Industrial Control Systems Assessments FY 2014 Overview and Analysis

Industrial Control Systems Cyber Emergency Response Team

Homeland Security

CONTENTS

FIGURES

TABLES

1. INTRODUCTION

1.1 Purpose and Scope

This report provides an overview and summary analysis of on-site assessments conducted by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in Fiscal Year 2014.

ICS-CERT is a component of the National Cybersecurity and Communications Integration Center (NCCIC), a division with the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C).

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

As a core part of its mission, ICS-CERT offers a range of cybersecurity assessment products and services at no cost to critical infrastructure owners and operators. Through a comprehensive voluntary public-private partnership, ICS-CERT works with critical infrastructure owners and operators, industrial control systems vendors, integrators, Sector-Specific Agencies, other Federal departments and agencies, State, Local, Tribal, Territorial (SLTT) governments, international partners, and others to assess various aspects of critical infrastructure pertinent to the control systems risk environment. Cybersecurity assessments help DHS and public and private sector stakeholders to understand ICS risks and implement policies, standards, and actions to mitigate that risk. This report contains the following core elements:

- An overview of ICS-CERT's Assessment Program, including a description of the assessment products and services ICS-CERT provides.
- Quantitative and qualitative summaries of assessment types, geographic location, and critical infrastructure sectors assessed in FY 2014.
- Assessment findings for FY 2014, including common ICS vulnerabilities and cybersecurity weaknesses.
- Guidance to assist critical infrastructure owners and operators in reducing cyber risk and enhancing industrial control systems security.
- Information for stakeholders interested in requesting an assessment and learning more about ICS-CERT and its programs.

1.2 Background

DHS established the Control Systems Security Program (CSSP) in 2003 to help secure the Nation's critical infrastructure against cybersecurity threats to industrial control systems. In 2012, ICS-CERT replaced the CSSP as part of a functional realignment of CS&C. ICS-CERT works through voluntary partnerships with a broad range of government, private-sector, and other stakeholders to provide a range of products, services, and capabilities that improve national capacity to detect, analyze, and mitigate cybersecurity threats and vulnerabilities to industrial control systems and to better respond to cybersecurity incidents.

The United States depends on critical infrastructure (CI)[1] to support national defense, public health and safety, economic vitality, and overarching societal well-being. Disruptions or significant damage to CI could result in potentially catastrophic and cascading consequences to the Nation.

Although CI sectors differ greatly, many share a common characteristic: a dependence on ICS for process automation and safety. Common ICS examples include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Process Control Systems (PCS). These systems control, monitor, and manage vital functions that support critical infrastructure, such as subway systems, dams, water treatment facilities, energy pipelines, chemical manufacturing plants, nuclear power plants, electric power generators, and telecommunications networks.

Traditionally, most control systems were purpose-built, stand-alone systems. Over time, however, the convergence of physical and cyber business processes and systems led to the integration of control systems networks with corporate enterprise networks as well as wireless, mobile, and cloud-based applications that support remote access and other capabilities. While improving efficiency and functionality, this integration also creates the potential for malicious cyber exploitation of what were traditionally stand-alone proprietary systems.

A successful cyber-attack on a control system could result in significant physical damage, loss of life, and cascading effects that could disrupt or destroy critical infrastructure at a local, regional, and even national level. In addition, significant cyberattacks could also undermine public confidence in the safety, security, and reliability of critical infrastructure.

[1] Critical infrastructure is defined as "… systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Presidential Policy Directive-21: Critical Infrastructure Security and Resilience identifies 16 critical infrastructure sectors: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

1.3 ICS-CERT's Assessment Program

The first step in protecting industrial control systems from harm is to understand the cybersecurity threats, vulnerabilities, and overarching cyber risk that critical infrastructure stakeholders face. DHS formally developed its control systems assessment program in 2009 to help CI asset owners and operators identify potential weaknesses in their ICS networks and to provide guidance for hardening those systems against cyber threats. ICS-CERT works with CI partners to review, verify, and provide recommendations for enhancing the protective and detective controls, policies, and procedural elements of their cybersecurity framework. ICS-CERT offers cybersecurity assessments of industrial control systems for companies, entities, and asset owner-operators across all 16 critical infrastructure sectors.

ICS-CERT assessments help critical infrastructure owners and operators do the following:

- Identify potential weaknesses or gaps within their ICS network.
- Understand cybersecurity threats and vulnerabilities.
- Establish a baseline security posture.
- Pursue risk mitigation options, as appropriate.

Requesting a Cybersecurity Assessment

ICS-CERT assessments are available at no cost to critical infrastructure asset owners and operators.

Following completion of DAR and NAVV assessments, ICS-CERT compiles an in-depth report for the asset owner, including analysis of key discoveries and practical mitigation options for enhancing ICS cyber security.

Information shared with ICS-CERT can be protected by DHS as Protected Critical Infrastructure Information (PCII).

To schedule an assessment, please contact ICS-CERT at icsassessments@hq.dhs.gov.

To learn more about ICS-CERT and its programs, go to: https://ics-cert.us-cert.gov/

2. ICS-CERT ONSITE ASSESSMENTS: OVERVIEW

ICS-CERT offers both self-assessment and facilitated onsite assessment products and services at no cost to CI owners and operators. ICS-CERT provides three primary assessment services:

- Cybersecurity Evaluation using the Cyber Security Evaluation Tool (CSET®).
- Design Architecture Review (DAR).
- Network Architecture Validation and Verification (NAVV).

ICS-CERT performs onsite assessments at the request of critical infrastructure asset owners and other entities. ICS-CERT tailors service offerings to the needs, size, and sophistication of asset owners. The types of organizations for which ICS-CERT conducts assessments vary greatly, ranging from small entities that have never completed an evaluation and review of their control system operations (from a cybersecurity perspective) to larger entities subject to strong regulation. ICS-CERT aligns its service offerings to asset owner requirements (e.g., level of detail and depth of evaluation the asset owner requests) as well as factors such as the risk profile of the organization, the current threat landscape, and known adversarial activity against specific entities or sectors.

2.1 ICS-CERT Assessment Types

ICS-CERT uses the National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems* (NIST 800-53) as a structured method to group and analyze vulnerabilities discovered during assessments. The 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. Data collected during these assessments is used for reporting and trending, and helps ICS-CERT to continually refine its assessment services. Appendix A, "NIST 800-53 Security Control Family Descriptions" lists NIST 800-53 control categories.

NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*,[2] implements an industrial control systems overlay to NIST 800-53, tailoring security guidance to the unique operational and system characteristics of industrial control systems. While NIST 800-82 applies generally to all critical infrastructure sector control systems, ICS-CERT can work with sector stakeholders to provide additional tailoring to unique aspects of the individual sectors, as necessary.

[2] Special publication 800-82, Revision 2 (Draft) *Guide to Industrial Control Systems (ICS) Security* is a document revision out for public comment at the time of this report, however, the guidance is being actively utilized and evaluated by the ICS-CERT Site Assessment team.

2.2 Cyber Security Evaluation Tool Assessments

ICS-CERT developed and maintains CSET, a software tool used to conduct cybersecurity assessments. DHS developed CSET to provide a snapshot of an organization's cybersecurity posture. CSET maps evaluation outputs to cybersecurity standards and best practices[3]. In FY 2014, ICS-CERT conducted 48 facilitated CSET assessments in partnership with various critical infrastructure stakeholders, as shown in Figure 1.

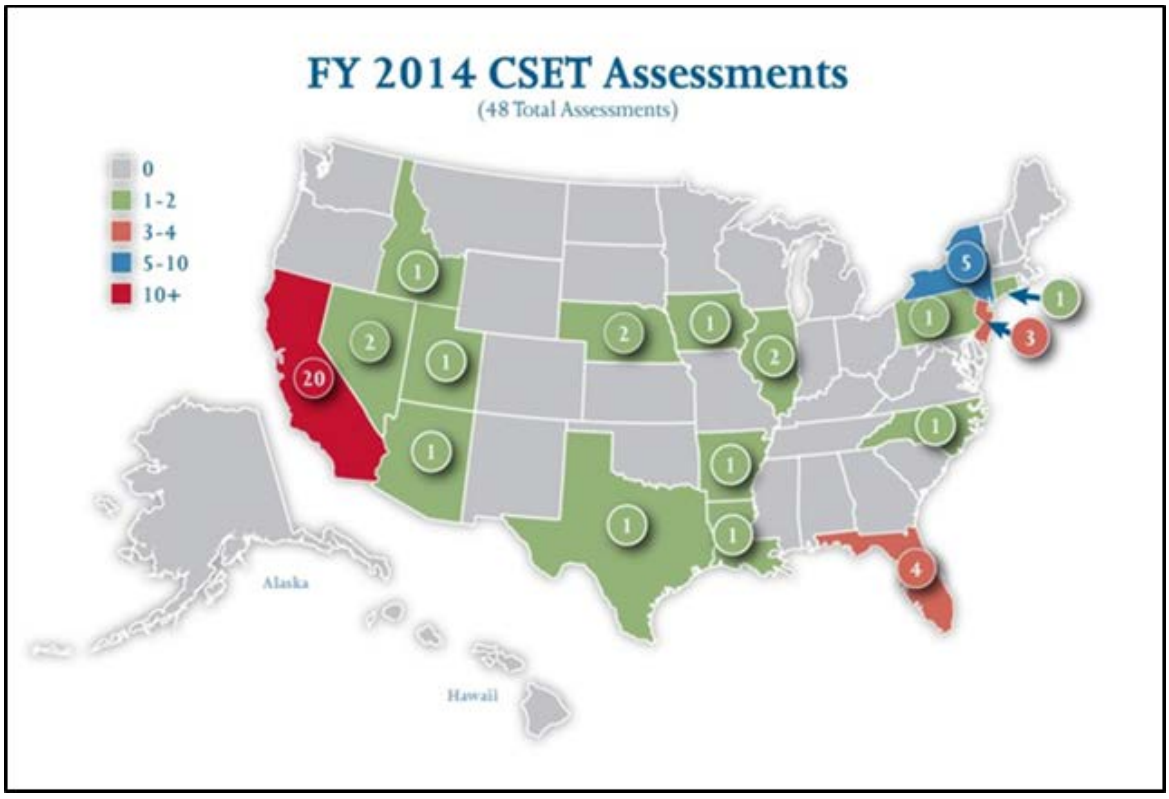

Figure 1. FY 2014 CSET Assessments by State.

Using CSET software, ICS-CERT provides on-site facilitated cybersecurity assessments as the introductory assessment within ICS-CERT's portfolio, but they are not a prerequisite for more in-depth assessments. CSET assessments typically take one day to complete (per control system architecture). While CSET is also available to asset owners as a downloadable self-assessment tool that can be used without the assistance of ICS-CERT, the onsite facilitated assessment provides a learning opportunity for asset owners to understand how to most effectively use the tool on a repeatable and continuous basis.

Figure 2 shows the high-level process that CSET assessments follow. The asset owner works with the ICS-CERT assessment team to conduct a discovery-oriented evaluation of the entity's underlying control processes, procedures, policies, methodologies, and protective and detective security controls. These compose the cybersecurity foundation for ensuring the availability and integrity of the control process.

[3]For example, NIST 800 SP82, NIST 800 SP53, Chemical Facility Anti-Terrorism Standards, Nuclear Regulatory Commission and the Critical Infrastructure Protection Subcommittee.

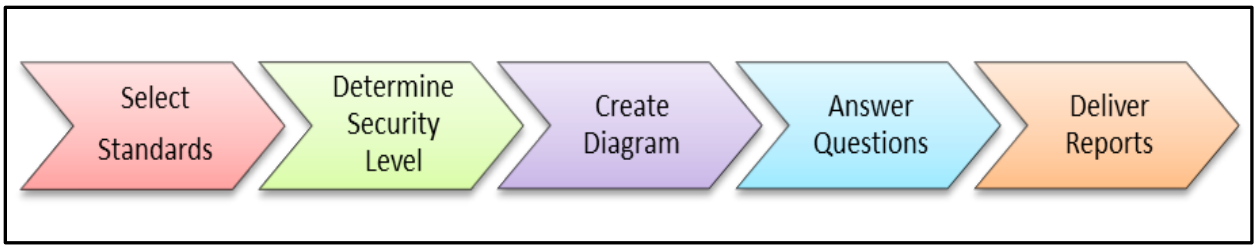

Figure 2. CSET Assessment High-Level Process.

2.3 Design Architecture Review

A Design Architecture Review (DAR) entails a deep-dive assessment and analysis of the operational process, focusing on the underlying ICS network architecture, integration of Information Technology (IT) and Operational Technology (OT) teams, vendor support, monitoring, cyber security controls, and a review of all internal and external connections utilized within the control systems environment. The DAR focuses heavily on three key areas:

- ICS Network Architecture.
- Asset Inventory.
- Protective and Detective Security controls.

This type of assessment generally takes two days to complete (per control system architecture). ICS-CERT can conduct DARs independently of or in conjunction with CSET assessments. A DAR includes a comprehensive evaluation and discovery process, focusing on defense-in-depth strategies associated with an asset owner's specific control systems network. 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.

DAR and NAVV Evaluation Benchmarks

ICS-CERT uses the National Institute of Standards and Technology's *Recommended Security Controls for Federal Information Systems* (NIST 800-53) as a structured method to group and analyze vulnerabilities found during DAR and NAVV assessments.

The 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. Data collected during these assessments is used for reporting and trending, and helps ICS-CERT to continually refine its assessment services.

2.4 Network Architecture Validation and Verification

The Network Architecture Validation and Verification (NAVV) assessment entails the analysis of network traffic (passively captured) occurring within the ICS network. Using a combination of both open-source and commercially available tools, ICS-CERT is able to strategically visualize and present the network traffic and device-to-device communications occurring within various ICS network segments.

The tools ICS-CERT utilizes also include relevant threat data and indicators, for which collected network traffic can be reviewed and verified. NAVV assessments enable asset owners to do the following:

- Verify the accuracy of ICS network diagrams.
- Identify potentially rogue/misconfigured devices or malicious data communications.
- Analyze data flows to ensure that 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 an accurate and 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 NAVV reviews as an extension to DARs, although this service is also offered independently. In FY 2014, ICS-CERT conducted 56 DAR and NAVV assessments, as shown in Figure 3.

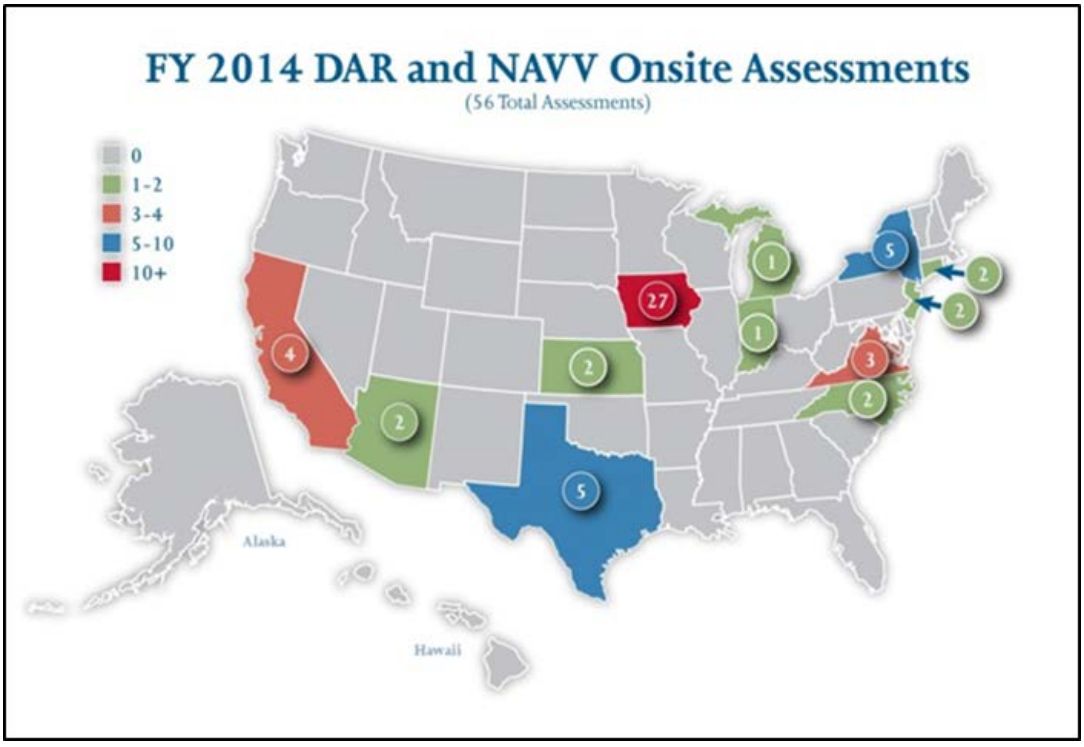

Figure 3. FY 2014 DAR and NAVV Assessments by State.

3. FY 2014 ASSESSMENT PROGRAM ACTIVITY & FINDINGS

At the request of its partners, ICS-CERT performed a total of 104 assessments in FY 2014, as shown in Figure 4. ICS-CERT's stakeholders drive the demand for cybersecurity assessments.

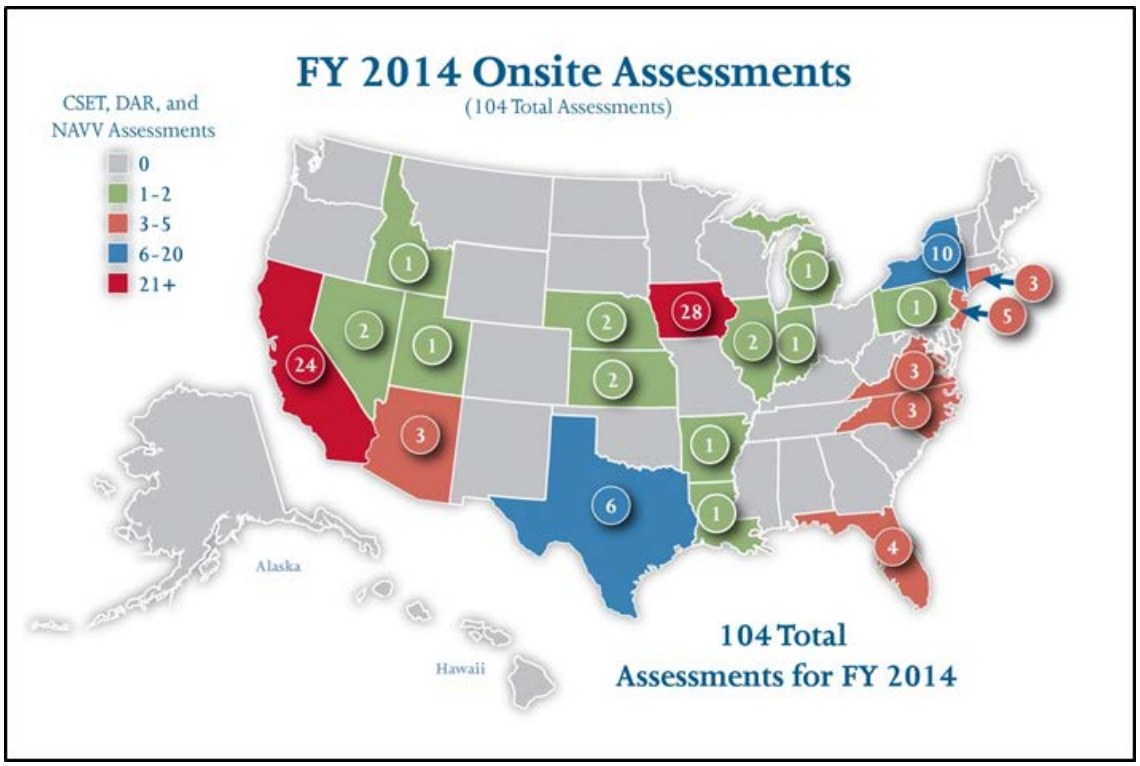

Figure 4. FY 2014 Total Assessments by State.

ICS-CERT's partners participate in ICS cybersecurity assessments on a voluntary basis, and stakeholder requests—along with factors such as sector risk profile, specific threat information, the dependence of specific critical infrastructure sectors on control systems, etc.—focus ICS-CERT's assessment activity. For example, in FY14, ICS-CERT and the Federal Energy Regulatory Commission's (FERC) Office of Energy Infrastructure Security (OEIS)[4] introduced a new technical assessment service offering. This offering provided select Energy Sector asset owners and operators with proactive and customized cyber security assessment services based upon their specific interest and areas of focus. As part of that engagement, various Energy Sector entities requested multiple assessment services, resulting in a comparatively high number of assessments conducted for that sector in 2014. The number of assessments in any given sector will fluctuate from year to year, based on the current threat landscape and other factors. Figure 5, on the next page, provides a percentage breakout of FY 2014 DAR and NAVV assessments by critical infrastructure sector.

[4] FERC OEIS is non-regulatory and its mission does not include compliance or enforcement actions.

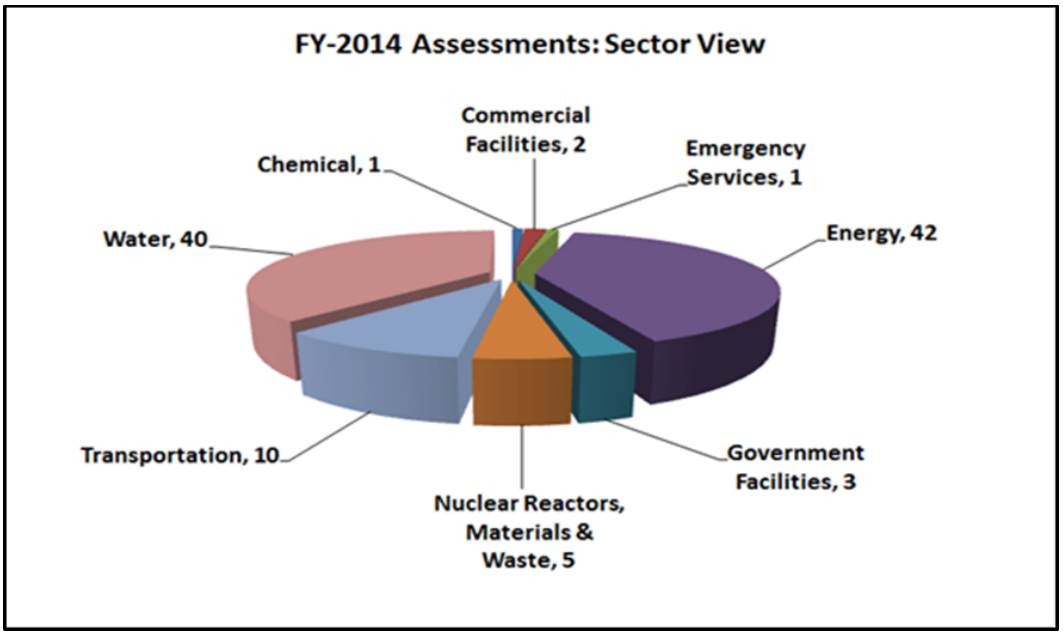

Figure 5. Number of FY 2014 DAR and NAVV Assessments Conducted by CI Sector.

DAR and NAVV assessments form the basis for identifying common vulnerabilities as they offer the most comprehensive evaluation of an organization's cybersecurity posture. In addition, ICS-CERT does not collect or retain data from CSET assessments (asset owners alone retain this data). DAR and NAVV assessments use NIST 800-53 security control families (see Appendix A, "NIST 800-53 Security Control Family Descriptions") as the evaluation benchmark. Table 1 lists the top-level NIST 800-53 Security Control Families; each control family also contains sub-categories.[5]

Table 1. NIST 800-53 Security Control Families.

NIST 800-53 Security Control Families			
ID	Security Control Family	**ID**	Security Control Family
AC	Access Control	**MP**	Media Protection
AT	Awareness and Training	**PE**	Physical and Environmental Protection
AU	Audit and Accountability	**PL**	Planning
CA	Security Assessment and Authorization	**PM**	Program Management
CM	Configuration Management	**PS**	Personnel Security
CP	Contingency Planning	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SC**	System and Communications Protection
MA	Maintenance	**SI**	System and Information Integrity

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

In FY 2014, ICS-CERT conducted 56 DAR and NAVV assessments (35 DARs and 21 NAVVs) in multiple critical infrastructure sectors. While ICS-CERT's assessments identified weaknesses across all control families, Table 2 shows that six vulnerabilities were most prevalent, representing approximately 28% of the total vulnerabilities discovered across assessed critical infrastructure sectors. Figure 6 shows the distribution of discovered vulnerabilities, mapped to sub-categories within NIST 800-53 Security Control Families.

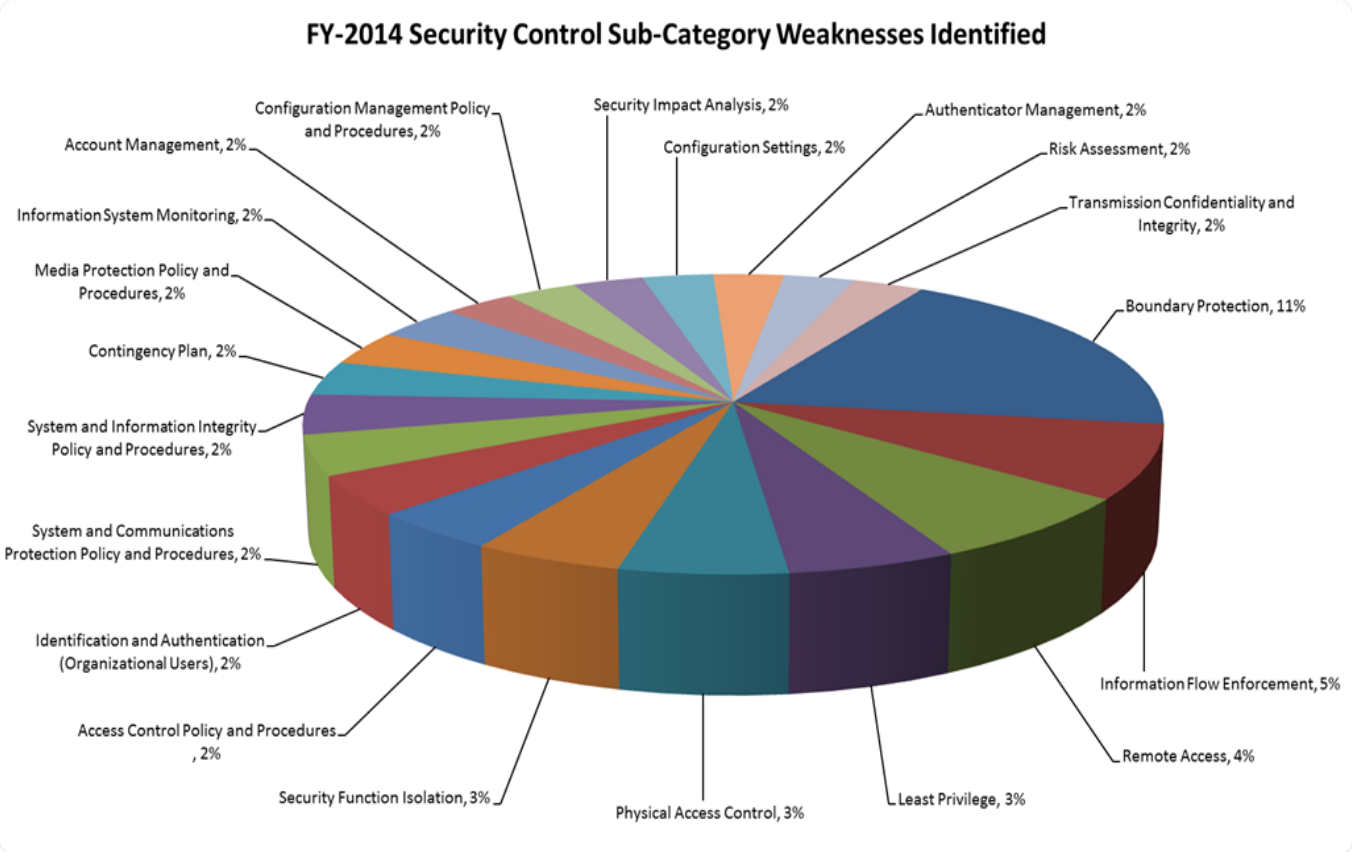

Figure 6. Identified Weaknesses by Security Control Family Sub-Category

ICS-CERT assessments most frequently found Boundary Protection, Information Flow Enforcement, and Remote Access vulnerabilities. Table 2, below, summarizes the six most common vulnerabilities by Security Control Family, sub-category weakness, and potential risk. Section 4 describes recommended mitigation activities and best practices for each of these common vulnerabilities.

Table 2. FY 2014 Common Vulnerabilities and Associated Risk.

FY 2014 DAR/NAVV: Common Vulnerabilities		
NIST 800-53 Security Control Family	**Sub-Category Assessment Discovery**	**Risk**
System and Communications Protection (SC)	Boundary Protection	• Without adequate boundary protections for the ICS network, it becomes very difficult to detect potentially malicious or nefarious activity. In addition, the lack of boundary protection provides various vectors for 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 a traditional enterprise network (or from untrusted systems like the internet).
Access Control (AC)	Information Flow Enforcement	• Without a comprehensive understanding and visibility of network traffic both within the ICS network and traffic sourced and/or destined to/from the ICS network, potential nefarious or malicious communications will likely go unnoticed, until an incident occurs. • Adversaries establish unauthorized or malicious data communications through the use of available ports, services, and communications channels (conduits). It is critical for asset owners to consider detection and monitoring capabilities for activity occurring within the ICS network in addition to enforcing robust user authentication protocols, strong password protection on ICS devices, and oversight for restricting the usage of non-dedicated mobile devices for interfacing with the ICS (e.g., laptops utilized on corporate or internet-accessible network segments).
Access Control (AC)	Remote Access	• Remote access is a common attack vector for interfacing with control systems. Weak remote access security controls introduce many avenues for interfacing with critical components and control system devices – possibly undetected by an organization. • Attack vectors can include internet facing devices, third party vendors or contractors whom have a direct connection to the ICS, weak virtual private network (VPN) configurations, the use of personal computing devices, and the exploitation of vulnerable Operating System services and configurations.
Access Control (AC)	Least Privilege	• An attacker or malicious insider can leverage user and computer accounts in trusted domains (or network segments) to potentially interface with the ICS. • Assigning elevated or enhanced privileges to personnel (above and beyond what they may require for their daily job functions) introduces many risks, and provides a means for either intentional (malicious insider/outsider) or unintentional (accidental) consequences. • Personnel utilizing elevated privileges and administrative accounts for daily job functions increases risk, which could ultimately impact operations. Common vulnerabilities associated with allowing unnecessary privileges include the installation of unapproved or untested software, the successful execution of malware or a malicious application on a critical asset, disabling security features and controls (A/V, host-based firewall), or modifying application permissions or configuration settings.
Physical and Environmental Protection (PE)	Physical Access Control	• Direct physical access to control system equipment (by either an outsider or a malicious insider) can allow an attacker easier access to ICS assets allowing direct manipulation (via a human-machine interface (HMI) station), reprogramming, or tampering with field controller equipment.
System and Communications Protection (SC)	Security Function Isolation	• Flat network architectures minimize the complexity required for successful exploitation or unauthorized access to the ICS. • Without appropriate boundary protections, multiple layers of authentication, and security controls, adversaries could utilize accounts and systems within the corporate (or trusted third-party) environments as a vector for downstream access to control system components. • In addition, flat architectures do not provide an inherent means to readily monitor and detect nefarious activity between systems and devices.

3.1 Recommended Mitigation Strategies and Best Practices

As the threat landscape evolves, and actors continue to develop new tools and techniques to find and exploit vulnerabilities in systems, it is imperative that ICS users implement a secure and robust architecture to support the availability and integrity of process automation and operations. The cyber security risks that organizations face decrease significantly with a strong ICS architectural framework that includes both protective and detective cybersecurity controls, implemented at multiple layers. Similarly, a robust architecture improves the organization's capability to adequately detect and defend against potential threats and exploits. The common vulnerabilities identified in Section 3 represent significant weaknesses that asset owners should understand and know how to mitigate. To assist critical infrastructure owners and operators, ICS-CERT offers the mitigation strategies and best practices described below.

3.2 Systems and Communications Protection

Without a comprehensive asset inventory of the devices and systems that directly support the OT environment, it can be difficult to establish a cyber-boundary and enforce protective and detective measures. To establish a sound defensive boundary and ensure the proper scope of security controls required to support operations, asset owners should conduct, document, and maintain a thorough asset inventory. The inventory should include the following:

- All ICS components, including all software and hardware
- Networking and communications system components
- Dependent systems and applications utilized in support of the process automation. These include, for example, domain controllers, backup servers, logging and auditing platforms, and alerting mechanisms.

To comprehensively incorporate cybersecurity within the OT architecture, asset owners should establish zones of protection around ICS systems. This requires a thorough understanding of network communications and system dependencies, based upon the operational requirements associated with the automated process. Understanding the nature of communication flows—including operational ingress/egress points—and protocol hierarchy helps define the logical boundary. It is also imperative to fully understand and define the range of ports and services required for the systems within the ICS environment, as these delineations are necessary for enforcing proper zoning. Without completing this analysis and understanding the required intercommunications at the design onset, existing security and segmentation controls (for example, firewalls, virtual local area networks [VLAN], and access-control lists) can quickly become ineffective, particularly if network paths must be continually opened and modified between devices and network segments.

Applying Control Systems Specific Standards

NIST Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, implements an industrial control systems overlay to NIST 800-53, tailoring security guidance to the unique operational and system characteristics of industrial control systems.

While NIST 800-82 applies generally to control systems in all critical infrastructure sectors, ICS-CERT can work with sector stakeholders to provide additional tailoring to the unique aspects of individual sectors, as necessary.

Once asset owners identify and verify the scope of required communication flows, the design of the infrastructure should support both virtual and logical separation of the ICS network, on physically separate devices from the enterprise/corporate network. Communications to and from the ICS network, and communications sourced from and/or destined to an untrusted network (e.g., the enterprise network), should traverse an intermediary demilitarized zone (DMZ) or perimeter network. The organization should create a defined perimeter, with specific ingress and egress points for data flows and "choke points" for enforcing monitoring and protective controls for data flows traversing from one zone to another. For additional information pertaining to designing ICS architectures, reference NIST 800-82 (Section 5 – Network Architecture).[6]

Proper segmentation must also include any safety and protective systems if they are accessible via a cyber-mechanism or network-based conduit. These systems are the last line of defense for an industrial process and should be further isolated from the cyber communication channels that govern the ICS (or other systems) using best practice boundary protections and isolation.

Perhaps most importantly, people are a key foundational element for enforcing, managing, monitoring, tuning, responding, and continually adapting and validating cyber security controls and practices employed throughout the enterprise. The design for automated control systems is highly dependent on the ability of people to architect, tune, monitor, and continually enhance protective and detective cyber security controls. Without this foundational element, even the most robust control systems architectures will not provide the necessary protections on a continual basis.

3.3 Access Control—Information Flow Enforcement

Understanding the communication flows occurring within the ICS network—and conversely those sourced from or destined to the ICS network—is an essential precursor to building a powerful detection and monitoring platform for verifying network traffic and ensuring the integrity and availability of the control process.

If devices do not have an operational need to establish a communications channel, the architecture should support the capability to deny and prevent devices and systems from communicating via a direct or indirect channel. In addition, asset owners should maintain the capability to log and record traffic for systems *attempting* to establish a communications channel, even if explicitly denied. Asset owners should also baseline intra-network traffic in accordance with the operational nature of the control process. Common examples include the following:

- Verifying and monitoring device-to-device communications.
- Establishing security controls and enhancing visibility into the commands transmitted between devices (e.g., reads, writes, function codes, acknowledge responses, and exception messages).
- Isolating and enhancing security controls pertaining to devices that can illicit write commands or make modifications to downstream devices.
- Verifying and monitoring for communication requests sourced from field devices attempting to "back-channel" into the core of the control network.

[6] NIST 800-82: guide to Industrial Control Systems Security (http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)

3.4 Access Control—Remote Access

The nature of distributed operations, coupled with an observed reduction in the personnel directly responsible for maintaining and monitoring process automation, presents a challenge for real-time monitoring, response, and investigative actions, an important part of control system operations. As asset owners and operators move away from maintaining personnel physically located within a control center to a more distributed model for maintaining and operating ICS architectures, this can create challenges. If not architected properly, remote access can elevate risk and become a catalyst for potential unauthorized access or nefarious activity.

Remote access should not sacrifice security for the sake of convenience. An insecure implementation and use of remote access capabilities can completely invalidate even the best security architecture. Control systems and their supporting systems must never be directly accessible through untrusted networks such as the internet; they should be protected and sequestered from untrusted (external) networks and systems.

When designing a network architecture that supports remote access, asset owners should consider detective and protective controls and include them as part of the underlying infrastructure. The design should provide an inherent means to do the following:

- Monitor and verify the scope of remote access communications and connectivity
- Monitor communication flows occurring via the remote access channel
- Log authentications (both successful and unsuccessful)
- Enforce protective and detective measures pertaining to failed connectivity attempts or nefarious traffic patterns
- Restrict the scope of remote access sessions to only those personnel assigned a responsibility for supporting the ICS and process operations
- Disable split-tunneling when connected via a remote session (effectively routing all traffic through the VPN or remote access gateway)
- Enforce connectivity from only authorized origination systems
- Implement application layer firewalls, application whitelisting, and endpoint policy enforcement for origination systems.

The architecture supporting remote access should not only account for access required by the organization’s internal engineers and operators, but also third-party contractors or vendors, who may be required to remotely assist the organization.

Asset owners should implement multiple defense layers for accessing control system networks from a remote location. Generally, most organizations require their personnel to utilize a VPN technology using encryption to interface with corporate systems and applications when accessing from a remote location. For control systems, the capability to directly interface with supporting systems and components should not be permissible directly from systems housed on the corporate or enterprise network. Rather, asset owners should only allow access through an intermediate system or “jump box” resident within a dedicated Control Systems DMZ.

Access to the intermediate system should require a second layer of authentication, which is unique and different from that used to remotely access the corporate environment or corporate systems via VPN. In addition, personnel accessing the control systems network from remote locations should authenticate using an appropriately strong mechanism (multi-factor authentication) from a validated and secured company issued and controlled device (e.g., desktop or laptop PC).

The intermediate system—or "jump box" within the Control Systems DMZ—provides a centralized means to monitor, restrict, and govern remote access into the control systems environment. This system also provides a capability to adequately limit the boundary of the control system perimeter. Rather than virtually extending the boundary to the initiating remote system, the boundary is now logically restricted to the intermediate system, where the necessary scope of applications and protective and detective security controls can be deployed.

For third party vendors or contractors, the organization must ensure that remote connectivity is subject to the same scope of security controls enforced for organizational personnel connectivity via a remote avenue. To the degree possible, security policy should limit the use of persistent VPN tunnels, and the organization should have the capability to directly control and authorize specific vendors or contractors to initiate remote sessions. Asset owners should monitor the duration of remote sessions and disable that function once service support is no longer required or is complete.

Once the architecture is implemented, verification of all remote access methods should be continuously enforced, to ensure adherence to the organization's defined policy and their supporting security controls. Asset owners should also test and verify the capability to readily bypass remote access controls. As a practical example, the usage of dial-up modems is still a common vector for remotely interfacing with various field device and systems. Modems are typically overlooked, and are sometimes not considered when performing audits and assessments of supporting components utilized as part of the control system infrastructure. If unsecured and unmonitored, modems can provide a backdoor for directly interfacing with ICS components, most likely undetected by the organization. Security controls for consideration include restricting dial-in capabilities (limiting use to emergency "dial-out"), limiting dial-back capabilities to pre-defined phone numbers, or enforcing a PIN or passphrase for initial authentication. Asset owners should also review the use of more recent technologies such as wireless Wi-Fi and Bluetooth, based on their potential to tie into enabled devices that result in bridging of networks. This may enable attackers to use these secondary communications pathways to connect to ICS devices, thus bypassing security controls.

3.5 Access Control—Least Privilege

Asset owners should assign roles and permissions to users of the various systems and applications in the automation process based upon the concept of least privilege. Least privilege is the practice of limiting access to the minimal level that allows for normal operations. Quite often, users are granted permissions beyond what is necessary based upon a person's assigned role or responsibility.

Before assigning users' specific permissions, an organization must formally define the roles and responsibilities required to support operational needs. Once user roles and responsibilities are defined, asset owners should review the technologies in place to ensure that the necessary mappings and restrictions can be enforced, tracked, audited, and verified. Whether this occurs

locally at the application level or centrally within an access-control technology (Active Directory, Identity Access Management platform), the organization must document and verify how it will apply and manage permissions within the scope of its infrastructure and platforms.

The organization can then map and assign users and operator permissions, based upon their operational need. Organizations should not allow the unnecessary use of elevated and administrative permissions for daily job functions, and personnel should utilize an account with minimal permissions assigned for normalized operations. If there is a need for use of a privileged account for daily job functions, the organization should harden that system and consider additional defense-in-depth measures to isolate and protect the system.

Logging and monitoring should track user activity and have the capability to provide a record (including timestamp) of user activity occurring on a system or within an application. Asset owners should log, audit, and review changes made by users, including changes pertaining to user mappings, roles, and privilege assignments. Additional logging and security controls should be enforced for users and groups that provide and assign an administrative or root-level context within a system or application. Specific to industrial control systems, least privilege and monitoring should include the following:

- Roles, mappings, and privilege assignments of responsibility within SCADA or HMI applications.
- An audit record of personnel attempting to use an elevated or administrative account to perform daily job functions (even for those personnel who do not require administrative access, but are attempting to elevate privileges).
- When monitoring and controlling an ICS process, it may not always be feasible to enforce an automated lock for display terminals or display boards for idle sessions. For these conditions, ensure that display terminals within areas of a facility where various personnel may have access present a “read-only” or “view-only” capability, and that a standard user or someone with unapproved access could not interface with a terminal and make unauthorized changes or modifications to the process. Asset owners should also enforce appropriate physical security controls for these areas (e.g., key card access on the doors to the control center).
- Monitoring for specific changes to roles assigned to users and/or groups.
- Monitoring of personnel or permissions assigned to groups, especially those that provide an administrative or privileged context within a control system application.
- Changes assigned to various areas of responsibility and privilege mappings.
- Monitoring of access attempts, for personnel who are attempting to access a resource or program function for which they are specifically denied or not assigned privileges.
- If the organization uses domain services—for example, Active Directory—in support of the ICS applications and systems, this domain should be separate and isolated from the domain services utilized in support of the enterprise or corporate environment. The accounts and services provided by the ICS domain should exist solely to support the ICS and automation process. It should not have a direct trust relationship with any other domains or third party entities.

3.6 Physical and Environmental Protection

Many asset owners rely upon physical security controls to safeguard and protect key systems utilized in support of the process and automation. If adversaries can exploit a weakness in physical security, this could lead to risks correlating to both cyber and physical consequences, including the following:

- Physical theft or damage to hardware and data.
- Unauthorized changes to configuration settings and processes within the control and automation environment.
- Disconnection of physical data links or interference of wireless (telemetry) data paths.
- Interception or manipulation (spoofing) of data, which could lead to system unavailability and impact the integrity of the control process.
- The practice of operating with Programmable Logic Controllers (PLCs) in "program" mode for the convenience of engineering and maintenance elevates risks associated with an unauthorized user modifying the controller's operating logic, which could compromise the integrity of the automated process.

As many control system environments are widely distributed over a large geographic area, remote sites and locations may not always be physically manned by personnel at all times. It is especially important to enforce both physical and cyber security controls, including monitoring for these environments. If a physical breach were to occur, this could provide a vector for an outsider to gain upstream access back into the core of the control systems infrastructure. Common examples of physical controls to include are as follows:

- A detailed inventory of all hardware and software components utilized in support of operations, including detailed information pertaining to device/model type, serial number, and firmware version.
- Physical access control measures for governing and restricting access to the facility, including areas within a facility (e.g., gates, buildings, doors, and rooms).
    - If utilizing keys, ensure that the physical control of keys is audited and maintained, especially for personnel no longer supporting the organization, or who no longer have a need to access various parts of the facilities.
    - Ensure that physical keys are marked with "DO NOT COPY" or "DO NOT DUPLICATE."
- Enforce intrusion detection alarms and alerts for all ingress/egress areas within a facility—including those at the perimeter and within various buildings and rooms (e.g., doors, windows, cabinets, racks, and card readers). Special attention should be given to alternate methods that can be utilized for circumventing traditional security controls for unauthorized physical access to a facility.
- If utilizing cameras for physical monitoring of a facility or site, ensure the following:
    - Default credentials and settings for the cameras are changed and modified.
    - The cameras are resident on a secured and controlled VLAN or network segment, which cannot be directly accessed by unauthorized personnel or systems within the organization.

    - The cameras cannot be used as a vector to gain unauthorized access or provide a "back channel" into the enterprise or control systems network infrastructure.
  - The cameras cannot be remotely accessed or viewed without authentication and logging of the connectivity attempts (both successful and unsuccessful).
  - The cameras provide adequate and clear coverage for the areas they monitor.
- For systems that centrally manage physical access controls (for example, an access control system that utilizes badge readers), ensure the following:
  - Restrict physical and virtual access (including enforcing role-based access control) for the centralized application that governs physical access control.
    - This should also include the workstations and systems that are initiating connectivity to manage and administer the physical access control system.
  - Systems housing the centralized application or backend database do not have the capability to establish an outbound session or communications channel to untrusted resources or networks (like the internet).
  - Testing of access control functionality, especially if communications from the centralized application to the card or badge readers is lost. Asset owners should understand whether the system operates based on the last configuration or "denies" access until communications have been re-established.
- If possible, place PLCs in "run" mode when in operation and remove and secure the key.

4. CONCLUSION

The protection of the Nation's critical infrastructure is essential for ensuring public confidence and safeguarding the Nation's safety, prosperity, and well-being. As the 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 automation and processes that support our Nation's critical infrastructure.

The high-level discoveries and mitigation recommendations outlined within this document should not be used as an all-inclusive focus of an assessment; rather, these areas should be carefully reviewed and encompassed within the scope of an organization's overall cyber security framework, design, and review. Addressing the best practices and recommendations in this report can greatly improve a CI asset owner's overall security posture and heighten awareness of potential threats or cyber-attacks targeting their specific operations.

Additional ICS-CERT Resources and Information

In addition to onsite assessment services, ICS-CERT offers a number of free services and products to help secure control systems. These services and products include training, recommended practices, white papers, incident response, and malware analysis.

For general questions or comments, contact ICS-CERT at ics-cert@hq.dhs.gov.

For information on training or downloading white papers and other useful documents on ICS cybersecurity, visit the web site https://ics-cert.us-cert.gov.

To report an incident or vulnerability, call 1-888-282-0870 or send an email to ics-cert@hq.dhs.gov.

Appendix A

NIST 800-53 Security Control Family Descriptions

ICS-CERT uses the National Institute of Standards and Technology's (NIST) Recommended Security Controls for Federal Information Systems (NIST 800-53) to categorize the vulnerabilities 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 sub-categories 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 below:

Access Control (AC) - The process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.

Awareness and Training (AT) - Policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and those accurate training records are maintained.

Audit and Accountability (AU) - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Security Assessment and Authorization (CA) - Assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.

Contingency Planning (CP) - Policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Configuration Management (CM) - Policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Identification and Authentication (IA) - The process of verifying 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) - Policies and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.

Maintenance (MA) - Policies and procedures to manage all maintenance aspects of an information system.

Media Protection (MP) - Policies and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.

Physical and Environmental Protection (PE) - Policies and procedures addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).

Planning (PL) - Development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents.

Personnel Security (PS) - Policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.

Risk Assessment (RA) - The process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

System and Services Acquisition (SA) - Allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation.

System and Communications Protection (SC) - Mechanisms for protecting both system and data transmission components.

System and Information Integrity (SI) - Policies and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls.

Program Management (PM) - Provides security controls at the organizational rather than the information-system level.

Department of Homeland Security

Office of Cybersecurity and Communications

National Cybersecurity and Communications Integration Center

Industrial Control System – Cyber Emergency Response Team

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