SITE CYBER SECURITY PLAN

CONTROL SYSTEMS CYBER SECURITY EVALUATION

Homeland Security

High Level Cyber Security Assessment

2/1/2012

Assessor: J. Doe

Disclaimer

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

The DHS does not endorse any commercial product or service, including the subject of the assessment or evaluation in this report. Any reference to specific commercial products, processes, or services by trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS's policies governing usage of the seal.

The report is prepared and intended for internal use by the organization that made the request. The contents of this report may be subject to government or private intellectual property rights. To request distribution of this report outside the organization for which it was prepared, contact the CSET® Program Office. The contents of this report may be reproduced or incorporated into other reports, but may not be modified without the prior express written permission of the CSET® Program Office.

Signatures

My signature indicates that I have reviewed and approve this Site Cyber Security Plan and the corresponding appendices. To the best of my knowledge, they accurately describe the security profile of the High Level Cyber Security Assessment security policies and procedures, including the operational, management, and technical controls under which they will be operated.

(Example only. Copy and replace the text in this signature block for each applicable position.)

_____ _____

Sample Corporate Officer, CEO John Doe ***Date***

Table of Contents

Introduction

Template instructions and directives are given in italicized 10 point font and should be replaced appropriately.

This security plan template is intended to be used as a tool for the development of a security plan. This template will assist you in identifying the controls in place and those needing further implementation based upon the answers provided in the accompanying CSET assessment. The basic process for this plan development would be to first determine risk, second select the countermeasures necessary to mitigate the risk to an acceptable level, and finally follow through to ensure that the countermeasures are implemented to the expected level.

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. The site cyber security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

The System Owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the System Security Manager

This template may also include:

- *Recommended templates for policies or procedures that have been identified as needed but not currently available based on the assessment answers.*
- *The basic network diagram*
- *An Inventory List of the components included in the diagram that will be associated with specific controls.*
- *The List of recommended security controls along with a status as can be determined from the assessment questions.*
- *A recommended implementation priorities list. This priority is based on incident occurrence on the ICS-CERT watch floor as of the date of publication the CSET tool. These recommendations do not take into account any cost benefit analysis with respect to implementing a control.*
- *Basic security assurance level determinations carried over from the assessment. In developing a security plan it is recommended that a deeper risk analysis is conducted to ensure that the selection of controls is not overly conservative (incurring undo costs) or optimistic (leaving excessive risk exposure).*

1. System Identification

Provide a brief one-two paragraph description of the main system assests the necessary protection levels for confidentiality, integrity, and availability. See section 3.1 for a more detailed description of confidentiality, integrity, and availability.

1.1. System Environment

Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- *The system is connected to the Internet;*
- *It is located in a harsh or overseas environment;*
- *Software is rapidly implemented;*
- *The software resides on an open network used by the general public or with overseas access;*
- *The application is processed at a facility outside of the organization's control; or*
- *The general support mainframe has dial-up lines.*

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

2. Roles and Responsibilities

This section defines the roles and responsibilities for cyber security within the company. Use this section to define the roles and responsibilities with respect to this plan for your company.

2.1. Executive Management

Often this role is comprised of the Board of Directors and CEO. Executive management is ultimately responsible for the security of organization but will most likely delegate tasks and actual implementation.

2.2. Chief Security Officer or Chief Information Security Officer (CISO)

CSO or CISO is the senior level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks, respond to incidents, establish appropriate standards and controls, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information related compliance.

Typically, the CISO's influence reaches the whole organization. Responsibilities include:

- Information security and information assurance
- Information regulatory compliance (e.g., US PCI DSS, FISMA, GLBA, HIPAA; UK Data Protection Act 1998; Canada PIPEDA)
- Information risk management
- Supply chain risk management
- Cybersecurity
- Information technology controls for financial and other systems
- Information privacy
- Computer Emergency Response Team / Computer Security Incident Response Team
- Identity and access management
- Security Architecture (e.g. Sherwood Applied Business Security Architecture)
- IT investigations, digital forensics, eDiscovery
- Disaster recovery and business continuity management
- Information Security Operations Center ISOC

2.3. Security Steering Committee

The security steering committee is composed of a representative of all the key stakeholders in IT

security. These stake holders are often representatives of the the excutive council, CISO or CSO, IT management, physical security personnel, help desk, and key application and digitial asset owners. This committee meets regularly often quarterly to review policies and procedures, security controls implementation progress, and determine future direction for security within a company.

The security steering committee is responsible for making decisions on tactical and strategic security issues within the enterprise as a whole and should not be tied to one or more business units. The group should be made up of people from all over the organization so they can view risks and the effects of security decisions on individual departments and the organization as a whole. The CEO should head this committee, and the CFO, CIO, department managers, and chief internal auditor should all be on it. This committee should meet at least quarterly and have a well defined agenda. So me of the group's responsibilities are listed next:

- Define the acceptable risk level for the organization.
- Develop security objectives and strategies.
- Determine priorities of security initiatives based on business needs.
- Review risk assessment and auditing reports.
- Monitor the business impact of security risks.
- Review major security breaches and incidents.
- Approve any major change to the security policy and program.

They should also have a clearly defined vision statement in place that is set up to work with and support the organizational intent of the business. The statement shouldbe structured in a manner that provides support for the goals of confidentiality, integrity, and availability as they pertain to the business objectives of the organization. Thisin turn should be followed, or supported, by a mission statement that provides support and definition to the processes that will apply to the organization and allow it to reachits business goals.

2.4. System Owners

The system owner is responsible for one or more systems, each of which may holdand process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisionsand development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role must ensure the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

2.5. Data Owners

The data owner (information owner) is usually a member of management who is incharge of a specific business unit, and who is ultimately responsible for the protectionand use of a specific subset of information. The data owner has due care responsibilitiesand thus will be held responsible for any negligent act that results in the corruption or disclosure of the data. The data owner decides upon the classification of the data he isresponsible for and alters that classification if the business need arises. This person is also responsible for ensuring that the necessary security controls are in place, defining security requirements per classification and backup requirements, approving any disclosure activities, ensuring that proper access rights are being used, and defining user access criteria. The data owner approves access requests or may choose to delegate thisfunction to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian.

2.6. Security Administrators

Anyone who has a root account on Unix or Linux systems or an administrator account on Windows or Macintosh systems actually has security administrator rights. (Unfortunately, too many people have these accounts in most environments.) This means they can give and take away permissions, set security configurations. However, just because a person has a root or administrator account does not mean they are fulfilling the security administrator role. A security administrator's tasks are many, and include creating new system user accounts, implementing new security software, testing security patches and components, and issuing new passwords. (The security administrator should not actually approve new system user accounts. This is the responsibility of the supervisor.) The security administrator must make sure access rights given to users support the policies and data owner directives.

2.7. Supervisors/Managers

The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. The supervisor responsibilities would include ensuring that employees understand their responsibilities with respect to security, distributing initial passwords, making sure the employees' account information is up-to-date, and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

2.8. Users

The user is any individual who routinely uses the data for work related tasks. The user must have the necessary level of access to the data to perform the duties within their position and is responsible for following operational security procedures to ensure the data's confidentiality, integrity, and availability to others.

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. If not yet performed yet it is recommended that the general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

threats × vulnerability × asset value = total risk

total risk – countermeasures = residual risk

Consequence

The examination of the consequences of an attack should include

If control systems were maliciously accessed and manipulated to cause harm in a worst case scenario

- *How many people could sustain injuries requiring a hospital stay?*
- *How many people could be killed?*
- *Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)*
- *Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and use and any costs associated with displacement.)*
- *Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, litigation, long term monitoring, etc.)*

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are set based on incident data collected at the ICS-CERT watch floor and subject matter experts as of the time of publication of CSET. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

Cost Benefit Analysis

The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

3.1. Basic Model

Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address the each of these areas with respect to data and systems.

3.1.1. Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

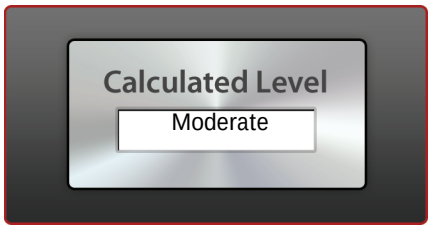
3.1.2. Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

3.1.3. Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

3.2. Security Assurance Level (SAL)



	Confidentiality	Integrity	Availability
Overall Values	Moderate	Moderate	Moderate

Calculated General Security Assurance Levels

	Onsite	Offsite
Physical Injury	None	None
Hospital Injury	None	None
Death	None	None
Capital Assets	None	None
Economic Impact	None	None
Environmental Impact	None	None

NIST SP800-60 (FIPS 199) Based Security Assurance Levels

	Confidentiality	Integrity	Availability
Adjusted For System Questions	None	None	None
Information Type	None	None	None

4. Security Plan Controls and Status List

This section of the security plan lists all the controls which constitute this security plan and their implementation status. To enable easier reading of the controls list a table key is included at the start of this section.

Table Key and Field Descriptions:

Requirement Title		CSET Question Category
Control Level	Implementation Status	Short Standard Name
Control Description		
Affected Zones (Optional may not be included in the table)		
Affected Components (Optional may not be included in the table)		
Related Questions and Answers		

Requirement Title: Is the control title as it is generally defined in the standard document from which this control is derived

CSET Question Category: Shows the CSET Question category from the global questions list. Questions from multiple standards have been consolidated together in the CSET tool and assigned a common category.

Control Level: Mapped to one of Low, Moderate, High, or Very High

Implementation Status: Shows the percentage complete as the number of yes answers / total related questions for this control. This percentage implemented will not necessarily be reflective of the amount of work required to implement the control but is merely an indicator of how many of the questions related to the control have been addressed so far.

Short Standard Name: An indicator of which standard this control is derived from.

Control Description: The full control text as defined in the standard from which the control is derived.

Affected Zones: Only applicable to controls derived from a diagram. If you have included a diagram in your original assessment this field will contain a list of zone in which atleast one component was found to require this control.

Affected Components: This field contains a list of the components that are directly applicable to this control.

Related Questions and Answers: A list of the questions and answers from which the implementation status of this control was determined.

2.1.1-Security Policy		Policies & Procedures General
Low	40%	Catalog of Recommendations Version 7

The organization develops, implements, and periodically reviews and updates: 1. A formal, documented, control system security policy that addresses: a. The purpose of the security program as it relates to protecting the organization's personnel and assets. b. The scope of the security program as it applies to all organizational staff and third-party contractors. c. The roles, responsibilities, management commitment, and coordination among organizational entities of the security program to ensure compliance with the organization's security policy and other regulatory commitments.2. Formal, documented procedures to implement the security policy and associated requirements. A control system security policy considers controls from each family contained in this document.

System Security Policy	U
Does the system security policy address the purpose of the security program as it relates to protecting the organization's personnel and assets?	Y
Does the system security policy address the scope of the security program as it applies to all organizational staff and third-party contractors?	Y
Security Procedure	N
Are security policies and procedures implemented to define roles, responsibilities, behaviors, and practices of an overall security program?	U

2.2.1-Organizational Security		Organizational
Low	0%	Catalog of Recommendations Version 7

The organization establishes policies and procedures to define roles, responsibilities, behaviors, and practices for the implementation of an overall security program.

Are security policies and procedures implemented to define roles, responsibilities, behaviors, and practices of an overall security program?	U

2.3.2-Personnel Security		Personnel
Low	100%	Catalog of Recommendations Version 7

The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically based on the organization's requirements or regulatory commitments.

Is a risk designation assigned to all positions and are screening criteria established for individuals filling those positions?	Y
Are position risk designations periodically reviewed and revised?	Y

2.3.3-Personnel Security		Personnel
Low	100%	Catalog of Recommendations Version 7

The organization screens individuals requiring access to the control system before access is authorized.

Requirement Enhancement - The organization rescreens individuals with access to organizational control systems based on a defined list of conditions requiring rescreening and the frequency of such rescreening.

Are individuals requiring access screened before access is authorized?	Y

2.3.6-Personnel Security		Personnel
Low	100%	Catalog of Recommendations Version 7

The organization completes appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the control system. The organization reviews and updates access agreements periodically.

Are appropriate agreements finalized before access is granted, including for third parties and contractors?	Y
Are access agreements periodically reviewed and updated?	Y

2.3.7-Personnel Security		Personnel
Low	100%	Catalog of Recommendations Version 7

The organization enforces security controls for third-party personnel and monitors service provider behavior and compliance.

Are security controls for third-party personnel enforced, and is service provider behavior and compliance monitored?	Y

2.4.2-Physical and Environmental Security		Physical Security
Low	100%	Catalog of Recommendations Version 7

The organization develops and maintains lists of personnel with authorized access to facilities containing control systems (except for areas within facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials at least annually, removing from the access list personnel no longer requiring access.

Requirement Enhancement 1 - The organization authorizes physical access to the facility where the control system resides based on position or role.

Requirement Enhancement 2 - The organization requires two forms of identification to gain access to the facility where the control system resides.

Are lists of personnel with authorized access developed and maintained, and are appropriate authorization credentials issued?	Y
Are the access list and authorization credentials reviewed and approved at least annually and those no longer requiring access removed?	Y

2.4.3-Physical and Environmental Security		Physical Security
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the control system resides (excluding those areas within the facility officially designated as publicly accessible)

2. Verifies individual access authorizations before granting access to the facility.

3. Controls entry to facilities containing control systems using physical access devices and guards.

4. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk.

5. Secures keys, combinations, and other physical access devices.

6. Inventories physical access devices on a periodic basis.

7. Changes combinations and keys on an organization-defined frequency and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

8. Controls and verifies physical access to information system distribution and transmission lines of communications within the organizational facilities.

9. Controls physical access to information system output devices (e.g., monitors, speakers, printers) to prevent unauthorized individuals from observing and obtaining information access.

Requirement Enhancement 1 - The organization limits physical access to control system assets independent of the physical access security mechanisms for the facility.

Requirement Enhancement 2 - The organization performs security checks at physical boundaries for unauthorized removal of information or system components.

Requirement Enhancement 3 - The organization ensures that every physical access point to the facility where the system resides is guarded or alarmed and monitored 24 hours per day, 7 days per week.

Requirement Enhancement 4 - The organization employs lockable physical casings to protect internal components of the system from unauthorized physical access.

Requirement Enhancement 5 - The organization identifies and inspects information and communication lines for evidence of tampering.

Are physical access authorizations enforced for all physical access points to the facility?	Y
Are individual access authorizations verified before granting access to the facility?	Y
Is entry to the facility controlled by physical access devices and/or guards?	Y
Are the areas officially designated as publicly accessible controlled in accordance with the organization's assessment of risk?	Y
Are keys, combinations, and other physical access devices secured?	Y
Are physical access devices inventoried on a periodic basis?	Y
Are combinations and keys changed on a defined frequency, and when keys are lost, combinations compromised, or individuals are transferred or terminated?	Y
Is physical access to distribution and communication lines controlled and verified?	Y
Is physical access to output devices controlled?	Y

2.4.4-Physical and Environmental Security		Physical Security
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Monitors physical access to the control system to detect and respond to physical security incidents.

2. Reviews physical access logs on an organization-defined frequency.

3. Coordinates results of reviews and investigations with the organization's incident response capability.

Requirement Enhancement 1 - The organization monitors real-time physical intrusion alarms and surveillance equipment.

Requirement Enhancement 2 - The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.

Are physical access logs reviewed on a defined frequency?	Y
Are results of reviews and investigations coordinated with the organization's incident response capability?	Y
Are real-time physical intrusion alarms and surveillance equipment monitored?	Y
Is physical access monitored to detect and respond to physical security incidents?	Y

2.4.16-Physical and Environmental Security		Physical Security
Low	90%	Catalog of Recommendations Version 7

The organization:

1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices.

2. Authorizes connection of mobile devices to organizational control systems.

3. Monitors for unauthorized connections of mobile devices to organizational control systems.

4. Enforces requirements for the connection of mobile devices to organizational control systems.

5. Disables control system functionality that provides the capability for automatic execution of code on removable media without user direction.

6. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

7. Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Requirement Enhancement 1 - The organization restricts the use of writable, removable media in organizational control systems.

Requirement Enhancement 2 - The organization prohibits the use of personally owned, removable media in

organizational control systems.

Requirement Enhancement 3 - The organization prohibits the use of removable media in organizational control systems when the media have no identifiable owner.

Are usage restrictions and implementation guidance established for organization-controlled mobile devices?	Y
Is mobile device connection to the system authorized?	Y
Are requirements for mobile device connection to the system enforced?	Y
Is the capability for automatic execution of code on removable media disabled?	Y
Are specially configured mobile devices issued to individuals traveling to locations of significant risk per policies and procedures?	Y
Are specified measures applied to mobile devices returning from locations of significant risk per policies and procedures?	Y
Is the use of writable, removable media restricted on the system?	Y
Is the use of personally owned, removable media prohibited on the system?	Y
Is the use of removable media with no identifiable owner prohibited on the system?	Y
Are unauthorized remote connections to the system monitored, including scanning for unauthorized mobile or wireless access points on a defined frequency and is appropriate action taken if an unauthorized connection is discovered?	N

2.4.21-Physical and Environmental Security		Physical Security
Low	100%	Catalog of Recommendations Version 7

The organization employs hardware (cages, locks, cases, etc.) to detect and deter unauthorized physical access to control system devices.

Requirement Enhancement - The organization ensures that the ability to respond appropriately in the event of an emergency is not hindered by using tamper-evident hardware.

Is hardware (cages, locks, cases, etc.) used to detect and deter unauthorized physical access to system devices?	Y

2.5.4-System and Services Acquisition		System and Services Acquisition
Low	75%	Catalog of Recommendations Version 7

The organization includes the following requirements and specifications, explicitly or by reference, in control system

acquisition contracts based on an assessment of risk and in accordance with applicable laws, directives, policies, regulations, and standards:

1. Security functional requirements/specifications.

2. Security-related documentation requirements.

3. Developmental and evaluation-related assurance requirements.

Requirements Enhancement 1 - The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls employed within the control system.

Requirements Enhancement 2 - The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls employed within the control system (including functional interfaces among control components).

Requirements Enhancement 3 - The organization limits the acquisition of commercial technology products with security capabilities to products that have been evaluated and validated through a government-approved process.

Are security functional requirements and specifications included in system acquisition contracts based on an assessment of risk?	Y
Are security-related documentation requirements included in system acquisition contracts based on an assessment of risk?	Y
Are developmental and evaluation-related assurance requirements (acceptance testing, compliance documentation) included in system acquisition contracts based on an assessment of risk?	N
Do acquisition documents require that vendors/contractors provide information describing the functional properties of the security controls employed within the system?	Y

2.5.7-System and Services Acquisition		System and Services Acquisition
Low	100%	Catalog of Recommendations Version 7

The organization implements policies and procedures to enforce explicit rules and management expectations governing user installation of software.

Are policies and procedures in place to enforce explicit rules and management expectations governing user installation of software?	Y

2.5.9-System and Services Acquisition		System and Services Acquisition
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Requires that providers of external control system services employ security controls in accordance with applicable laws, directives, policies, regulations, standards, guidance, and established service-level agreements. 2. Defines government oversight and user roles and responsibilities with regard to external control system services. 3. Monitors security control compliance by external service providers.

Are providers of external system services required to employ security controls in accordance with applicable, policies, regulations, standards, guidance, and established service level agreements?	Y
Is security control compliance by external service providers monitored?	Y

2.5.11-System and Services Acquisition		System and Services Acquisition
Moderate	100%	Catalog of Recommendations Version 7

The control system developer/integrator:

1. Develops a security test and evaluation plan.

2. Implements a verifiable error remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.

3. Documents the result of the security testing/evaluation and error remediation processes.

Requirement Enhancement 1 - The organization requires that control system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

Requirement Enhancement 2 - The organization requires that control system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

Requirement Enhancement 3 - The organization requires that information system developers/integrators create a security test and evaluation plan and implement this plan under independent verification and validation.

Does the system developer have a security test and evaluation plan?	Y
Does the system developer have a verifiable error remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process?	Y
Does the system developer/integrator document the result of the security testing/evaluation and error remediation processes?	Y

2.6.1-Configuration Management		Configuration Management
Low	100%	Catalog of Recommendations Version 7

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented configuration management policy that addresses:

a. The purpose of the configuration management policy as it relates to protecting the organization's personnel and assets.

b. The scope of the configuration management policy as it applies to all the organizational staff and third-party contractors.

c. The roles, responsibilities, management accountability structure, and coordination among organizational entities contained in the configuration management policy to ensure compliance with the organization's security policy and other regulatory commitments.

2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

3. The personnel qualification levels required to make changes, the conditions under which changes are allowed, and what approvals are required for those changes.

Configuration Management Policy	Y
Configuration Management Procedure	Y
Are the personnel qualification levels reviewed and periodically updated for personnel to make changes, conditions for allowing changes, and the approvals required for changes?	Y

2.6.2-Configuration Management		Configuration Management
Low	100%	Catalog of Recommendations Version 7

The organization develops, documents, and maintains a current baseline configuration of the control system and an inventory of the system's constituent components.

Requirement Enhancement 1 - The organization reviews and updates the baseline configuration as an integral part of control system component installations.

Requirement Enhancement 2 - The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the control system.

Requirement Enhancement 3 - The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

Requirement Enhancement 4 - The organization employs a deny-all, permit-by-exception authorization policy to identify software allowed on organizational control systems.

Has a current baseline configuration been developed, documented, and maintained for the system?	Y

Is the baseline configuration of the system reviewed and updated?	Y

2.6.3-Configuration Management		Configuration Management
Moderate	67%	Catalog of Recommendations Version 7

The organization:

1. Authorizes and documents changes to the control system.

2. Retains and reviews records of configuration-managed changes to the system.

3. Audits activities associated with configuration-managed changes to the system.

Requirement Enhancement 1 - The organization employs automated mechanisms to:a. Document proposed changes to the control system.b. Notify appropriate approval authorities.c. Highlight approvals that have not been received in a timely manner.d. Inhibit change until necessary approvals are received.e. Document completed changes to the control system.

Requirement Enhancement 2 - The organization tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational control system. The organization ensures that testing does not interfere with control system operations. The tester fully understands the corporate cyber and control system security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process.

Are changes to the system authorized and documented?	Y
Are records of configuration-managed changes to the system reviewed and retained?	Y
Are configuration-managed changes to the system audited?	N

2.6.4-Configuration Management		Configuration Management
Low	100%	Catalog of Recommendations Version 7

The organization implements a process to monitor changes to the control system and conducts security impact analyses to determine the effects of the changes.

Does a process exist to monitor changes to the system and conduct security impact analyses to determine the effects of the changes?	Y

2.6.8-Configuration Management	Configuration Management

Low	100%	Catalog of Recommendations Version 7

The organization develops, documents, and maintains an inventory of the components of the control system that:

1. Accurately reflects the current control system.

2. Is consistent with the authorization boundary of the control system.

3. Is at the level of granularity deemed necessary for tracking and reporting.

4. Includes defined information deemed necessary to achieve effective property accountability.

Requirement Enhancement 1 - The organization updates the inventory of control system components and programming as an integral part of component installation, replacement and system updates.

Requirement Enhancement 2 - The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of control system components, configuration files and setpoints, alarm settings and other required operational settings.

Requirement Enhancement 3 - The organization employs automated mechanisms to detect the addition of unauthorized components/devices/component settings into the control system.

Requirement Enhancement 4 - The organization disables network access by such components/devices or notifies designated organizational officials.

Requirement Enhancement 5 - The organization includes in property accountability information for control system components, the names of the individuals responsible for administering those components.

Has an inventory of the components of the system been developed, documented and maintained that accurately reflects the current system?	Y
Has an inventory list of the components of the system been developed, documented, and maintained that is consistent with the system boundary?	Y
Has an inventory list of the components of the system been developed, documented, and maintained that is at the level of granularity deemed necessary for tracking and reporting?	Y
Has an inventory of the components of the system been developed, documented, and maintained that includes defined information deemed necessary to achieve effective property accountability?	Y
Is the inventory of system components and programming updated as an integral part of component installation, replacement, and system updates?	Y

2.6.10-Configuration Management		Configuration Management
Low	100%	Catalog of Recommendations Version 7

The organization changes all factory default authentication credentials on control system components and

applications upon installation. Requirement Enhancement - Known legacy operational equipment needs compensatory access restrictions to protect against loss of authentication. In addition, these components need to be identified, tested, and documented to verify that proposed compensatory measures are effective.	
Are all factory default authentication credentials changed on system components and applications upon installation?	Y

2.6.11-Configuration Management		Configuration Management
Moderate	0%	Catalog of Recommendations Version 7
The organization develops and implements a configuration management plan for the control system that: 1. Addresses roles, responsibilities, and configuration management processes and procedures. 2. Defines the configuration items for the control system. 3. Defines when in the system development life cycle, the configuration items are placed under configuration management. 4. Defines the means for uniquely identifying configuration items throughout the system development life cycle. 5. Defines the process for managing the configuration of the controlled items. Requirement Enhancement 1 - The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.		

2.7.2-Strategic Planning		Organizational
Low	89%	Catalog of Recommendations Version 7
The organization: 1. Develops a security plan for the system that: a. Aligns with the organization's enterprise architecture. b. Explicitly defines the authorization boundary for the system. c. Describes relationships with or connections to other systems.		

d. Provides an overview of the security requirements for the system.

e. Describes the security controls in place or planned for meeting those requirements.

f. Specifies the authorizing official or authorizing official designated representative who reviews and approves the control system security plan prior to implementation.

2. Reviews the security plan for the system on an organization-defined frequency, at least annually.

3. Revises the plan to address changes to the system/environment of operation or problems identified during plan implementation or security control assessments.

Requirement Enhancement - Secure control system operations require more in-depth and specialized security plans, which limit data ports, physical access, specific data technology (Fiber), additional physical and electronic inspections and physical separation requirements.

Security Plan	Y
Does the security plan align with the organization's enterprise architecture?	U
Does the security plan explicitly define the authorization boundary of the system?	Y
Does the security plan describe the relationships with or connections to other systems?	Y
Does the security plan provide an overview of the security requirements for the system?	Y
Does the security plan describe the security controls in place or planned?	Y
Is the authorizing official or designated representative who reviews and approves the system security plan specified?	Y
Is the security plan for the system reviewed on a defined frequency, but at least annually?	Y
Is the security plan revised to address changes to the system/environment or problems identified during plan implementation or security control assessments?	Y

2.7.4-Strategic Planning		Organizational
Low	100%	Catalog of Recommendations Version 7

The organization's control system security plan defines and communicates the specific roles and responsibilities in relation to various types of incidents.

Does the security plan define and communicate the specific roles and responsibilities in relation to various types of incidents?	Y

2.7.11-Strategic Planning		Organizational
Low	100%	Catalog of Recommendations Version 7

The organization establishes and makes readily available to all control system users a set of rules that describes their responsibilities and expected behavior with regard to control system usage. The organization obtains signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the control system.

Requirement Enhancement - The organization includes in the rules of behavior explicit restrictions on the use of social networking sites, posting information on commercial web sites, and sharing system account information.

Are a set of rules that describes the system users responsibilities and expected behavior established and made available?	Y
Has a signed acknowledgment been obtained from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the system?	Y

2.8.4-System and Communication Protection		Communication Protection
Moderate	100%	Catalog of Recommendations Version 7

The control system prevents unauthorized or unintended information transfer via shared system resources.

Requirement Enhancement - The information system does not share resources that are used to interface with systems operating at different security levels.

Does the system prevent unauthorized or unintended information transfer via shared system resources? (e.g., register, main memory, secondary storage)	Y

2.8.5-System and Communication Protection		Communication Protection
Low	100%	Catalog of Recommendations Version 7

The control system protects against or limits the effects of denial-of-service attacks based on an organization's defined list of types of denial-of-service attacks.

Requirement Enhancement 1 - The control system restricts the ability of users to launch denial-of-service attacks against other control systems or networks.

Requirement Enhancement 2 - The control system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

Does the system protect against or limit the effects of denial-of-service attacks based on a defined list of types of denial-of-service attacks?	Y

2.8.7-System and Communication Protection		Communication Protection
Low	100%	Catalog of Recommendations Version 7

The organization defines the external boundaries of the control system. Procedural and policy security functions define the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components. The control system monitors and manages communications at the operational system boundary and at key internal boundaries within the system.

Requirement Enhancement 1 - The organization physically allocates publicly accessible control system components to separate subnetworks with separate, physical network interfaces. Publicly accessible control system components include public web servers. Generally, no control system information should be publicly accessible.

Requirement Enhancement 2 - The organization prevents public access into the organization's internal control system networks except as appropriately mediated.

Requirement Enhancement 3 - The organization limits the number of access points to the control system to allow for better monitoring of inbound and outbound network traffic.

Requirement Enhancement 4 - The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted.

Requirement Enhancement 5 - The control system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

Requirement Enhancement 6 - The organization prevents the unauthorized release of information outside the control system boundary or any unauthorized communication through the control system boundary when an operational failure occurs of the boundary protection mechanisms.

Requirement Enhancement 7 - The organization prevents the unauthorized release of information across managed interfaces.

Requirement Enhancement 8 - The control system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.

Requirement Enhancement 9 - The control system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external systems.

Requirement Enhancement 10 - The control system prevents remote devices that have established connections with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks.

Requirement Enhancement 11 - The control system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.

Requirement Enhancement 12 - The organization selects an appropriate failure mode (e.g., fail open or fail close), depending on the critical needs of system availability.

Are the external boundaries of the system defined?	Y
Are the operational system boundary, the strength required of the boundary, and the respective barriers to unauthorized access and control of system assets and components defined?	Y
Are externally accessible system components physically allocated to separate subnetworks (DMZ) with separate, physical network interfaces?	Y
Is external access into the organization's internal system networks prevented, except as appropriately mediated? (e.g., configuration files and settings, alarm points, passwords, etc.)	Y
Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system?	Y
Are the number of access points to the system limited to allow for better monitoring of inbound and outbound network traffic?	Y
Is the external communication interface connections implemented with security measures appropriate to the required protection of the integrity and confidentiality of the information being transmitted?	Y
Does the system deny network traffic by default and allow network traffic by exception?	Y
Does the system prevent remote devices that have established connections (e.g., PLC, remote laptops) with the system from communicating outside that communications path with resources on uncontrolled/unauthorized networks?	Y

2.8.8-System and Communication Protection		Communication Protection
Moderate	100%	Catalog of Recommendations Version 7

The control system design and implementation protects the integrity of electronically communicated information.

Requirement Enhancement 1 - The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).

Requirement Enhancement 2 - The use of cryptography within a control system will introduce latency to control system communication. The latency introduced from the use of cryptographic mechanisms must not degrade the operational performance of the control system or impact personnel safety.

Requirement Enhancement 3 - Failure of a cryptographic mechanism must not create a denial of service. Control systems generally support the objectives of availability, integrity, and confidentiality. Therefore, the use of cryptography should be determined after careful consideration.

Requirement Enhancement 4 - The control system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.	
Do you encrypt communication over all untrusted communication channels?	Y

2.8.11-System and Communication Protection		Communication Protection
Low	100%	Catalog of Recommendations Version 7

When cryptography is required and employed within the control system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Requirement Enhancement - The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Are cryptographic keys established and managed using automated mechanisms?	Y

2.8.12-System and Communication Protection		Communication Protection
Low	50%	Catalog of Recommendations Version 7

The organization develops and implements a policy governing the use of cryptographic mechanisms for the protection of control system information. The organization ensures all cryptographic mechanisms comply with applicable laws, regulatory requirements, directives, policies, standards, and guidance.

Requirement Enhancement 1 - The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.

Requirement Enhancement 2 - The organization selects cryptographic hardware with remote key management capabilities.

Cryptographic Policy	Y
Do communication cryptographic mechanisms comply with applicable regulatory requirements, policies, standards, and guidance?	N

2.8.18-System and Communication Protection		Communication Protection
Low	100%	Catalog of Recommendations Version 7

All external control system and communication connections are identified and protected from tampering or damage.	
Are all external system and communication connections identified and protected from tampering or damage?	Y

2.8.19-System and Communication Protection		Communication Protection
Low	100%	Catalog of Recommendations Version 7
The control system design and implementation specifies the security roles and responsibilities for the users of the system.		
Does the system design and implementation process define the security roles and responsibilities for the users of the system?		Y

2.8.20-System and Communication Protection		Communication Protection
Moderate	100%	Catalog of Recommendations Version 7
The control system provides mechanisms to protect the authenticity of device-to-device communications sessions. Requirement Enhancement - Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.		
Does the system provide mechanisms to protect the authenticity of device-to-device communications sessions?		Y

2.9.1-Information and Document Management		Information and Document Management
Low	100%	Catalog of Recommendations Version 7
The organization develops, disseminates, and periodically reviews and updates: 1. A formal, documented, control system information and document management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 2. Formal, documented procedures to facilitate the implementation of the control system information and document management policy and associated system maintenance controls.		
Information and Document Management Policy		Y
Information and Document Management Procedure		Y

2.9.6-Information and Document Management		Information and Document Management
Moderate	100%	Catalog of Recommendations Version 7

The organization develops policies and procedures to classify data, including establishing:

1. Retention policies and procedures for both electronic and paper media.

2. Classification policies and methods (e.g., restricted, classified, general).

3. Access and control policies, to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

4. Access to the data based on formally assigned roles and responsibilities for the control system.

Requirement Enhancement - The organization periodically reviews information that requires special control or handling to determine whether such special handling is still required.

Are there policies and procedures for the classification of data, both electronic and paper media?	Y
Do the data policies and procedures establish retention policies and procedures for both electronic and paper media?	Y
Do the data policies and procedures address sharing, copying, transmittal, and distribution appropriate for the level of protection required?	Y
Do the data policies and procedures establish access to the data based on formally assigned roles and responsibilities for the system?	Y

2.9.10-Information and Document Management		Information and Document Management
Moderate	100%	Catalog of Recommendations Version 7

The organization:

1. Marks, in accordance with organizational policies and procedures, removable system media and system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

2. Exempts an organization-defined list of media types or hardware components from marking as long as the exempted items remain within the organization-defined protected environment (e.g., controlled areas).

Is removable system media and system output marked indicating the distribution limitations, handling caveats, and applicable security markings?	Y
Is there a list of media types or hardware components that is exempt from marking as long as the exempted items remain within the organization-defined protected environment?	Y

2.10.3-System Development and Maintenance		Software
Moderate	50%	Catalog of Recommendations Version 7
The organization conducts periodic security vulnerability assessments according to the risk management plan. The control system is then updated to address any identified vulnerabilities in accordance with organization's control system maintenance policy.		
Are periodic security vulnerability assessments conducted according to the risk management plan?		Y
Is the system updated to address any identified vulnerabilities in accordance with the system maintenance policy?		N

2.10.4-System Development and Maintenance		Software
Low	100%	Catalog of Recommendations Version 7
The organization makes and secures backups of critical system software, applications, and data for use if the control system operating system software becomes corrupted or destroyed.		
Are backups of critical system software, applications, and data created and secured?		Y

2.11.1-Security Awareness and Training		Training
Low	50%	Catalog of Recommendations Version 7
The organization develops, disseminates, and periodically reviews and updates:1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. 2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
Awareness and Training Policy		Y
Awareness and Training Procedure		N

2.11.2-Security Awareness and Training		Training
Low	100%	Catalog of Recommendations Version 7
The organization provides basic security awareness training to all control system users (including managers, senior executives, and contractors) before authorizing access to the system, when required by system changes, and at least		

annually thereafter. The effectiveness of security awareness training, at the organization level, needs to be reviewed once a year at a minimum. Requirement Enhancement 1 - All control system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training.Requirement Enhancement 2 - The organization includes practical exercises in security awareness training that simulate actual cyber attacks.	
Is basic security awareness training provided to all system users before authorizing access to the system, when required by system changes and at least annually thereafter?	Y
Is the effectiveness of security awareness training reviewed once a year at a minimum?	Y

2.11.3-Security Awareness and Training		Training
Low	100%	Catalog of Recommendations Version 7
The organization:1. Defines and documents system security roles and responsibilities throughout the system development life cycle. 2. Identifies individuals having system security roles and responsibilities.3. Provides security-related technical training: (a) before authorizing access to the system or performing assigned duties, (b) when required by system changes, and (c) on an organization-defined frequency, thereafter.		
Are individuals with system security roles and responsibilities identified?		Y
Are system security roles and responsibilities defined and documented throughout the system development life cycle, and are the individuals who have these roles and responsibilities identified and trained?		Y
Is security-related technical training provided before authorizing access to the system or performing assigned duties, when required by system changes and on an periodic basis?		Y

2.12.2-Incident Response		Incident Response
Low	100%	Catalog of Recommendations Version 7
The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan. Requirement Enhancement 1 - The continuity of operations plan delineates that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities. Requirement Enhancement 2 - The organization initiates a root cause analysis for the event and submits any findings		

from the analysis to the organizations corrective action program.

Requirement Enhancement 3 - The organization then resumes normal operation of the system in accordance with its policies and procedures.

Continuity of Operations Plan	Y
Does the continuity of operations plan address the issue of maintaining or re-establishing production in case of an undesirable interruption for the system?	Y
Do designated officials review and approve the continuity of operations plan?	Y
Does the continuity of operations plan delineate that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities?	Y
Is a root cause analysis initiated for the security events and any findings from the analysis submitted to the organizations corrective action program?	Y
Is normal operation of the system resumed in accordance with its policies and procedures after a security event?	Y

2.12.7-Incident Response		Incident Response
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

2. Coordinates incident handling activities with contingency planning activities.

3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly.

Requirement Enhancement - The organization employs automated mechanisms to administer and support the incident handling process.

Is an incident handling capability implemented for security incidents that include preparation, detection and analysis, containment, eradication, and recovery?	Y
Are incident handling activities coordinated with contingency planning activities?	Y
Are lessons learned from ongoing incident handling activities incorporated into incident response procedures?	Y
Are automated mechanisms used to administer and support the incident handling process and to assist in the reporting of security incidents?	Y

2.12.15-Incident Response	Incident Response

Moderate	60%	Catalog of Recommendations Version 7

The organization identifies an alternate control center, necessary telecommunications, and initiates necessary agreements to permit the resumption of control system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable.

Requirement Enhancement 1 - The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards.

Requirement Enhancement 2 - The organization identifies potential accessibility problems to the alternate control center in the event of an areawide disruption or disaster and outlines explicit mitigation actions.

Requirement Enhancement 3 - The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

Requirement Enhancement 4 - The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability.

Requirement Enhancement 5 - The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

Are necessary communications for the alternate control center identified, and are agreements in place to permit the resumption of system operations for critical functions within a defined time period when the primary control center is unavailable?	N
Is an alternate control center identified that is geographically separated from the primary control center?	N
Are potential accessibility problems to the alternate control center identified in the event of an area-wide disruption or disaster and are explicit mitigation actions outlined?	Y
Are alternate control center agreements in place that contain priority-of-service provisions in accordance with the availability requirements?	Y
Does the alternate processing site provide information security measures equivalent to that of the primary site?	Y

2.12.16-Incident Response		Incident Response
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Conducts backups of user-level information contained in the system on an organization-defined frequency.

2. Conducts backups of system-level information (including system state information) contained in the system on an organization-defined frequency.

3. Protects the confidentiality and integrity of backup information at the storage location.

Requirement Enhancement 1 - The organization tests backup information periodically to verify media reliability and information integrity.

Requirement Enhancement 2 - The organization selectively uses backup information in the restoration of control system functions as part of contingency plan testing.

Requirement Enhancement 3 - The organization stores backup copies of the operating system and other critical control system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

Are backups of user-level information contained in the system performed on a defined frequency? (user account)	Y
Are backups of system-level information contained in the system performed on a defined frequency?	Y
Is the confidentiality and integrity of backup information protected at the storage location?	Y
Is backup information periodically tested to verify media reliability and information integrity?	Y

2.12.17-Incident Response		Incident Response
Low	50%	Catalog of Recommendations Version 7

The organization provides the capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure.

Requirement Enhancement 1 - The organization implements transaction recovery for systems that are transaction-based (e.g., database management systems).

Requirement Enhancement 2 - The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state.

Requirement Enhancement 3 - The organization provides the capability to re-image system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

Is there a capability to recover and reconstitute the system to a known secure state after a disruption, compromise, or failure?	Y
Is there transaction recovery for systems that are transaction-based?	N

2.13.2-Media Protection		Info Protection
Low	100%	Catalog of Recommendations Version 7

The organization ensures that only authorized users have access to information in printed form or on digital media, whether integral to or removed from the control system.

Requirement Enhancement - The organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted. Note: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media are stored.

Do only authorized users have access to information in printed form or on digital media?	Y
Are automated mechanisms (e.g., card or keypad entry) used to ensure and audit authorized access to media storage areas?	Y

2.13.5-Media Protection		Info Protection
Moderate	100%	Catalog of Recommendations Version 7

The organization physically manages and securely stores control system media within protected areas. The sensitivity of the material delineates how the media are stored.

Is the system media securely stored within protected areas?	Y
Does the sensitivity of the material determine how the media are stored?	Y

2.14.3-System and Information Integrity		System Integrity
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or (b) inserted through the exploitation of system vulnerabilities.

2. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures.

3. Configures malicious code protection mechanisms to: (a) perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed and (b) disinfect and quarantine infected files.

4. Considers using malicious code protection software products from multiple vendors as part of defense-in-depth.

5. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Requirement Enhancement 1 - The organization centrally manages malicious code protection mechanisms.

Requirement Enhancement 2 - The system automatically updates malicious code protection mechanisms (including signature definitions).

Requirement Enhancement 3 - The system prevents users from circumventing host-based malicious code protection capabilities.

Requirement Enhancement 4 - The system updates malicious code protection mechanisms only when directed by a privileged user.

Requirement Enhancement 5 - The organization does not allow users to introduce removable media into the system.

Requirement Enhancement 6 - The system implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly (i.e., block, quarantine, send alert to administrator) when the system encounters data not explicitly allowed by the security policy.

Requirement Enhancement 7 - The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the system.

Are malicious code protection mechanisms used at system entry and exit points and at workstations, servers, or mobile computing devices?	Y
Are malicious code protection mechanisms updated whenever new releases are available in accordance with configuration management policy and procedures?	Y
Are malicious code protection mechanisms configured to perform periodic scans of the system on a defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed, and disinfect and quarantine infected files?	Y
Are malicious code protection software products from multiple vendors used?	Y
Are the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system addressed?	Y
Are malicious code protection mechanisms centrally managed?	Y
Does the system automatically update malicious code protection mechanisms?	Y
Does the system prevent users from circumventing host-based malicious code protection capabilities?	Y
Does the use of mechanisms to centrally manage malicious code protection avoid degradation of the operational performance of the system?	Y

2.14.4-System and Information Integrity		System Integrity
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Monitors events on the system.

2. Detects system attacks.

3. Identifies unauthorized use of the system.

4. Deploys monitoring devices (a) strategically within the system to collect organization-determined essential information and (b) at ad hoc locations within the system to track specific types of transactions of interest to the organization.

5. Heightens the level of system monitoring activity whenever an indication of increased risk exists to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

6. Consults legal counsel with regard to system monitoring activities.

Requirement Enhancement 1 - The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

Requirement Enhancement 2 - In situations where the ICS cannot support the use of automated tools to support near real-time analysis of events, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Requirement Enhancement 3 - The organization employs automated tools to support near real-time analysis of events.

Requirement Enhancement 4 - The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

Requirement Enhancement 5 - The control system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions include the presence of malicious code, the unauthorized export of information, or signaling to an external control system.

Requirement Enhancement 6 - The control system provides a real-time alert when indications of compromise or potential compromise occur.

Requirement Enhancement 7 - The system prevents users from circumventing host-based intrusion detection and prevention capabilities.

Requirement Enhancement 8 - In situations where the ICS cannot prevent nonprivileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Requirement Enhancement 9 - The system notifies a defined list of incident response personnel of suspicious events

and takes a defined list of least disruptive actions to terminate suspicious events.

Requirement Enhancement 10 - The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

Requirement Enhancement 11 - The organization tests/exercises intrusion monitoring tools on a defined time-period.

Requirement Enhancement 12 - The organization makes provisions so that encrypted traffic is visible to system monitoring tools.

Requirement Enhancement 13 - The system analyzes outbound communications traffic at the external boundary of the system and, as deemed necessary, at selected interior points within the system to discover anomalies.

Requirement Enhancement 14 - The use of monitoring tools and techniques must not adversely impact the operational performance of the control system.

Are events on the system monitored?	Y
Are system attacks detected? (Attacks can be detected via log monitoring, IDS system monitoring, Signature/indicators)	Y
Is unauthorized use of the system identified? (e.g., log monitoring)	Y
Are monitoring devices deployed strategically to collect essential information within the system to track specific types of transactions of interest?	Y
Is the level of system monitoring activity heightened whenever an indication of increased risk exists?	Y
Is legal counsel consulted with regard to system monitoring activities?	Y
Are automated tools used to support near real-time analysis of events?	Y
Are automated tools used to integrate intrusion detection tools into access control and flow control mechanisms in support of attack isolation and elimination?	Y
Does the system monitor inbound and outbound communications for unusual or unauthorized activities or conditions?	Y
Does the system provide a real-time alert when indications of compromise or potential compromise occur?	Y
Does the system prevent users from circumventing host-based intrusion detection and prevention capabilities?	Y

2.14.5-System and Information Integrity		System Integrity
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Receives system security alerts, advisories, and directives from designated external organizations on an ongoing basis.

2. Generates internal security alerts, advisories, and directives as deemed necessary.

3. Disseminates security alerts, advisories, and directives to an organization-defined list of personnel.

4. Implements security directives in accordance with timeframes established by the directives, or notifies the issuing organization of the degree of noncompliance. Shutting down and restarting the ICS on the identification of an anomaly are not recommended because the event logs can be erased.

Requirement Enhancement - The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Are system security alerts, advisories, and directives received from designated external organizations on an ongoing basis?	Y
Are internal security alerts, advisories, and directives generated?	Y
Are security alerts, advisories, and directives disseminated to a list of personnel?	Y

2.14.7-System and Information Integrity		System Integrity
Moderate	100%	Catalog of Recommendations Version 7

The system monitors and detects unauthorized changes to software and information.

Does the system monitor and detect unauthorized changes to software and information?	Y
Is the integrity of software and information reassessed by performing, on a defined frequency, integrity scans of the system, and are they used with extreme caution on designated high-availability systems?	Y

2.14.8-System and Information Integrity		System Integrity
Moderate	100%	Catalog of Recommendations Version 7

The organization:

1. Employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.

2. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

3. Considers using spam protection software products from multiple vendors as part of defense-in-depth.

Requirement Enhancement 1 - The organization centrally manages spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on a control system. The use of

mechanisms to centrally managed spam protection must not degrade the operational performance of the system. Requirement Enhancement 2 - The control system automatically updates spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on designated high-availability systems. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the system.

Are spam protection mechanisms used at system entry points and at workstations, servers, or mobile computing devices?	Y
Are spam protection mechanisms updated when new releases are available in accordance with configuration management policy and procedures?	Y
Is spam protection software products from multiple vendors used?	Y

2.15.1-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The organization develops, disseminates, and periodically reviews and updates:

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Requirement Enhancement 1 - Public access to ICS is not permitted.

Requirement Enhancement 2 - Business IT and general corporation access to the ICS is not permitted.

Access Control Policy	Y
Access Control Procedure	Y

2.15.3-Access Control		Access Control
Low	87%	Catalog of Recommendations Version 7

The organization manages system accounts, including:

1. Identifying account types (i.e., individual, group, and system).

2. Establishing conditions for group membership.

3. Identifying authorized users of the system and specifying access rights and privileges.

4. Requiring appropriate approvals for requests to establish accounts.

5. Authorizing, establishing, activating, modifying, disabling, and removing accounts.

6. Reviewing accounts on a defined frequency.

7. Specifically authorizing and monitoring the use of guest/anonymous accounts.

8. Notifying account managers when system users are terminated, transferred, or system usage or need -to-know/need-to-share changes.

9. Granting access to the system based on a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage.

Requirement Enhancement 1 - The organization employs automated mechanisms to support the management of system accounts.

Requirement Enhancement 2 - The system automatically terminates temporary and emergency accounts after a defined time period for each type of account.

Requirement Enhancement 3 - The system automatically disables inactive accounts after a defined time period.

Requirement Enhancement 4 - The system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

Requirement Enhancement 5 - The organization reviews currently active system accounts on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.

Requirement Enhancement 6 - The organization prohibits the use of system account identifiers as the identifiers for user electronic mail accounts.

Are system accounts identified by account type and managed?	Y
Do system accounts have conditions for group membership?	Y
Are the access rights and privileges specified, and are authorized users identified for system accounts?	Y
Are appropriate approvals required for requests to establish accounts?	Y
Are system accounts authorized, established, activated, modified, disabled, and removed?	Y
Are system accounts reviewed on a defined frequency?	Y
Is the use of guest/anonymous accounts specifically authorized and monitored?	Y
Are account managers notified when system users are terminated; transferred, or system usage or need-to-know/need-to-share changes?	Y
Is access to the system granted based on a valid need-to-know or need-to-share as determined by official duties and satisfying all security criteria?	Y
Are automated mechanisms such as active directory used to support the management of system accounts?	N

Does the system automatically terminate temporary and emergency accounts after a defined time period for each type of account?	N
Does the system automatically disable inactive accounts after a defined time period?	Y
Does the system automatically audit account creation, modification, disabling, and termination actions and notify appropriate individuals?	Y
Are currently active system accounts reviewed on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated?	Y
Are user account names different than email user accounts?	Y

2.15.4-Access Control		Access Control
Low	0%	Catalog of Recommendations Version 7

The organization manages system identifiers for users and devices by:

1. Receiving authorization from a designated organizational official to assign a user or device identifier.

2. Selecting an identifier that uniquely identifies an individual or device.

3. Assigning the user identifier to the intended party or the device identifier to the intended device.

4. Archiving previous user or device identifiers.

Is there an official assigned to authorize a user or device identifier?	N
Are identifiers selected that uniquely identify an individual or device?	N
Are the user identifiers assigned to the intended party or the device identifier to the intended device?	N
Are previous user or device identifiers archived?	N

2.15.5-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The organization manages system authenticators for users and devices by:

1. Verifying, as part of the initial authenticator distribution for a user authenticator, the identity of the individual receiving the authenticator.

2. Establishing initial authenticator content for organization-defined authenticators.

3. Ensuring that authenticators have sufficient strength of mechanism for their intended use.

4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.

5. Changing default content of authenticators upon system installation.

6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate).

7. Changing or refreshing authenticators periodically, as appropriate for authenticator type.

8. Protecting authenticator content from unauthorized disclosure and modification.

9. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Requirement Enhancement 1 - The system, for PKI-based authentication:a. Validates certificates by constructing a certification path with status information to an accepted trust anchor.b. Enforces authorized access to the corresponding private key.c. Maps the authenticated identity to the user account. Note: Status information for certification paths includes certificate revocation lists or online certificate status protocol responses.

Requirement Enhancement 2 - The organization requires that the registration process to receive a user authenticator be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

Requirement Enhancement 3 - The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.

Requirement Enhancement 4 - The organization requires unique authenticators be provided by vendors and manufacturers of system components.

Is there a mechanism in place to verify the identity whenever an authenticator (password, token) is created, distributed, or modified?	Y
Do authenticators have sufficient strength of mechanism for their intended use?	Y
Are there administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators? (e.g., passwords, tokens, cards, etc.)	Y
Is the default content of authenticators changed on system installation?	Y
Are there minimum and maximum lifetime restrictions and reuse conditions for authenticators?	Y
Are authenticators changed or refreshed periodically as appropriate for authenticator type?	Y
Is authenticator content protected from unauthorized disclosure and modification? (i.e., not transmitting over email as open text)	Y
Are users required to take, and devices implement, specific measures to safeguard authenticators?	Y
Are certificates validated for PKI-based authentication by constructing a certification path with status information to an accepted trust anchor?	Y
Is the registration process to receive a user authenticator carried out in person before a designated registration authority?	Y
Does the system enforce authorized access to the corresponding private key for PKI-based authentication?	Y
Does the system map the authenticated identity to the user account for PKI-based authentication?	Y

2.15.7-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The control system enforces assigned authorizations for controlling logical access to the system in accordance with applicable policy.

Requirement Enhancement 1 - The system enforces dual authorization, based on organizational policies and procedures for organization-defined privileged commands. Note: The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.

Requirement Enhancement 2 - The system enforces one or more organization-defined nondiscretionary access control policies over organization-defined set of users and resources where the policy rule set for each policy specifies:a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day).b. Required relationships among the access control information to permit access. Note: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, and Originator Controlled Access Control.

Requirement Enhancement 3 - The system prevents access to organization-defined security-relevant information except during secure, nonoperable system states. Note: Security relevant information is any information within the system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, nonoperable system states are states in which the system is not performing mission/business-related processing (e.g., the system is offline for maintenance, troubleshooting, bootup, shutdown).

Does the system enforce assigned authorizations for controlling electronic access to the system?	Y

2.15.8-Access Control		Access Control
Moderate	100%	Catalog of Recommendations Version 7

The organization:

1. Establishes division of responsibilities and separates duties of individuals as necessary to eliminate conflicts of interest.

2. Implements separation of duties through assigned system access authorizations.

Is there a division of responsibilities and separation of duties of individuals to eliminate conflicts of interest?	Y

Is the separation of duties implemented through assigned system access authorizations?	Y

2.15.9-Access Control		Access Control
Moderate	100%	Catalog of Recommendations Version 7

The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users), as necessary, to accomplish assigned tasks.

Requirement Enhancement 1 - The organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information. Note: Explicitly authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.

Requirement Enhancement 2 - The organization requires that users of system accounts with access to organization-defined list of security functions or security-relevant information, use nonprivileged accounts when accessing other system functions, and if feasible, audits any use of privileged accounts for such functions.

Requirement Enhancement 3 - The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the system.

Is the concept of least privilege used to accomplish assigned tasks?	Y
Is access to a defined list of security functions and security-relevant information explicitly authorized?	Y
Are users of system accounts with access to a defined list of security functions or security-relevant information required to use nonprivileged accounts when accessing other system functions?	Y

2.15.10-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Requirement Enhancement 1 - The system employs multifactor authentication for remote access and for access to privileged accounts.

Requirement Enhancement 2 - The system employs multifactor authentication for network access and for access to privileged accounts.

Requirement Enhancement 3 - The system employs multifactor authentication for local and network access.	
Does the system uniquely identify and authenticate organizational users?	Y
Does the system employ multifactor authentication for remote access?	Y
Does the system employ multifactor authentication for network access and for access to privileged accounts?	Y

2.15.14-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The control system employs authentication methods that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Requirement Enhancement - Failure of cryptographic module authentication must not create a denial of service or adversely impact the operational performance of the control system.

Does the system employ authentication methods that meet the requirements of applicable policies, standards, and guidance for authentication to a cryptographic module?	Y
If your authentication encryption module fails can you still authenticate without creating a denial of service that impacts operational performance of system?	Y

2.15.16-Access Control		Access Control
Low	50%	Catalog of Recommendations Version 7

The organization develops and enforces policies and procedures for control system users concerning the generation and use of passwords. These policies stipulate rules of complexity, based on the criticality level of the systems to be accessed.

Requirement Enhancement - ICS deployment will require two-factor authentication or comparable compensating measures to ensure only approved authorized access is allowed

Are there policies and procedures concerning the generation and use of passwords?	Y
Do the password policies stipulate rules of complexity, based on the criticality level of the systems to be accessed?	N

2.15.21-Access Control	Access Control

Moderate	100%	Catalog of Recommendations Version 7

The system:

1. Prevents further access to the system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user.

2. Retains the session lock until the user re-establishes access using appropriate identification and authentication procedures.

Requirement Enhancement - The system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.

Does the system prevent further access to the system by initiating a session lock after a defined time period of inactivity or a user initiated session lock?	Y
Does the system retain the session lock until the user re-establishes access using appropriate identification and authentication procedures?	Y

2.15.22-Access Control		Access Control
Moderate	100%	Catalog of Recommendations Version 7

The system terminates a network connection at the end of a session or after an organization-defined time period of inactivity.

Requirement Enhancement - Automatic session termination applies to local and remote sessions. The control system terminates a network connection at the end of a session or after a period of inactivity per organization policy and procedures.

Does the system terminate a network connection at the end of a session or after a defined time period of inactivity?	Y

2.15.23-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Documents allowed methods of remote access to the system.

2. Establishes usage restrictions and implementation guidance for each allowed remote access method. 3. Authorizes remote access to the system prior to connection. 4. Enforces requirements for remote connections to the system.

Are allowed methods of remote access to the system documented?	Y
Are there usage restrictions and implementation guidance for each allowed remote access method?	Y
Does remote access to the network require authentication prior to system connection?	Y
Are the requirements for remote connections to the system enforced?	Y

2.15.24-Access Control		Access Control
Low	80%	Catalog of Recommendations Version 7

The organization authorizes, monitors, and manages all methods of remote access to the control system.

Requirement Enhancement 1 - The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Requirement Enhancement 2 - The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. Note: The encryption strength of mechanism is selected based on the FIPS 199 impact level of the information.

Requirement Enhancement 3 - The system routes all remote accesses through a limited number of managed access control points.

Requirement Enhancement 4 - The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the system.

Requirement Enhancement 5 - The system protects wireless access to the system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary.

Requirement Enhancement 6 - The organization monitors for unauthorized remote connections to the system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered. Note: Organizations proactively search for unauthorized remote connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to those areas within the facility containing the systems. Yet, the scan is conducted outside those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

Requirement Enhancement 7 - The organization disables, when not intended for use, wireless networking capabilities

internally embedded within system components prior to issue.

Requirement Enhancement 8 - The organization does not allow users to independently configure wireless networking capabilities.

Requirement Enhancement 9 - The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

Requirement Enhancement 10 - The organization ensures that remote sessions for accessing an organization-defined list of security functions and security-relevant information employ additional security measures (organization defined security measures) and are audited.

Requirement Enhancement 11 - The organization disables peer-to-peer wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.

Requirement Enhancement 12 - The organization disables Bluetooth wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.

Are all the methods of remote access to the system authorized, monitored, and managed?	Y
Are automated mechanisms used to facilitate the monitoring and control of remote access methods?	Y
Is cryptography used to protect the confidentiality and integrity of remote access sessions?	Y
Does the system route all remote accesses through a limited number of managed access control points?	Y
Is remote access for privileged commands and security-relevant information authorized only for compelling operational needs and is the rationale for such access documented?	N
Is Bluetooth wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?	Y
Does the system protect wireless access using authentication and encryption?	Y
Are unauthorized remote connections to the system monitored, including scanning for unauthorized mobile or wireless access points on a defined frequency and is appropriate action taken if an unauthorized connection is discovered?	N
Do you employ rigorous security measures for remote sessions with administrative privileges and are they audited?	Y
Is peer-to-peer wireless networking capability disabled except for explicitly identified components in support of specific operational requirements?	Y

2.15.26-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Eestablishes use restrictions and implementation guidance for wireless technologies.

2. Authorizes, monitors, and manages wireless access to the control system.

Requirement Enhancement 1 - The organization uses authentication and encryption to protect wireless access to the control system. Any latency induced from the use of encryption must not degrade the operational performance of the control system.

Requirement Enhancement 2 - The organization scans for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact control systems. The scan is not limited to only those areas within the facility containing the high-impact control systems.

Are there use restrictions and implementation guidance for wireless technologies?	Y
Is wireless access to the system authorized, monitored, and managed?	Y
Is authentication and encryption used to protect wireless access to the system and the latency induced does NOT degrade the operational performance of the system?	Y
Is the system scanned for unauthorized wireless access points at a specified frequency, and is appropriate action taken if such access points are discovered?	Y
Is there a thorough scan for unauthorized wireless access points in facilities containing high-impact systems?	Y

2.15.28-Access Control		Access Control
Low	100%	Catalog of Recommendations Version 7

The organization employs mechanisms in the design and implementation of a control system to restrict public access to the control system from the organization's enterprise network.

Are there mechanisms in the design and implementation of the system to restrict access to the system from the enterprise network? (firewall, DMZ, VPN)	Y

2.16.2-Audit and Accountability		Audit and Accountability
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Determines, based on a risk assessment in conjunction with mission/business needs, which system-related events require auditing (e.g., an organization-defined list of auditable events and frequency of [or situation requiring] auditing for each identified auditable event).

2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

3. Ensures that auditable events are adequate to support after-the-fact investigations of security incidents.

4. Adjusts, as necessary, the events to be audited within the system based on current threat information and ongoing assessments of risk.

Requirement Enhancement 1 - The organization reviews and updates the list of organization-defined auditable events on an organization-defined frequency.

Requirement Enhancement 2 - The organization includes execution of privileged functions in the list of events to be audited by the system.

Is there a frequency of auditing for each identified auditable event?	Y
Is the security audit function coordinated with other organizational entities requiring audit-related information?	Y
Are auditable events adequate to support after-the-fact investigations of security incidents?	Y
Are the events to be audited adjusted within the system based on current threat information and ongoing assessments of risk?	Y
Is the list of defined auditable events reviewed and updated on a defined frequency?	Y
Is execution of privileged functions (account creations, modifications, and object permission changes) included in the list of events to be audited by the system?	Y

2.16.6-Audit and Accountability		Audit and Accountability
Low	100%	Catalog of Recommendations Version 7

The organization:

1. Reviews and analyzes system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to designated organizational officials.

2. Adjusts the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

Requirement Enhancement 1 - The system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.

Requirement Enhancement 2 - The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Requirement Enhancement 3 - The system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.

Requirement Enhancement 4 - The organization integrates analysis of audit records with analysis of performance and network monitoring information to enhance further the ability to identify inappropriate or unusual activity.	
Are system audit records reviewed and analyzed on a defined frequency, and are findings reported to designated officials?	Y
Is the level of audit review, analysis, and reporting within the system adjusted when a change in risk exists?	Y

2.18.2-Risk Management and Assessment		Risk Management and Assessment
Low	100%	Catalog of Recommendations Version 7
The organization develops a risk management plan. A senior organization official reviews and approves the risk management plan.		
Has a risk management plan been developed?		Y
Does a senior official review and approve the risk management plan?		Y

2.18.5-Risk Management and Assessment		Risk Management and Assessment
Low	50%	Catalog of Recommendations Version 7
The organization: 1. Authorizes all connections from the system to other systems outside the authorization boundary through the use of system connection agreements. 2. Documents the system connections and associated security requirements for each connection. 3. Monitors the system connections on an ongoing basis verifying enforcement of documented security requirements.		
Does the security plan describe the relationships with or connections to other systems?		Y
Are the system connections monitored on an ongoing basis verifying enforcement of documented security requirements?		N

2.18.11-Risk Management and Assessment		Risk Management and Assessment
Low	100%	Catalog of Recommendations Version 7
The organization:		

1. Scans for vulnerabilities in the system on an organization-defined frequency and randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system are identified and reported.

2. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent checklists and test procedures; and (c) measuring vulnerability impact.

3. Analyzes vulnerability scan reports and remediates legitimate vulnerabilities within a defined timeframe based on an assessment of risk.

4. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other systems.

Requirement Enhancement 1 - The organization employs vulnerability scanning tools that include the capability to readily update the list of system vulnerabilities scanned.

Requirement Enhancement 2 - The organization updates the list of system vulnerabilities scanned on an organization-defined frequency or when new vulnerabilities are identified and reported.

Requirement Enhancement 3 - The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., system components scanned and vulnerabilities checked).

Requirement Enhancement 4 - The organization attempts to discern what information about the system is discoverable by adversaries.

Requirement Enhancement 5 - The organization performs security testing to determine the level of difficulty in circumventing the security controls of the system.

Requirement Enhancement 6 - The organization includes privileged access authorization to organization-defined system components for selected vulnerability scanning activities to facilitate more thorough scanning.

Requirement Enhancement 7 - The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.

Requirement Enhancement 8 - The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational systems and notify designated organizational officials.

Are periodic security vulnerability assessments conducted according to the risk management plan?	Y
Are vulnerability scans performed for in the system on a defined frequency and randomly in accordance with company policy?	Y
Are vulnerability scanning tools and techniques used that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent, checklists, and test procedures; and (c) measuring vulnerability impact?	Y

Is information obtained from the vulnerability scanning process shared with designated personnel throughout the organization?	Y
Are vulnerability scanning tools used that include the capability to readily update the list of system vulnerabilities scanned?	Y

2.18.12-Risk Management and Assessment		Risk Management and Assessment
Low	100%	Catalog of Recommendations Version 7
The organization identifies, classifies, prioritizes, and analyzes potential security threats, vulnerabilities, and consequences to their control systems assets using accepted methodologies.		
Are potential security threats, vulnerabilities, and consequences identified, classified, prioritized, and analyzed using accepted methodologies?		Y

2.19.2-Information Security Program Plan		Organizational
Low	100%	Catalog of Recommendations Version 7
The organization appoints a senior security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.		
Is a senior security officer appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program?		Y

2.19.5-Information Security Program Plan		Organizational
Low	100%	Catalog of Recommendations Version 7
The organization develops and maintains an inventory of its systems and critical components.		
Is there an inventory of systems and critical components and is it maintained?		Y

2.19.7-Information Security Program Plan		Organizational
Low	100%	Catalog of Recommendations Version 7
The organization develops an enterprise architecture with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation.		
Is the enterprise architecture developed with consideration for security and the resulting risk?		Y