Assessment Program (RRAP).

RRAP is a cooperative assessment of specific CI within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues.

The RRAP program presents results from RRAP activities, research, and analysis in a Resiliency Assessment report with key findings that provide RRAP participants option for consideration for enhanced resilience. Facility owners and operators, regional organizations, and government agencies use the Resiliency Assessment and key findings to guide strategic investments in equipment, planning, training, and resources to enhance the resilience and protection of facilities, surrounding communities, and entire regions.

For more information, please send an e-mail to Resilience@hq.dhs.gov.

Sectors did not request assessments in FY 2016. Figure 2 compares assessments conducted in FY 2015 and FY 2016. The types of organizations for which ICS-CERT conducts assessments vary and include both small and large facilities with a range of cybersecurity resources and technical expertise. ICS-CERT anonymizes data collected during assessments for use in trend and other analyses.

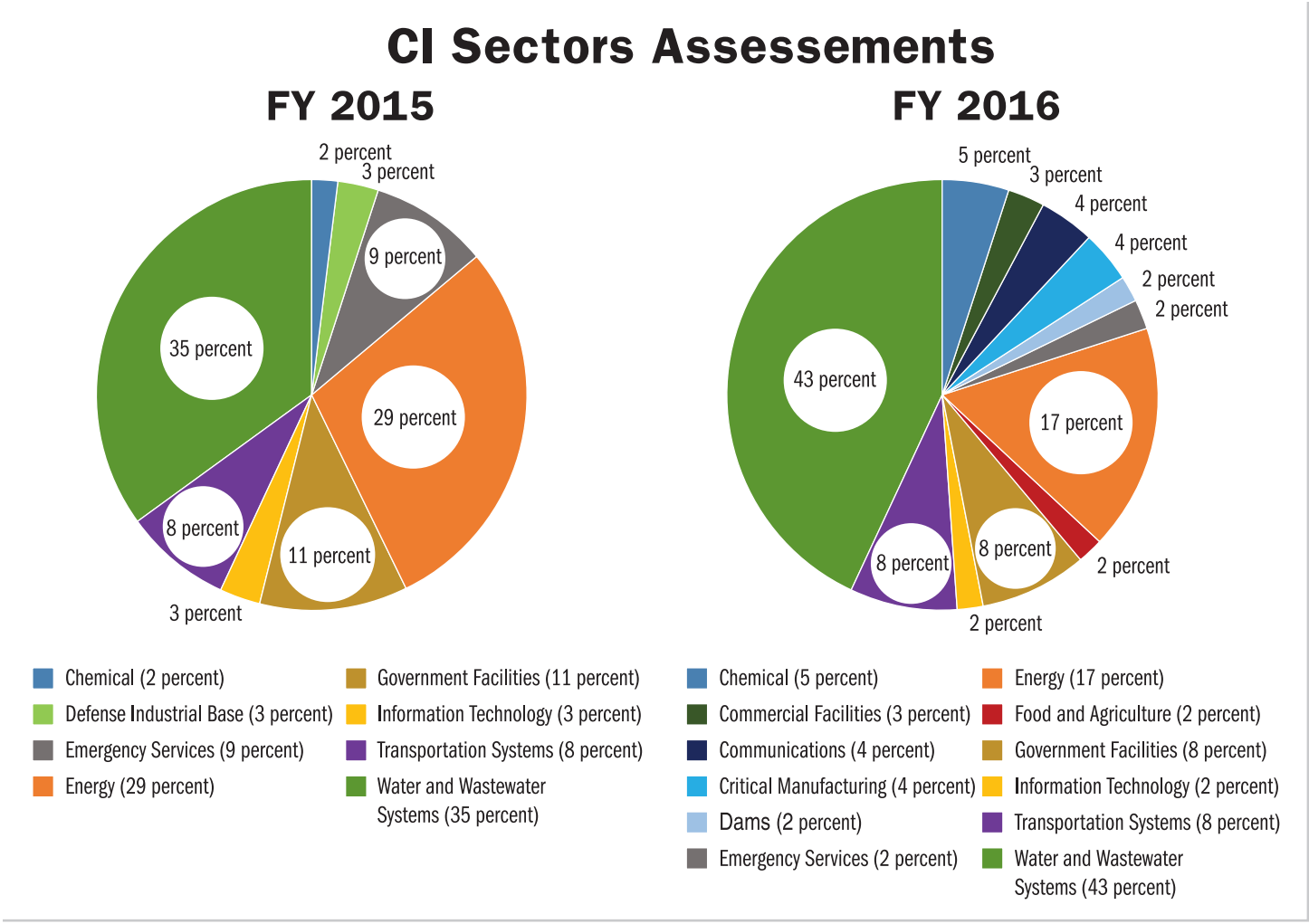

Figure 2: FY 2015 - 2016 Assessment Comparison by CI Sector

ICS-CERT conducted the majority of its assessments in FEMA Region 9, with California (25 assessments) and Arizona (18 assessments) accounting for the lion's share of assessments in that region. California, Arizona, and Texas (Region 6, 16 assessments) together accounted for 45 percent of all assessment locations. Figure 3 shows all assessments by state.

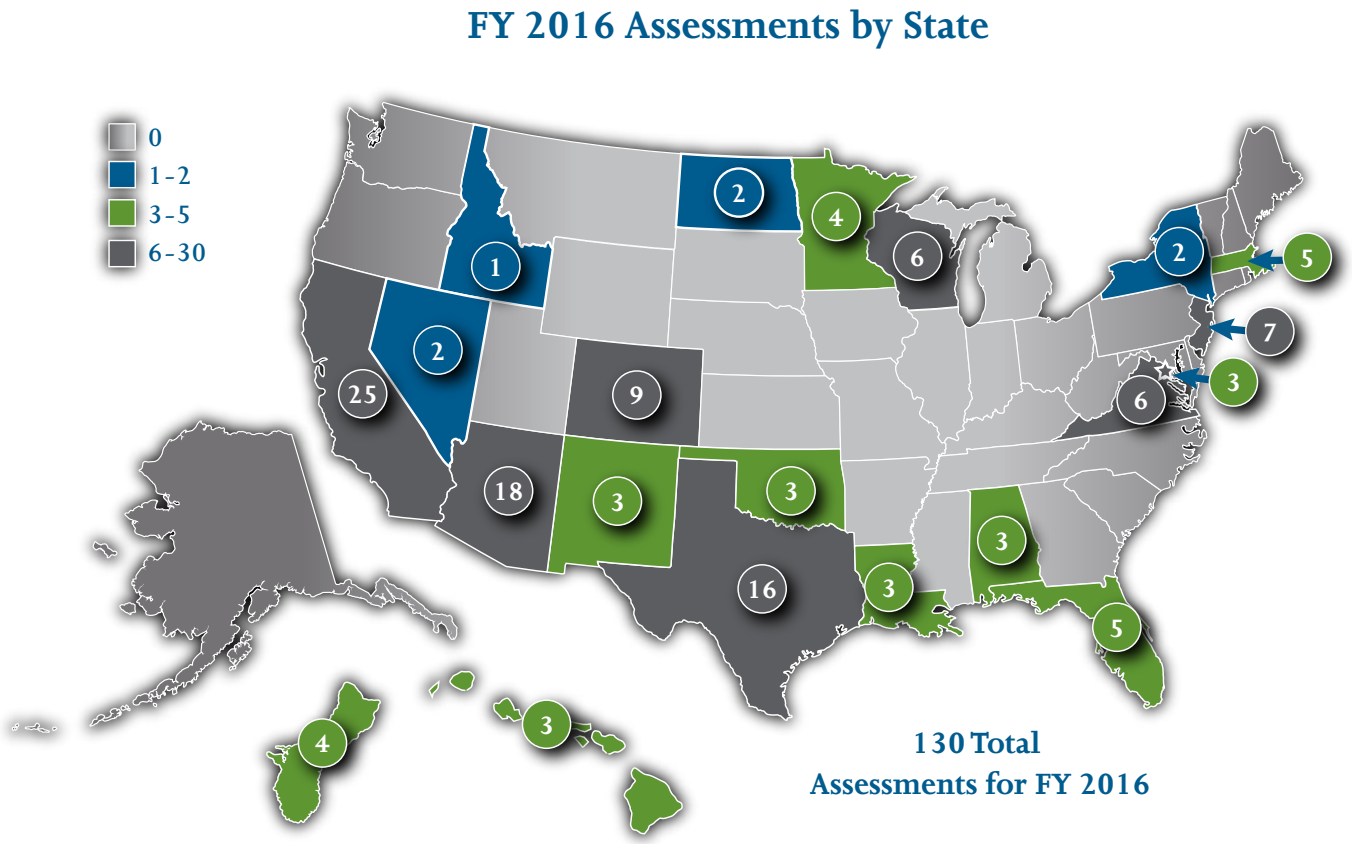

Figure 3: FY 2016 Assessment by State

3. Primary Discoveries and Mitigation Recommendations

This section describes specific discoveries and mitigation recommendations for the top six weaknesses ICS-CERT assessment teams found in FY 2016. It also provides a complete list of all weakness categories.

The recommendations provided in this section are consistent with best security practices for protecting control systems from threats of unauthorized use. In addition, to support overarching ICS security, ICS-CERT maintains a portfolio of guidance and best practices documents on its website (https://ics-cert.us-cert.gov/). These include, for example, ICS-CERT's *Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* and *Seven Steps to Effectively Defend Industrial Control Systems* reports. ICS-CERT encourages its partners to review these and other ICS-CERT information products. In its FY2015 *Industrial Control Systems Assessment Summary Report*, ICS-CERT also identified several overarching observations impacting ICS security. Summarized below, these observations remain pertinent in FY 2016.

A. Inadequate access security controls for virtual machines (VMs).

Inadequate user access security controls to the hypervisor (VM monitor) host management interface may provide a single point of failure and entry that adversaries could use to gain access to every guest VM on the host computer, allowing potential unauthorized access to any part of the ICS.

B. Insecure implementation of remote access.

Whether access is from the corporate network to the ICS or from the Internet to the ICS, this access may present 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 virtual private network (VPN) connection.

C. Improper use of Virtual Local Area Network (VLAN).

While VLANs can logically segment networks, if users do not follow best practices of the hardware vendors, unauthorized users can traverse to other VLAN segments. Default and native VLANs that remain unchanged on trunk ports provide an avenue to traverse from one VLAN to another.

D. Weak Bring-Your-Own-Device (BYOD) security policies for ICS.

Mobile and other devices are not typically managed by the organization and security policies implemented by the organization are often not implemented on the portable devices. Use of BYOD devices to access personal email, web pages, and social media applications, are inherently high risk to ICS.

E. Insufficient hardening of cloud services security and Service Level Agreements (SLAs) for critical ICS functions.

Organizations must ensure that the parts of any ICS architecture hosted externally maintain security levels consistent with the criticality of the ICS functions. Organizations should also ensure that SLAs are sufficient to maintain ICS operational functions associated with recovery, event/incident management, failover, forensic support, monitoring, and other operational functions that may require support by the cloud-hosting service provider.

F. Inadequate adoption of ICS Network Monitoring as a core Defense-in-Depth (DiD) strategy.

Network monitoring is an essential security measure for any critical system as an important part of the attacker life cycle is to establish a command and control presence in the system. An attacker will leverage this to receive system discovery information and determine how to best implement a customized attack toolkit to exploit system vulnerability and achieve attack goals. Most CI organizations have some level of monitoring at the corporate level, rarely within ICS networks.

Figure 4, on the following page, illustrates these potential network attack scenarios.

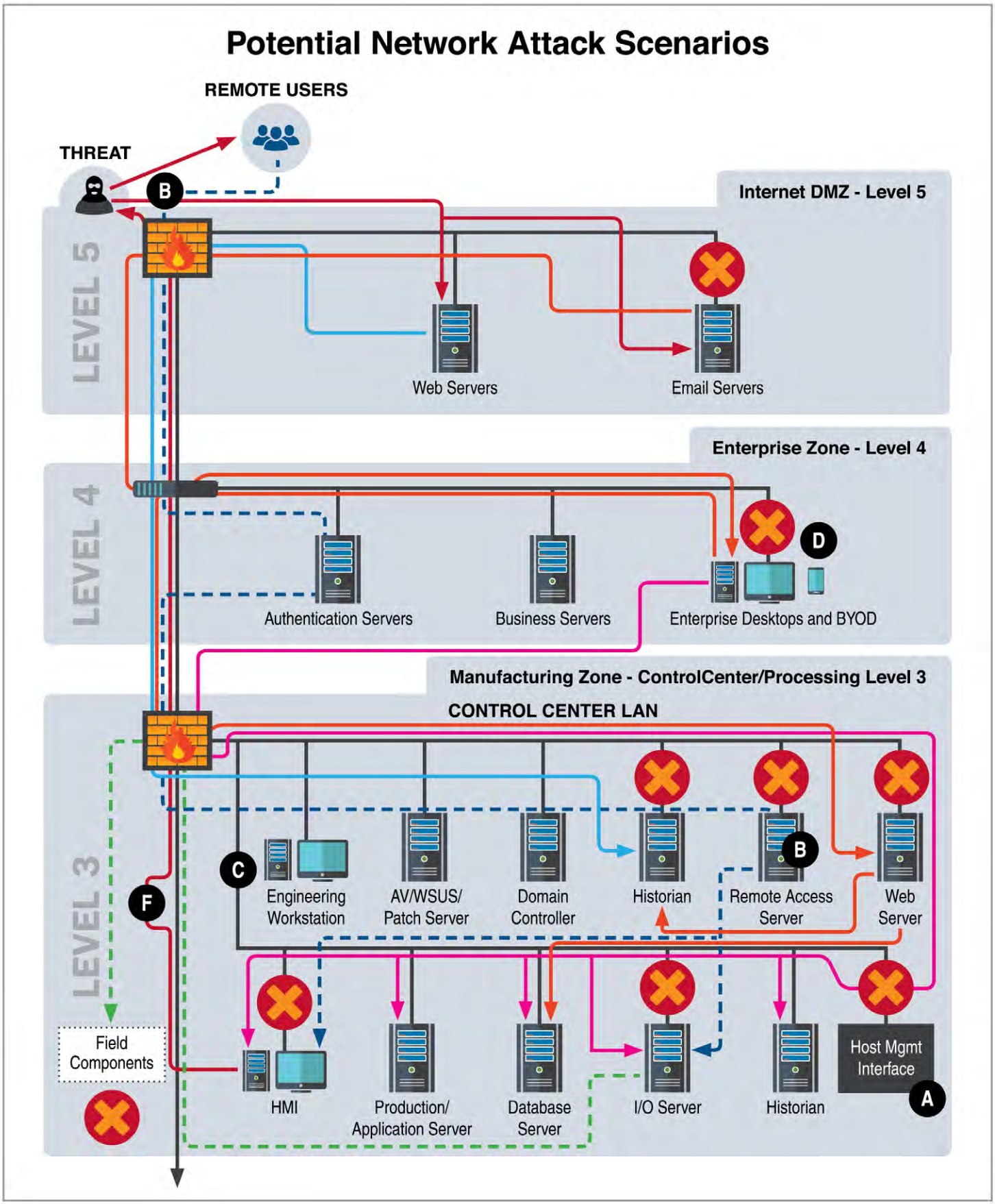

Figure 4: Potential Network Attack Scenarios

3.1 Detailed Discussion of Top Identified Vulnerabilities

While ICS-CERT assessments identified weaknesses across all control families, six categories represented roughly 36 percent of the total vulnerabilities discovered across assessed CI sectors. The top six categories were Boundary Protection; Least Functionality; Identification and Authentication; Physical Access Control; Audit Review, Analysis, and Reporting; and Authenticator Management. ICS-CERT's assessment methodology categorizes weaknesses based on the National Institute of Standards and Technology's (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," control family sub-categories (See Appendix A for Control Family descriptions). This section summarizes the six most common vulnerabilities by Security Control Family, subcategory, prevalence, potential risk, and recommended mitigations.

1. System and Communications Protection: Boundary Protection (SC-7) 94 DISCOVERIES		
Description	**Why is Boundary Protection Important?**	**Recommended Mitigation**
• 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.	• Inadequate boundary protections for the ICS network make it more difficult to detect unauthorized activity. Weak boundary protection provides various vectors for unauthorized interfacing with devices and systems that 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 such as the Internet).	• 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 ICS. • The DMZ should house a dedicated "jump" server that permits systems on the enterprise network (or those accessing via a remote method such as VPN) to access data elements derived from the ICS network. • Harden the jump server, running only essential services. Credentials for this server should not be the same as those used for authentication to systems on the enterprise network. • Restrict communication flows to this server to the minimal subset of those required to support secure methods for accessing ICS systems (when needed to access from outside the standard ICS network). • Incorporate logging and monitoring of information derived from this system with continued verification. • Security devices and systems need to be resident n 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) 42 DISCOVERIES		
Description	**Why is Least Functionality Important?**	**Recommended Mitigation**
• Controls associated with minimizing the computing resources of systems functions, ports, protocols, and services to only those required to support system essential operations.	• 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.	• 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: Identification and Authentication (IA-2) 36 DISCOVERIES		
Description	**Why is Identification and Authentication Important?**	**Recommended Mitigation**
• Controls implemented for the identification and authentication of authorized organizational users (or processes acting on behalf of organizational users).	• Without proper identification and authentication, there is lack of accountability for individual user actions. • Weak identification and authentication 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	• 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 integrate 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 and log books.

4. Physical and Environmental Protection: Physical Access Control (PE-3) 28 DISCOVERIES		
Description	**Why is Physical Access Control Important?**	**Recommended Mitigation**
• This control applies to organizational employees and visitors. Companies determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or system users. • Physical access devices include, for example, keys, locks, combinations, and card readers. • Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected systems equipment in secured areas.	• Unauthorized access to sensitive facilities could occur without challenge, during which time a malicious party may directly connect to the SCADA system and potentially set up a more permanent and remote connection for ongoing unauthorized access at a later time. • Keys allowing physical access may be out of the facilities' control, possibly allowing unauthorized personnel to access critical or sensitive areas.	• Follow through on processes to identify parties accessing remote facilities at all times. Treat all alarms as a serious breach until otherwise verified. • Develop, document, and enforce a key management policy. Investigate using an electronic key solution where feasible to limit the amount of physical keys that need tracked.

5. Audit and Accountability: Audit Review, Analysis, and Reporting (AU-6) 26 DISCOVERIES		
Description	**Why is Audit Review, Analysis, and Reporting Important?**	**Recommended Mitigation**
• Audit review, analysis, and reporting covers information security-related event data collection and analysis including, for example, monitoring of account usage, remote access, mobile device connection, configuration settings, and system component inventory. • Use findings for information security analysis and incident response.	• Without formalized review and validation of logs, unauthorized users, applications, or other unauthorized events may be present in the system and operate in the ICS network without detection.	• Determine events of interest (for example, privileged account creation, login attempt failures, and configuration changes) and implement a process that collects them and provides for performance of review, analysis, and response. • Implement a centralized log collection and analysis service (and a Security Information and Event Management tool). • By collecting all logs and events through a centralized service, analysts can save time and resources, improve efficiency, and be able discover anomalous activity at a system-wide level.

6. Identification and Authentication: Authenticator Management (AC-5) 24 DISCOVERIES		
Description	**Why is Authenticator Management Important?**	**Recommended Mitigation**
• Controls associated with the management of system authenticators. • Often ICS or operations control centers either don't support strong password management or operational implementation of individual passwords is not appropriate to the operating environment.	• 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 (that is, account passwords that never expire or inactive/ legacy accounts not disabled when not in use).	• 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 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 PKI certificate), and something a user is (that is, biometrics, such as a voice print).

3.2 All Weaknesses Discovered in FY 2016

In FY 2016, ICS-CERT identified 700 weaknesses through its 98 DAR and NAVV assessments. The top 30 categories of weaknesses, listed in Table 4 below, make up roughly 79 percent of all identified weaknesses.

TOP 30 IDENTIFIED WEAKNESSES IN FY 2016			
NIST 800-53 Weakness Categories	**Instances**	**Percentage**	**Order**
Boundary Protection	94	13.4%	1
Least Functionality	42	6.0%	2
Identification and Authentication (Organizational Users)	36	5.1%	3
Physical Access Control	28	4.0%	4
Audit Review, Analysis, and Reporting	26	3.7%	5
Authenticator Management	24	3.4%	6
Least Privilege	20	2.9%	7
Allocation of Resources	19	2.7%	8
Account Management	17	2.4%	9
Remote Access	16	2.3%	10
Security Awareness Training	16	2.3%	11
System Security Plan	15	2.1%	12
Flaw Remediation	15	2.1%	13
Information System Monitoring	15	2.1%	14
Security Impact Analysis	14	2.0%	15
Transmission Confidentiality and Integrity	13	1.9%	16
Baseline Configuration	12	1.7%	17
Contingency Plan	12	1.7%	18
Information System Backup	12	1.7%	19
Security Engineering Principles	12	1.7%	20
Information System Component Inventory	11	1.6%	21
Media Use	11	1.6%	22
Role-Based Security Training	10	1.4%	23
Configuration Change Control	10	1.4%	24
System Interconnections	9	1.3%	25
Configuration Settings	9	1.3%	26
Publicly Accessible Content	8	1.1%	27
Audit Events	8	1.1%	28
Incident Response Plan	8	1.1%	29
Protection of Information at Rest	8	1.1%	30
Total Discoveries Identified for Top 30 Weaknesses	550		
Total Discoveries Identified in FY2016	700		

Table 4: Top 30 Weaknesses in Order of Prevalence

4. ICS-CERT's Assessment Program

ICS-CERT launched the Assessment Program in 2009 with the goal of helping CI owners and operators understand and improve their control systems security posture. Initially focused on facilitated assessments using CSET — which provides a good initial security overview — in 2012, the assessment program expanded its offerings to include detailed, in-depth technical assessments through DAR and NAVV assessments.

4.1 Support Structure for Government and Private Sector Customers

In FY 2016, ICS-CERT established a dedicated federal facilities assessment team and a dedicated private sector assessment team. These teams provide support to their respective customers under an integrated management and data sharing structure that ensures anonymized and protected information gleaned from both federal and private sector assessments support analytical efforts to improve overarching control systems security.

4.1.1 ICS-CERT Private Sector Assessment Team

A core part of ICS-CERT's mission to reduce risk to the Nation's CI is to provide onsite cybersecurity assessments to CI asset owners and operators to strengthen their ICS cybersecurity posture. ICS-CERT bases assessments on standards, guidelines, and best practices, and are provided to CI asset owners and operators at no cost using our congressional funding. Our assessment methodologies provide a structured framework that asset owners and operators can use to assess, re-assess, protect, detect, and continually validate the cybersecurity of their ICS networks. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing their cybersecurity posture.

ICS-CERT's Private Sector Assessment team works with CI asset owners to determine which set of assessment services best fits the needs of that particular organization. The services provided may include a combination of a facilitated CSET, DAR, and/or NAVV assessments, depending on the current state and goals of the organization. Information shared with ICS-CERT can be protected under the auspices of the Protected Critical Infrastructure Information (PCII) Program.

4.1.2 Industrial Control Systems Federal Critical Infrastructure Assessment Team (ICSFCIA)

In FY 2016, ICS-CERT established the ICSFCIA to provide dedicated assessment support for federal partners. The ICSFCIA offers federal organizations a comprehensive suite of assessment services, including a research-based "state of security" evaluation that explores potentially risky open source information about a facility or system, a Maturity Level Evaluation (MLE) using CSET, identification of indicators of compromise, DAR and NAVV assessments, log analysis, and Operational Sustainability. Upon completion of all assessments, ICSFCIA will compile an in-depth report for the federal facility owner, which includes a prioritized analysis of key discoveries and practical mitigations for enhancing the cybersecurity posture of the organization.

Through this program, ICS-CERT also works closely with the NCCIC's NCATS team. NCATS conducts cybersecurity assessments on enterprise networks, with a focus on the Federal Government's most critical assets. ICS-CERT works with NCATS to provide ICS-specific assessments and technical expertise to improve ICS security for these assets.

4.2 Assessment Elements

In order to categorize assessment discoveries, ICS-CERT bases assessment and analysis of security vulnerabilities on NIST Special Publication 800-53. 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 works with sector stakeholders to provide additional tailoring to unique aspects of individual customers, as necessary. Appendix A shows the top-level NIST 800-53 Security Control Families.

ICS-CERT offers a combination of processes in support of an integrated assessment product suite. Assessment products and services include

- Cybersecurity Evaluation Tool (CSET)
- Design Architecture Review (DAR)
- Network Validation and Verification (NAVV)

ICS-CERT's cybersecurity assessment services include evaluation of ICS design architecture, verification and validation of network traffic, and systems log review and analysis. An evaluation of the design architecture includes a high level preliminary evaluation of the site security posture, leveraging CSET, followed by an in-depth review and evaluation of the ICS network design, configuration, and inter-connectivity to internal and external systems. This system analysis provides ICS asset owners with a comprehensive cybersecurity evaluation focusing on defensive strategies associated with their specific control systems network.

Network data traffic analysis provides asset owners with information to identify anomalous and potentially suspicious communications sourced from, or destined for, control systems assets. This service offering provides a sophisticated analysis of the asset owner's network traffic, which asset owners collect, from within their control system network environment. ICS-CERT subject matter experts (SME) analyze the captured network traffic using a combination of open source and commercially available tools to develop a detailed representation of the communications, flows, and relationships between devices.

4.2.1 Cyber Security Evaluation Tool

DHS developed CSET to enable CI owners and operators to conduct a basic evaluation of their ICS cybersecurity posture based on standards and practices best suited to their sector.

CI customers can use CSET to support both self-assessments as well as ICS-CERT facilitated assessments, undertaken in conjunction with DAR and NAVV assessments. CSET is available as a no-cost download. CSET maps user input to questions associated with selected cybersecurity standards and best practices. To maximize the effectiveness of the CSET evaluation process, the asset owner should include SMEs 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. In FY 2016, ICS-CERT released CSET Version 8.0, which added a number of new features to the tool, including a simplified user interface, five new standards, specialized question sets, and new component additions to the network diagram function.

4.2.2 Design Architecture Review

A DAR is an assessment process facilitated by ICS-CERT assessment personnel. ICS-CERT works with system owners and operators to perform a thorough manual assessment and analysis of the operational process. ICS-CERT focuses on assessing the security of the underlying control system architecture, the integration of Information Technology (IT) and Operational Technology (OT), vendor support, network monitoring, cybersecurity controls, and a review of internal and external connections used within the control systems environment. The process focuses heavily on ICS Network Architecture, Asset Inventory, and Protective and Detective Security controls.

This review provides asset owners with a thorough evaluation of system interdependencies, vulnerabilities, and mitigation options. ICS-CERT 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.

4.2.3 Network Architecture Validation and Verification

The NAVV assessment process entails the analysis of (passively captured) traffic within the ICS network. Using a combination of open-source and commercially available tools, ICS-CERT visualizes and performs analysis on the network traffic and device-to- device communications occurring within various ICS network segments to identify potentially unauthorized or suspect communications. Threat data analysis of the traffic evaluates indicators of known unauthorized attacks in the user's network.

This assessment enables asset owners to

- Verify the accuracy of ICS network diagrams;
- Identify rogue or 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); and
- Gain practical knowledge of how to passively monitor and verify the communications occurring within their ICS networks.

The process provides organizations with a comprehensive 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 this review as a part of the overall assessment service, however they also offer it independently.

4.3 The Assessment Process: What to Expect

ICS-CERT schedules and conducts assessments based on available resources. The integrated assessment process typically contains several phases. A baseline evaluation begins the assessment using CSET, followed by DAR and NAVV assessments. While assessments could be performed at any of the levels individually (CSET, DAR, or NAVV), the process is most effective when all three elements are performed together. Figure 5 describes ICS-CERT's assessment process.

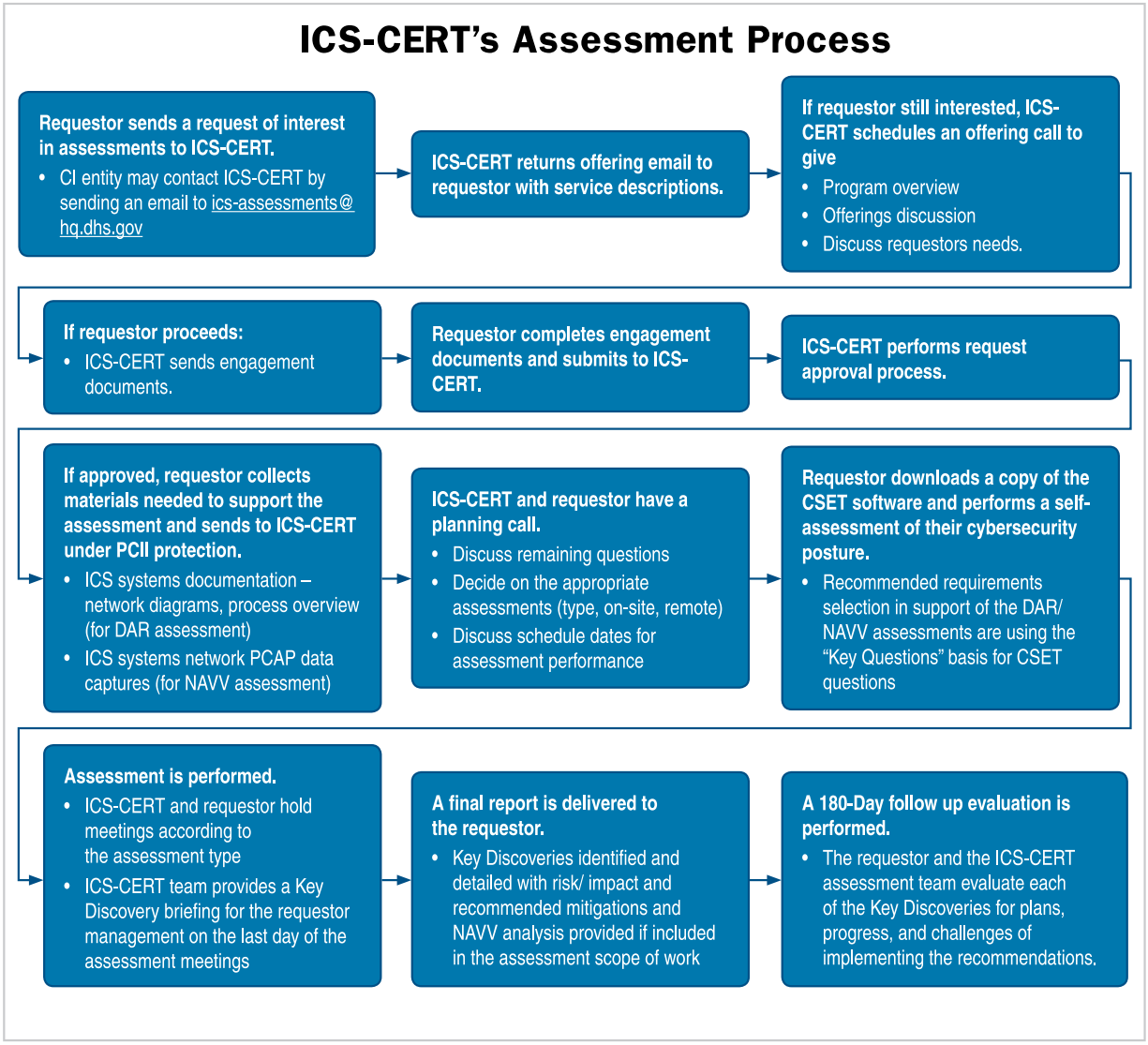

Figure 5: ICS-CERT's Assessment Process

4.3.1 Preparing for the Assessment

The ICS-CERT assessment team makes every effort to accommodate the needs and special circumstances of the organizations with which it is working. Before scheduling an assessment, ICS-CERT must receive all pre-engagement paperwork. Organizations should complete general pre-assessment documentation (that is, Request for Technical Assistance, Logistics Form Request, and PCII Express Statement) and, following approval of those, network diagrams, network header data, and inventory lists to review and discuss prior to scheduling the assessment.

Typical assessments take three to four days to complete, depending on the number and size of the systems assessed. Organizations should invite any personnel who are familiar with or influence their site's security policies, control system architecture, topologies, and protocols to attend the assessment. These include control systems operators/engineers, information technology personnel, policy and management personnel, and SMEs. ICS-CERT's assessment team does not connect to customers' networks. The team will work from the information provided prior to the assessment, which it will evaluate prior to visiting with the facility.

Upon completion of the assessment process, ICS-CERT compiles an in-depth report for the asset owner, including a prioritized analysis of key discoveries and practical mitigations for enhancing the organization's cybersecurity posture. ICS-CERT also captures post-assessment feedback through a questionnaire and follow-up discussion 180 days after the assessment. The feedback helps ICS-CERT improve its assessment offerings, gather information about the value of ICS-CERT's recommendations, and understand the degree to which the asset owner's cybersecurity posture improved after the assessment.

5. A Look Ahead to FY 2017

In FY 2017, ICS-CERT is launching a number of important initiatives to improve its assessment products, services, and capabilities.

Our Private Sector Assessment team is transitioning the services it provides to CI customers from discrete CSET, DAR, and NAVV assessments to an integrated process that includes all assessment offerings along with advanced analytics that provide actionable feedback to asset owners. This integrated process will include a baseline assessment performed using CSET, followed by a deep-dive design architecture review of the ICS, communications, and networking architecture, and analysis of the network data communications. In FY 2017, the ICS-CERT Assessment Program will also add log analysis to its assessment services. Log analysis can rapidly identify issues such as misconfigured equipment and communications links and, more importantly, system intrusions. Asset owners submit useful system or event logs, which provide a sampling of the central control system elements, such as an ICS server, a Historian/Database collector, or a remotely connected human-machine interface (HMI) system.

Successfully piloted in FY 2016, this integrated assessment process found abnormal network traffic, which indicated a potential system breach during several onsite assessments. On such occasions, the ICS-CERT assessment team coordinated with the asset owner and contacted the NCCIC's incident response team to provide additional assistance through the mitigation process.

ICS-CERT will also expand the scope and number of assessment services it provides federal facility partners through its newly established ICSFCIA program. ICSFCIA focuses on identifying the health of the control systems within the Federal Government against advance persistent threats. These assessments provide federal partners with in-depth security evaluations, information on attack paths, indicators of compromise, and mitigation techniques to secure ICS environments. ICS-CERT is also adding an operational sustainability capability to help review and maintain prepared, resilient, and secure federal ICS.

Through the ICSFCIA program, ICS-CERT will also be a primary contributor to a comprehensive and coordinated interagency effort to secure building and access control systems for more than 9,000 facilities in the federal portfolio. In close partnership with the General Services Administration, Federal Protective Service, and the Interagency Security Committee, ICS-CERT is providing assessment services for the highest-risk federal facilities, technical expertise, and training resources to support this important interagency effort. ICS-CERT will also support and participate in developing the standards utilized by federal facilities for assessing cyber risk to control systems (for example, Interagency Security Committee standards).

6. Conclusion

ICS-CERT looks forward to continuing to support its private sector and government partners in securing their control systems. Leveraging the insights gained through our assessment data and customer feedback in FY 2016, we will build upon and enhance the capabilities and technical expertise we added to our assessment program for FY 2017. This includes ongoing maturation of the ICSFCIA program for our federal partners, continued evolution of our private sector assessments from individual offerings into a more comprehensive assessment process that includes log analysis, and building additional features into CSET to best meet our customers' needs. We will also continue to coordinate closely with other federal agencies, providing their constituents with access to ICS-CERT assessment and other cybersecurity offerings. ICS-CERT thanks its partners for the opportunity to support them and for their continued commitment to control systems security.

Appendix A. NIST 800-53 Cybersecurity Control Families

NIST 800-53 Security Control Family Descriptions

ICS-CERT uses NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," 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 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 (for example, 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 (for example, temperature, and emergency provisions (for example, shutdown, power, lighting, and fire protection). and emergency provisions (for example, 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.

Contact ICS-CERT

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

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

International: (208) 526-0900

Email: ics-cert@hq.dhs.gov

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

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

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

Contact NCCIC

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

NCCIC Service Desk and Customer Service

Phone: (888) 282-0870

Email: NCCICCustomerService@hq.dhs.gov

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

Phone: (703) 235-5273

Email: NCCIC@hq.dhs.gov

NCCIC