Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*	Awareness & Training	PR.AT-1	All users are informed and trained	AT-1, AT-2
		PR.AT-2	Privileged users understand roles & responsibilities	AT-1, AT-2
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	AT-2
		PR.AT-4	Senior executives understand roles & responsibilities	AT-1
		PR.AT-5	Physical and information security personnel understand roles & responsibilities	PS-4, AT-1
	Data Security	PR.DS-1	Data-at-rest is protected	PM-5, MP-2
		PR.DS-2	Data-in-transit is protected	PM-4, SC-14, SC-23, SC-24
		PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	PM-1
		PR.DS-4	Adequate capacity to ensure availability is maintained	MA-1, CM-7
		PR.DS-5	Protections against data leaks are implemented	IA-4
		PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	IR-3
		PR.DS-7	The development and testing environment(s) are separate from the production environment	CM-4
	Information Protection Processes and Procedures (IP)	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained	SA-3
		PR.IP-2	A System Development Life Cycle to manage systems is implemented	CM-1, CM-6
		PR.IP-3	Configuration change control processes are in place	SA-3
		PR.IP-4	Backups of information are conducted, maintained, and tested periodically	SA-5
		PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	PE-4
		PR.IP-6	Data is destroyed according to policy	MP-1
		PR.IP-7	Protection processes are continuously improved	AU-6
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	AU-7
		PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	ANSI/AWWA J100/G440/M19
		PR.IP-10	Response and recovery plans are tested	PS-4

Function	Category	Sub-Category	Description	AWWA Guidance Control
PROTECT – *cont.*		PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	AT-2
		PR.IP-12	A vulnerability management plan is developed and implemented	AU-5
	Maintenance	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	MA-1
		PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-1
	Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PM-3
		PR.PT-2	Removable media is protected and its use restricted according to policy	MP-1
		PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality (whitelisting)	SC-10, SC-19
		PR.PT-4	Communications and control networks are protected	IA-7
DETECT	Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	Not addressed
		DE.AE-2	Detected events are analyzed to understand attack targets and methods	SC-5
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors	Not addressed
		DE.AE-4	Impact of events is determined	PM-3
		DE.AE-5	Incident alert thresholds are established	CM-7
	Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events	CM-7
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	PE-1, CM-7
		DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	CM-7, SA-5
		DE.CM-4	Malicious code is detected	SC-5
		DE.CM-5	Unauthorized mobile code is detected	SA-4
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	IA-2
		DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	PS-1
		DE.CM-8	Vulnerability scans are performed	IR-2
	Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability and adequate awareness of anomalous events	PS-2
		DE.DP-2	Detection activities comply with all applicable requirements	IR-3

Function	Category	Sub-Category	Description	AWWA Guidance Control
DETECT – *cont.*		DE.DP-3	Detection processes are tested	ANSI/AWWA G430, G440
		DE.DP-4	Event detection information is communicated to appropriate parties	IA-2
		DE.DP-5	Detection processes are continuously improved	SC-4
RESPOND	Response Planning	RS.PL-1	Response plan is executed during or after an event	AT-1
	Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed	ANSI/AWWA G430, G440
		RS.CO-2	Events are reported consistent with established criteria	G430
		RS.CO-3	Information is shared consistent with response plans	SC-6
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans	ANSI/AWWA G430, G440
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	MA-2
	Analysis	RS.AN-1	Notifications from detection systems are investigated	SC-5
		RS.AN-2	The impact of the incident is understood	ANSI/AWWA J100
		RS.AN-3	Forensics are performed	AT-3
		RS.AN-4	Incidents are categorized consistent with response plans	AT-3
	Mitigation	RS.MI-1	Incidents are contained	IR-1
		RS.MI-2	Incidents are mitigated	IR-1
		RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	IR-2
	Improvements	RS.IM-1	Response plans incorporate lessons learned	ANSI/AWWA G430, G440
		RS.IM-2	Response strategies are updated	ANSI/AWWA G430, G440
RECOVER	Recovery Planning	RC.RP-1	Recovery plan is executed during or after an event restoration of systems or assets affected by cybersecurity events	AU-7
	Improvements	RC.IM-1	Recovery plans incorporate lessons learned	ANSI/AWWA G430, G440
		RC.IM-2	Recovery strategies are updated	ANSI/AWWA G430, G440
	Communications	RC.CO-1	Public relations are managed	ANSI/AWWA G430, G440
		RC.CO-2	Reputation after an event is repaired	ANSI/AWWA G430, G440
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	ANSI/AWWA G430, G440

NOTES

NOTES

About AWWA

AWWA is an international, nonprofit, scientific and educational society dedicated to providing total water solutions assuring the effective management of water. Founding 1881, the Association is the largest organization of water supply professionals in the world. Our membership includes nearly 4,200 utilities that supply roughly 80 percent of the nation's drinking water and treat almost half of the nation's wastewater. Our over 50,000 total memberships represent the full spectrum of the water community: public water and wastewater systems, environmental advocates, scientists, academicians, and others who hold a genuine interest in water, our most important resource. AWWA unites the diverse water community to advance public health, safety, the economy, and the environment.

Appendix L

CATALOG OF RECOMMENDATIONS

Catalog of Control Systems Security: Recommendations for Standards Developers

April 2011

Homeland Security

Control Systems Security Program

National Cyber Security Division

ACKNOWLEDGMENT

This document was developed by the U.S. Department of Homeland Security to help facilitate the development of control systems cybersecurity industry standards. The original author team consisted of representatives from the Department of Homeland Security Control Systems Security Program (CSSP), National Institute of Standards and Technology (NIST), Argonne National Laboratory (ANL), Idaho National Laboratory (INL), Oak Ridge National Laboratory (ORNL), Pacific Northwest National Laboratory (PNNL), and Sandia National Laboratories (SNL).

For additional information or comments, please send inquires to the Control Systems Security Program at cssp@hq.dhs.gov with the word "Catalog" in the subject line.

EXECUTIVE SUMMARY

This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalog are grouped into 19 families, or categories, that have similar emphasis. The recommendations within each family are displayed with a summary statement of the recommendation, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the recommendation under special situations.

This catalog is not limited for use by a specific industry sector. All sectors can use it to develop a framework needed to produce a sound cybersecurity program. The number of new and updated published Cyber Security Standards and guidelines has increased significantly this past year. An attempt has been made to reference and include the best practices introduced by these new and updated documents to interested users for consideration as input into individual industrial cybersecurity plans under development and review. This catalog should be viewed as a collection of guidelines and recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cybersecurity standards for control systems. The recommendations in this catalog are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cybersecurity standards specific to their individual security needs. These recommendations are subservient to existing legal rules and regulations pertaining to specific industry sectors, and the user is urged to consult and follow those applicable regulations.

CONTENTS

TABLES

ACRONYMS

AC	access control
AGA	American Gas Association
AT	awareness and training
AU	audit and accountability
CA	security assessment and authorization
CAG	consensus audit guidelines
CC	critical control
CD	compact disc
CIKR	critical infrastructures and key resources
CIP	critical infrastructure protection
CM	Configuration Management
CP	Contingency Planning
DHS	Department of Homeland Security
DNS	Domain Name System
DOE	Department of Energy
DVD	digital video disc
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IA	identification and authenticity
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	IP Security
IPS	intrusion prevention system
IR	incident response
ISA	International Society of Automation
ISO	International Organization for Standardization

IT	information technology
Key	cryptographic key
MA	System Development and Maintenance
MP	media protection
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OSI	Open System Interconnection
PDF	portable document file
PE	physical and environmental protection
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PL	planning
PM	program management
PS	personnel security
RA	risk assessment
RFID	radio frequency identification
RG	regulatory guide
SA	system and services acquisition
SC	System and communications protection
SCADA	Supervisory Control and Data Acquisition
SD	secure digital memory card
SI	system and information integrity
SP	Special Publication
TCB	Trusted Computing Base
UHF	ultra high frequency
USB	universal serial bus
US-CERT	United States Computer Emergency Readiness Team
VHF	very high frequency
VoIP	Voice-Over Internet Protocol
VPN	Virtual Private Network

Catalog of Control Systems Security: Recommendations for Standards Developers

1. INTRODUCTION

Protecting critical infrastructures and key resources (CIKR) is essential to the security, public health and safety, economic vitality, and way of life for our nation's citizens. Fundamental to the protection of CIKR is ensuring the security of the systems that control these infrastructures. Developing and applying robust security standards enables control systems to be secure.

Development of security standards specific to CIKR control systems is maturing. However, many standards lack the detailed guidance needed to ensure adequate protection from the emerging threats of cyber attacks on control systems. This catalog of recommended security controls is specifically designed to provide various industry sectors the framework needed to develop sound security standards, guidelines, and best practices. These recommendations are not intended to replace the need for applying sound engineering judgment, best practices, and risk assessments. Decisions regarding when, where, and how these standards should be used are best determined by the specific industry sectors. This document provides those decision-makers with a common catalog (framework) from which to select security controls for control systems.

The term "control systems," as used throughout this document, includes supervisory control and data acquisition systems, process control systems, distributed control systems, and other control systems specific to any of the critical infrastructure industry sectors. Although differences in these systems exist, their similarities enable a common framework for discussing and defining security controls. Currently, control system security standards and guidelines are being created by a variety of Standards Development Organizations to meet the needs of different industry sectors and regulatory environments. However, the standards produced for a specific sector may not always be consistent, compatible, or comparable with similar standards developed in another sector. These developing standards often have differing priorities, emphases, and levels of detail concerning specific security controls based on specific industrial acceptable risks and regulations.

This document attempts to encompass these differences and provide a way to clarify security programs for similar control systems. Use of this document is not limited to a specific industry sector. This catalog should be viewed as a collection of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cybersecurity standards for control systems. While many of the documents referenced in the preparation of this catalog are still in draft or do not apply directly to control systems, they still supply information useful for the security of control systems.

Throughout the development of this document, the following aspects of control systems were considered:

- **Proprietary Control System Technology**—A large percentage of deployed control system hardware and software is proprietary. However, some vendors are moving toward marketing products that use nonproprietary, commercial off-the-shelf technologies, as these newer systems provide more functions, with better efficiency, costs (acquisition, operation, and maintenance), and effectiveness. Control system networks also may use proprietary or industry-specific protocols. The proprietary nature of installed control systems currently requires professionals with system-specific knowledge to operate them, but that is slowly changing as older systems get replaced and upgraded.
- **Control System Equipment Life Cycle**—The life cycle for control system hardware is from 5 to 15 years (or more) as compared to the 2 to 3-year (or shorter) life cycle for information technology (IT) business systems. Building security into control system equipment is a recent development.

Typically, legacy control systems do not contain the standard security functionality included in many IT systems such as cryptography or auditing.

- **Real Time Operation**—The systems that control CIKR are designed and constructed to be in operation continuously. Any interruption in service may have catastrophic results to human life and property. This is a key difference between control systems and IT business systems. Real time operation presents a unique challenge for securing these systems because security cannot compromise the reliable operation of the control system.

The goal of a control systems security program is to balance security while operating within resource limits. When developing a security policy to address control systems, these characteristics must be considered. Security is not meant to impede operation and should be as transparent as possible. The most successful security program is one that integrates seamlessly and becomes a common aspect of daily operation. The intent of this document is to help facilitate such a program.

2. RECOMMENDATIONS FOR STANDARDS DEVELOPERS

This section contains a detailed listing of recommended controls from several sources. The organization of each recommendation is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, but modified to convey control system language. The recommended controls are organized into families primarily based on NIST SP 800-53 and include contributions from "Key Elements to a Cyber Security Management System," (Clause 5) found in the Draft Instrumentation, Systems, and Automation Society (ISA)-d9900.02 document. The families have been realigned from the format of NIST SP 800-53, Revision 3 to facilitate the security management of the control system environments. However, all the families addressed in NIST SP 800-53, Revision 3 are also addressed in this document. A cross-reference of the subsections below in Section 2 and the NIST SP 800-53, Revision 3 families is provided in Table 1. Table 1 demonstrates that this document expands on the NIST SP 800-53, Revision 3 families by adding subsections addressing *Security Policy*, *Organizational Security*, *Information and Document Management*, and *Monitoring and Reviewing Control System Security Policy* to provide a comprehensive catalog of control systems security recommendations.

Table 1. Catalog of Recommendations and NIST SP 800-53 comparison.

Catalog of Recommendations Subsections	NIST SP 800-53 Revision 3 Families
2.1 Security Policy	Each of the 18 control family initial elements relates to its own policy and procedures (e.g., AC- 1 through PM-1)
2.2 Organizational Security	Access Control—AC Program Management—PM
2.3 Personnel Security	Access Control—AC Personnel Security—PS
2.4 Physical and Environmental Security	Access Control—AC Physical and Environmental Security—PE
2.5 System and Services Acquisition	System and Services Acquisition—SA
2.6 Configuration Management	Configuration Management—CM
2.7 Strategic Planning	Planning—PL
2.8 System and Communication Protection	Access Control—AC System and Communication Protection—SC
2.9 Information and Document Management	Contingency Planning—CP Media Protection—MP
2.10 System Development and Maintenance	Maintenance—MA
2.11 Security Awareness and Training	Awareness and Training—AT
2.12 Incident Response	Incident Response—IR
2.13 Media Protection	Media Protection—MP
2.14 System and Information Integrity	System and Information Integrity—SI
2.15 Access Control	Access Control—AC Identification Authentication—IA
2.16 Audit and Accountability	Audit and Accountability—AU

Table 1. (continued).

Catalog of Recommendations Subsections	NIST SP 800-53 Revision 3 Families
2.17 Monitoring and Reviewing Control System Security Policy	Security Assessment and Authorization—CA
2.18 Risk Management and Assessment	Assessment and Authorization—CA Risk Assessment—RA
2.19 Security Program Management	Program Management—PM

This DHS catalog contains 250 recommended controls compared to 347 controls defined in NIST SP 800-53 Revision 3. Of these controls, seven catalog of recommendation controls are not specifically addressed in NIST SP 800-53 Revision 3. NIST SP 800-53 Revision 3 does not ignore these seven controls; rather, they are implied within several other control families. This change is reflective of the increased granularity for each control element within the NIST document. The new consensus audit guidelines (CAG) and regulatory guide (RG) 5.71 guidelines also follow this trend. As an example, catalog of recommendation control element 2.9.8, "Document Destruction," addresses document retention and destruction. However, areas, such as visitor control, incident management, and configuration management, require different document retention and destruction requirements and policies. Other areas, such as roles and responsibilities and access control, are also broken down and inserted as needed into control elements to assist the user to understand and effectively deploy the security control being discussed.

The "Requirement" section for each security control includes detailed recommended security practices and mechanisms. The "Supplemental Guidance" section provides additional information that may be beneficial for understanding and implementing the recommendation. The last section, "Requirement Enhancements," includes supplementary security constraints for the recommendation that will result in a more secure environment based on the organization's predetermined level of protection required for the control system used for the critical process. Not all the recommendations are appropriate for all applications, so it will be necessary to determine the level of protection needed and only apply the guidance as appropriate. Industrial controls have an availability requirement that may require compensating controls instead of following the recommendations (see Appendix I of NIST SP 800-53 Revision 3, "Industrial Control Systems"). A few examples of these areas may be password, multiple session, and patch management controls where interference with operations becomes unacceptable because of operational requirements, testing, and certification requirements (e.g., substation automation, certain refinery operations, flight controls). The following recommendations were obtained from a review of the controls found in various industry standards. Similar controls were identified, and a single recommendation was prepared that addressed the intent of the original controls. Appendix A presents a cross reference of standards and guidelines used to develop these recommendations.

2.1 Security Policy

Security policies are the specific controls and behavior expectations that each member of the organization's staff is required to meet in the daily operation of the control system. The development of the organization's security policy is the first and most important step in developing an organizational security program. Security policies lay the groundwork for securing the organization's physical, enterprise, and control system assets. Security procedures define how an organization implements the security policy. Using a predefined security policy best practices guide can help the organization to develop a cogent security policy.

2.1.1 Security Policy and Procedures

2.1.1.1 Requirement

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.

2.1.1.2 Supplemental Guidance

The security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the control system in particular, when required.

2.1.1.3 Requirement Enhancements

None

2.1.1.4 References

NIST SP 800-53r3	AC-1, SC-14, PM-1
CAG	CC-9
API 1164r2	4, 5.5, 7.1.3, Annex A, Annex B.4.1.2
NERC CIPS	CIP 003-3, B.R1
NRC RG 5.71	App. A.2, App. B.1.1

2.2 Organizational Security

Organizational security involves setting organization-wide policies and procedures that define acceptable behavior and practices concerning security. Organizational security includes management accountability, physical controls, and cyber-related functions. Organizational policies and procedures specify direction, commitment, responsibility, and oversight and define the security posture for the control system. These policies and procedures also apply to third-party contractors, integrators, and vendors used by the organization.

2.2.1 Management Policy and Procedures

2.2.1.1 Requirement

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

2.2.1.2 Supplemental Guidance

The scope and responsibilities of the security program include management accountability, physical security, and information security for the enterprise and control systems. This program applies to third-party contractors, outsourcing partners, and the supply chain components of the organization.

2.2.1.3 Requirement Enhancements

None

2.2.1.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2, Annex A, Annex B.4.1.2
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. B.3.11

2.2.2 Management Accountability

2.2.2.1 Requirement

The organization defines a framework of management leadership accountability. This framework establishes roles and responsibilities to approve cybersecurity policy, assign security roles, and coordinate the implementation of cybersecurity across the organization**.**

2.2.2.2 Supplemental Guidance

This framework is not limited to traditional IT systems but also extends to control systems and the organization's supply chain.

2.2.2.3 Requirement Enhancements

None

2.2.2.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2
NERC CIPS	CIP 003-3, B.R2, B.R5

2.2.3 Baseline Practices

2.2.3.1 Requirement

Baseline practices that organizations employ for organizational security include, but are not limited to:

1. Executive management accountability for the security program.
2. Responsibility for control system security within the organization includes sufficient authority and an appropriate level of funding to implement the organization's security policy.
3. The organization's security policies and procedures that provide clear direction, accountability, and oversight for the organization's security team. The security team assigns roles and responsibilities in accordance with the organization's policies and confirms that processes are in place to protect company assets and critical information.
4. The organization's contracts with external entities that address the organization's security policies and procedures with business partners, third-party contractors, and outsourcing partners.

5. The organization's security policies and procedures that ensure coordination or integration with the organization's physical security plan. Organization roles and responsibilities are established that address the overlap and synergy between physical and control system security risks.

2.2.3.2 Supplemental Guidance

None

2.2.3.3 Requirement Enhancements

None

2.2.3.4 References

NIST SP 800-53r3	PM-1
API 1164r2	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8
NRC RG 5.71	App. C.11.3

2.2.4 Coordination of Threat Mitigation

2.2.4.1 Requirement

The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers, and other relevant organizations in the event of a security incident.

2.2.4.2 Supplemental Guidance

The organization expands relationships with local emergency response personnel to include information sharing and coordination of contingency plans as well as coordinated response to cybersecurity incidents. Entities, such as US-CERT and ICS-CERT, are available for threat assistance.

2.2.4.3 Requirement Enhancements

None

2.2.4.4 References

NIST SP 800-53r3	PM-9
API 1164r2	Section 3, Annex B and B.3
NERC CIPS	CIP 003-3, B.R1

2.2.5 Security Policies for Third Parties

2.2.5.1 Requirement

The organization holds external suppliers and contractors that have an impact on the security of the control center to the same security policies and procedures as the organization's own personnel. The organization ensures security policies and procedures of second and third-tier suppliers comply with corporate cybersecurity policies and procedures if they will impact control system security.

2.2.5.2 Supplemental Guidance

The organization considers the increased security risk associated with outsourcing as part of the decision-making process to determine what to outsource and what outsourcing partner to select. Contracts with external suppliers govern physical as well as logical access. The organization clearly defines confidentiality or nondisclosure agreements and intellectual property rights. The organization also clearly defines change management procedures.

2.2.5.3 Requirement Enhancements

None

2.2.5.4 References

NIST SP 800-53r3	PS-7
API 1164r2	3.4, 7.3.4, Annex A
NERC CIPS	CIP 004-3, B.R4, B.R4.1
NRC RG 5.71	App. B.1.21

2.2.6 Termination of Third-Party Access

2.2.6.1 Requirement

The organization establishes procedures to remove external supplier physical and electronic access at the conclusion/termination of the contract in a timely manner.

2.2.6.2 Supplemental Guidance

The organization clearly defines the timeliness for removal of external supplier access in the contract.

2.2.6.3 Requirement Enhancements

The organization periodically reviews existing authorized physical and electronic access permissions to ensure they are current. This check provides validation that terminated entities have been removed from physical and electronic access.

2.2.6.4 References

NIST SP 800-53r3	AC-2, PS-4
CAG	CC-9, CC-11
API 1164r2	7.3.4, Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. B.1.21, App. C.2.2

2.3 Personnel Security

Personnel security addresses security program roles and responsibilities implemented during all phases of staff employment, including staff recruitment and termination. The organization screens applicants for critical positions in the operation and maintenance of the control system. The organization trains personnel when they are hired and provides subsequent refresher training on their job tasks, responsibilities, and behavioral expectations concerning the security of the control system. The organization may consider implementing a confidentiality or nondisclosure agreement that employees and third-party users of control system facilities must sign before being granted access to the control system. The organization also documents and implements a process to secure resources and revoke access privileges when personnel terminate.

2.3.1 Personnel Security Policy and Procedures

2.3.1.1 Requirement

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

1. A formal, documented, personnel 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 the 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 facilitate the implementation of the personnel security policy and associated personnel security controls
3. Formal procedures to review and document the list of approved personnel with access to control systems.

2.3.1.2 Supplemental Guidance

The organization ensures the personnel security policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular control system, when required.

2.3.1.3 Requirement Enhancements

None

2.3.1.4 References

NIST SP 800-53r3	PS-1
API 1164r2	3.1
NERC CIPS	CIP 003-3, A, B.R1, B.1.1-1.3
NRC RG 5.71	App. B.1.21, App. C.2.1

2.3.2 Position Categorization

2.3.2.1 Requirement

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.

2.3.2.2 Supplemental Guidance

Designated officials within the organization assign a risk level for every position within the control system as determined by the position's potential for adverse impact to the integrity and efficiency of the control system.

2.3.2.3 Requirement Enhancements

None

2.3.2.4 References

NIST SP 800-53r3	PS-2
API 1164r2	3.1
NERC CIPS	CIP 003-3, B.R5.1, B.5.1.1
NRC RG 5.71	App. B.1.21

2.3.3 Personnel Screening

2.3.3.1 Requirement

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

2.3.3.2 Supplemental Guidance

The organization maintains consistency between the screening process and organizational policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.

Basic screening requirements include:

1. Past 5 years of employment
2. Past 5 years of education, with verification of the highest degree received
3. Past 3 years of residency
4. References
5. Past 5 years of law enforcement records.

2.3.3.3 Requirement Enhancements

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.

2.3.3.4 References

NIST SP 800-53r3	PS-3
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R5.1, B.R5.1.2
NRC RG 5.71	App. B.1.21

2.3.4 Personnel Termination

2.3.4.1 Requirement

When an employee is terminated, the organization revokes logical and physical access to control systems and facilities and ensures all organization-owned property is returned and that organization-owned documents and data files relating to the control system that are in the employee's possession are transferred to the new authorized owner within the organization. Complete execution of this control occurs within 24 hours for employees or contractors terminated for cause.

2.3.4.2 Supplemental Guidance

Organization-owned property includes system administration manuals, keys, identification cards, building passes, computers, cell phones, and personal data assistants. Organization-owned documents include field device configuration and operational information, control system network documentation.

Exit interviews ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all system-related property.

2.3.4.3 Requirement Enhancements

The organization implements automated processes to revoke access permissions that are initiated by the termination. Periodic reviews of physical and electronic access are conducted to validate that terminated account access was completed.

2.3.4.4 References

NIST SP 800-53r3	PS-4
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. B.1.2, App. C.2.2

2.3.5 Personnel Transfer

2.3.5.1 Requirement

The organization reviews electronic and physical access permissions to control systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. Complete execution of this control occurs within 7 days for employees or contractors who no longer need to access control system resources.

2.3.5.2 Supplemental Guidance

Appropriate actions may include:

1. Returning old and issuing new keys, identification cards, and building passes
2. Closing old accounts and establishing new accounts
3. Changing system access authorizations
4. Providing access to official records created or managed by the employee at the former work location and in the former accounts.

2.3.5.3 Requirement Enhancements

The organization periodically reviews existing authorized physical and electronic access permissions to ensure they are current. This check is to provide validation that transferred entities have been added, changed, or removed correctly from necessary physical and electronic access.

2.3.5.4 References

NIST SP 800-53r3	PS-5
API 1164r2	Annex A
NERC CIPS	CIP 004-3, B.R4, B.4.2
NRC RG 5.71	App. C.2.2

2.3.6 Access Agreements

2.3.6.1 Requirement

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.

2.3.6.2 Supplemental Guidance

Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the control system to which access is authorized. Electronic signatures are acceptable for acknowledging access agreements unless specifically prohibited by organizational policy or applicable government regulations.

2.3.6.3 Requirement Enhancements

None

2.3.6.4 References

NIST SP 800-53r3	PS-6
API 1164r2	2.4.2, 2.4.3
NERC CIPS	CIP 004-3, B.R4, B.R.4.1, B.4.2
NRC RG 5.71	App. B.1.1, App. B.1.21

2.3.7 Third-Party Personnel Security

2.3.7.1 Requirement

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

2.3.7.2 Supplemental Guidance

Third-party providers include service bureaus, contractors, and other organizations providing control system operation and maintenance, development, IT services, outsourced applications, and network and security management. The organization explicitly includes personnel security controls in acquisition-related contract and agreement documents.

2.3.7.3 Requirement Enhancements

None

2.3.7.4 References

NIST SP 800-53r3	PS-7
API 1164r2	3.1
NERC CIPS	CIP 004-3, A-3, B.R2.1
NRC RG 5.71	App. B.1.1, App. B.1.21, App. B.1.22, App. B.3.11, App. C.3.5

2.3.8 Personnel Accountability

2.3.8.1 Requirement

The organization employs a formal accountability process for personnel failing to comply with established control system security policies and procedures and clearly documents potential disciplinary actions for failing to comply.

2.3.8.2 Supplemental Guidance

The organization ensures that the accountability process is consistent with applicable federal and local government statutory requirements (directives, policies, and regulations), standards, and guidance. The accountability process can be included as part of the organization's general personnel policies and procedures.

2.3.8.3 Requirement Enhancements

None

2.3.8.4 References

NIST SP 800-53r3	PS-8
API 1164r2	1.2
NERC CIPS	CIP 003-3, B.R2.1-2.4
NRC RG 5.71	App. B.1.11, App. B.3.11

2.3.9 Personnel Roles

2.3.9.1 Requirement

The organization provides employees and contractors with complete job descriptions and unambiguous and detailed expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.

2.3.9.2 Supplemental Guidance

None

2.3.9.3 Requirement Enhancements

Employees and contractors acknowledge understanding by signature.

2.3.9.4 References

API 1164r2	1.2, 3.1, Annex A
NERC CIPS	CIP 003-3, B.R2, R2.1-2.4
NRC RG 5.71	App. B.1.1, App. C.10.10

2.4 Physical and Environmental Security

Physical and environmental security encompasses protection of physical assets from damage, misuse, or theft. Physical security addresses the physical security mechanisms used to create secure areas around hardware. Physical access control, physical boundaries, and surveillance are examples of security practices used to ensure that only authorized personnel are allowed to access control system equipment. Environmental security addresses the safety of assets from damage from environmental concerns. Control system equipment can be very expensive and may ensure human safety; therefore, protection is important from fire, water, and other possible environmental threats.

2.4.1 Physical and Environmental Security Policy and Procedures

2.4.1.1 Requirement

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

1. A formal, documented physical security policy that addresses:
   a. The purpose of the physical security program as it relates to protecting the organization's personnel and assets
   b. The scope of the physical security program as it applies to all the organizational staff and third-party contractors

c. The roles, responsibilities, management commitment, and coordination among organizational entities of the physical security program to ensure compliance with the organization's security policy and other regulatory commitments.

2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

2.4.1.2 Supplemental Guidance

The organization ensures the physical and environmental protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The organization includes the physical and environmental protection policy as part of the general control system security policy for the organization. The organization develops physical and environmental protection procedures for the security program in general and for a particular control system's components when required.

2.4.1.3 Requirement Enhancements

None

2.4.1.4 References

NIST SP 800-53r3	PE-1
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1
NRC RG 5.71	App. B.1.1, App. C.5.1

2.4.2 Physical Access Authorizations

2.4.2.1 Requirement

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.

2.4.2.2 Supplemental Guidance

The organization promptly removes from the access list personnel no longer requiring access to facilities containing control system assets or who are denied access based on organizationally defined accountability procedures.

2.4.2.3 Requirement Enhancements

1. The organization authorizes physical access to the facility where the control system resides based on position or role.
2. The organization requires two forms of identification to gain access to the facility where the control system resides.

2.4.2.4 References

NIST SP 800-53r3	PE-2
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, B.R1, R1.5
NRC RG 5.71	C.3.3.1.1, App. C.5.4

2.4.3 Physical Access Control

2.4.3.1 Requirement

Control: 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.

2.4.3.2 Supplemental Guidance

Physical access devices include keys, locks, combinations, and card readers. Workstations and associated peripherals (monitors, speakers, and printing devices) connected to (and part of) an organizational system should be located in areas designated as limited access such as secure control rooms with access to such devices being safeguarded. This may include protecting, identifying, and inspecting information and communication lines for evidence of tampering. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of Federal Information Processing Standard (FIPS) 201. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST SP 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST SP 800-76.

2.4.3.3 Requirement Enhancements

1. The organization limits physical access to control system assets independent of the physical access security mechanisms for the facility.
2. The organization performs security checks at physical boundaries for unauthorized removal of information or system components.
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.
4. The organization employs lockable physical casings to protect internal components of the system from unauthorized physical access.
5. The organization identifies and inspects information and communication lines for evidence of tampering.

2.4.3.4 References

NIST SP 800-53r3	PE-3, PE-4, PE-5
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.4
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. B.1.22, App. C.5.5, App. C.5.6

2.4.4 Monitoring Physical Access

2.4.4.1 Requirement

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.

2.4.4.2 Supplemental Guidance

Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities are part of the organization's incident response capability.

2.4.4.3 Requirement Enhancements

1. The organization monitors real-time physical intrusion alarms and surveillance equipment.
2. The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.

2.4.4.4 References

NIST SP 800-53r3	PE-6
API 1164r2	4, Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. C.5.8

2.4.5 Visitor Control

2.4.5.1 Requirement

The organization controls physical access to the system by authenticating visitors before authorizing access to the facility where the system resides other than areas designated as publicly accessible.

2.4.5.2 Supplemental Guidance

Contractors and others with permanent authorization credentials are not considered visitors.

2.4.5.3 Requirement Enhancements

The organization escorts visitors and monitors visitor activity as required according to security policies and procedures.

The organization requires two forms of identification for access to the facility.

2.4.5.4 References

NIST SP 800-53r3	PE-7
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6
NRC RG 5.71	C.3.3.1.1, App. B.1.1

2.4.6 Visitor Records

2.4.6.1 Requirement

The organization maintains visitor access records to the control system facility (except for those areas within the facility officially designated as publicly accessible) that include:

1. Name and organization of the person visiting
2. Signature of the visitor
3. Form of identification
4. Date of access
5. Time of entry and departure
6. Purpose of visit
7. Name and organization of person visited.

2.4.6.2 Supplemental Guidance

Designated officials within the organization review the access logs after close-out and periodically review access logs based on an organization-approved frequency.

2.4.6.3 Requirement Enhancements

The organization employs automated mechanisms to facilitate the maintenance and review of access records.

2.4.6.4 References

NIST SP 800-53r3	PE-8
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R1, R1.6, R1.6.1
NRC RG 5.71	App. B.1.1, App. C.5.9

2.4.7 Physical Access Log Retention

2.4.7.1 Requirement

The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.

2.4.7.2 Supplemental Guidance

None

2.4.7.3 Requirement Enhancements

None

2.4.7.4 References

NIST SP 800-53r3	PE-8
API 1164r2	Annex A
NERC CIPS	CIP 006-3c, A, B, R7
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. C.5, App. C5.9

2.4.8 Emergency Shutoff

2.4.8.1 Requirement

The organization, for specific locations within a facility containing concentrations of control system resources, protects emergency power shutoff capability from unauthorized activation.

2.4.8.2 Supplemental Guidance

The design of the control systems facility includes an emergency shutoff to cut power to critical control system resources outside any area prone to flooding.

2.4.8.3 Requirement Enhancements

The organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.

2.4.8.4 References

NIST SP 800-53r3	PE-10
API 1164r2	Annex A
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.9 Emergency Power

2.4.9.1 Requirement

The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of noncritical control system components in the event of a primary power source loss.

2.4.9.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.9.3 Requirement Enhancements

1. The organization provides a long-term alternate power supply for the system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
2. The organization provides a long-term alternate power supply for the system that is self-contained and not reliant on external power generation.

2.4.9.4 References

NIST SP 800-53r3	PE-11
API 1164r2	4, Annex A
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.10 Emergency Lighting

2.4.10.1 Requirement

The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and includes lighting for emergency exits and evacuation routes.

2.4.10.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.10.3 Requirement Enhancements

None

2.4.10.4 References

NIST SP 800-53r3	PE-12
API 1164r2	4, Annex A
NRC RG 5.71	C.3.2, App. C.9

2.4.11 Fire Protection

2.4.11.1 Requirement

The organization implements and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

2.4.11.2 Supplemental Guidance

Fire suppression and detection devices/systems include sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.11.3 Requirement Enhancements

1. The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.
2. The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.
3. The organization employs an automatic fire suppression capability in facilities that are not staffed continuously.

2.4.11.4 References

NIST SP 800-53r3	PE-13
API 1164r2	Annex A
NRC RG 5.71	C.3.2

2.4.12 Temperature and Humidity Controls

2.4.12.1 Requirement

The organization regularly monitors the temperature and humidity within facilities containing control system assets and ensures they are maintained within acceptable levels.

2.4.12.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.12.3 Requirement Enhancements

None

2.4.12.4 References

NIST SP 800-53r3 PE-14

NRC RG 5.71 C.3.2

2.4.13 Water Damage Protection

2.4.13.1 Requirement

The organization protects the control systems from damage resulting from water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

2.4.13.2 Supplemental Guidance

This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.13.3 Requirement Enhancements

The organization implements automated mechanisms to close shutoff valves and provide notification to key personnel in the event of a water leak within facilities containing control systems.

2.4.13.4 References

NIST SP 800-53r3 PE-15

NRC RG 5.71 C.3.2, C.9

2.4.14 Delivery and Removal

2.4.14.1 Requirement

The organization authorizes and limits the delivery and removal of control system components (i.e., hardware, firmware, software) from control system facilities and maintains appropriate records and control of that equipment. The organization documents policies and procedures governing the delivery and removal of control system assets in the control system security plan.

2.4.14.2 Supplemental Guidance

The organization secures delivery areas and, if possible, isolates delivery areas from the control system to avoid unauthorized physical access.

2.4.14.3 Requirement Enhancements

None

2.4.14.4 References

NIST SP 800-53r3 PE-16

2.4.15 Alternate Work Site

2.4.15.1 Requirement

The organization establishes an alternate control center with proper equipment and communication infrastructure to compensate for the loss of the primary control system work site. The organization implements appropriate management, operational, and technical security measures at alternate control centers.

2.4.15.2 Supplemental Guidance

Alternate work sites may include government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

2.4.15.3 Requirement Enhancements

The organization provides methods for employees to communicate with control system security staff in case of security problems.

2.4.15.4 References

NIST SP 800-53r3	PE-17
API 1164r2	3.4
NERC CIPS	CIP 002-3, B.R1.2.1, R3
NRC RG 5.71	C.3.2, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.16 Portable Media

2.4.16.1 Requirement

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.

2.4.16.2 Supplemental Guidance

Mobile devices include portable storage media (e.g., USB [Universal Serial Bus] memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Usage restrictions and implementation guidance related to mobile devices can include configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident

software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of control system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family.

2.4.16.3 Requirement Enhancements

1. The organization restricts the use of writable, removable media in organizational control systems.
2. The organization prohibits the use of personally owned, removable media in organizational control systems.
3. The organization prohibits the use of removable media in organizational control systems when the media have no identifiable owner.

2.4.16.4 References

NIST SP 800-53r3	MP-2
API 1164r2	Annex A
NERC CIPS	CIP 007-3, B.R7.1, R7.2
CAG	CC-15

2.4.17 Personnel and Asset Tracking

2.4.17.1 Requirement

The organization implements asset location technologies to track and monitor the movements of personnel and vehicles within the organization's controlled areas to ensure they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.

2.4.17.2 Supplemental Guidance

None

2.4.17.3 Requirement Enhancements

Electronic monitoring mechanisms alert control system personnel when unauthorized access or an emergency occurs.

2.4.17.4 References

None

2.4.18 Location of Control System Assets

2.4.18.1 Requirement

The organization locates control system assets to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

2.4.18.2 Supplemental Guidance

Physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Where a completely enclosed (six-wall) border cannot be established, the organization implements and documents alternate measures to control physical access to the control system assets. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the control system security program. Organizations should avoid duplicating actions already covered.

2.4.18.3 Requirement Enhancements

The organization considers the risks associated with physical and environmental hazards when planning new control system facilities or reviewing existing facilities. Risk mitigation strategies are documented in the control system security plan.

2.4.18.4 References

NIST SP 800-53r3	PE-18
API 1164r2	Annex A
NERC CIPS	CIP 002-3, B.R1-R4, CIP 006-3, B.R1.1
NRC RG 5.71	C.2, C.3.1, C.3.1.3, C.3.3.3, C.3.3.2.9, C.3.14, C.4

2.4.19 Information Leakage

2.4.19.1 Requirement

The organization protects the control system from information leakage.

2.4.19.2 Supplemental Guidance

The organization considers all forms of information leakage such as removable media, official documents, remote access, misconfigured perimeter security devices, and electromagnetic signals emanations. This requirement supports confidentiality more than availability and, hence, is not as critical for control system applications.

The FIPS 199 security categorization (for confidentiality) of the system and organizational security policy guides the application of safeguards and countermeasures employed to protect the system against information leakage because of electromagnetic signals emanations.

2.4.19.3 Requirement Enhancements

None

2.4.19.4 References

NIST SP 800-53r3	PE-19
API 1164r2	Annex A
NRC RG 5.71	C.3.1.3 , C.3.2, App. B.2.5, App. B.5.1, App. C.2.1, App. C.3.4, App. C.3.11, App. C.6, App. C.8, App. C.9

2.4.20 Power Equipment and Power Cabling

2.4.20.1 Requirement

The organization protects control system power equipment and power cabling from damage and destruction.

2.4.20.2 Supplemental Guidance

None

2.4.20.3 Requirement Enhancements

The organization employs redundant power equipment and parallel power cabling paths for the control system.

2.4.20.4 References

NIST SP 800-53r3	PE-9
API 1164r2	4, Annex A
NRC RG 5.71	C.2, C.3.1, C.3.3.2.9

2.4.21 Physical Device Access Control

2.4.21.1 Requirement

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

2.4.21.2 Supplemental Guidance

Tamper-evident hardware includes, but is not limited to: (1) metal or hard plastic production-grade enclosures, (2) opaque enclosures with tamper-evident seals or pick-resistant locks for doors or removable covers, and (3) tamper detection/response envelopes with tamper response.

2.4.21.3 Requirement Enhancements

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

2.4.21.4 References

NIST SP 800-53r3	PE-3, PE-4, PE-5
API 1164r2	5.9, 8.1
NRC RG 5.71	C.3.3.2.5, App. B.1.1, App. B.1.11, App. B.1.15, App. B.1.19, App. B.4.2, App. B.4.5, App. C.3.1, App. C.5.5, App. C.5.6

2.5 System and Services Acquisition

Systems and services acquisition covers the contracting and acquiring of control system components, software, and services from third parties. The organization includes security as part of the acquisition process to ensure that the products received fit into the organization's security plan and have associated risk commensurate with defined risk acceptance levels. A strong policy with detailed procedures for reviewing acquisitions helps to eliminate the introduction of additional or unknown vulnerabilities into the control system.

2.5.1 System and Services Acquisition Policy and Procedures

2.5.1.1 Requirement

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

1. A formal, documented, system and services acquisition policy that includes control system security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

2. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

2.5.1.2 Supplemental Guidance

The organization ensures the system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular control system when required.

2.5.1.3 Requirement Enhancements

None

2.5.1.4 References

NIST SP 800-53r3	SA-1
CAG	CC-3
API 1164r2	3.1
NRC RG 5.71	C.3.4, C.3.3.3, C.3.3.3.1

2.5.2 Allocation of Resources

2.5.2.1 Requirement

The organization:

1. Includes a determination of control system security requirements for the system in mission/business case planning
2. Determines, documents, and allocates the resources required to protect the control system as part of its capital planning and investment control process.

2.5.2.2 Supplemental Guidance

The organization determines the security controls for the control systems in mission/business case planning and establishes a discrete line item for control system security in its programming and budgeting documentation.

2.5.2.3 Requirement Enhancements

None

2.5.2.4 References

NIST SP 800-53r3	SA-2
API 1164r2	3.6
NRC RG 5.71	C.3.1.1, C.3.1.3, App. B.3.5

2.5.3 Life-Cycle Support

2.5.3.1 Requirement

The organization manages the control system using a system development life-cycle methodology that includes control system security considerations.

2.5.3.2 Supplemental Guidance

None

2.5.3.3 Requirement Enhancements

None

2.5.3.4 References

NIST SP 800-53r3	SA-3
CAG	CC-7
NRC RG 5.71	C.4, C.4.1, C.4.2.1

2.5.4 Acquisitions

2.5.4.1 Requirement

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:

- Security functional requirements/specifications
- Security-related documentation requirements
- Developmental and evaluation-related assurance requirements.

2.5.4.2 Supplemental Guidance

The acquisition documents for control systems and services include, either explicitly or by reference, security requirements that describe: (1) required security capabilities (security needs and, as necessary, specific security controls), (2) required design and development processes, (3) required test and evaluation procedures, and (4) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

2.5.4.3 Requirement Enhancements

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.
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).
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.

2.5.4.4 References

NIST SP 800-53r3	SA-4
CAG	CC-3, CC-7
NRC RG 5.71	C.3.3.3, App. B.5.4, App. C.12.4

2.5.5 Control System Documentation

2.5.5.1 Requirement

The organization:

1. Obtains, protects as required, and makes available to authorized personnel, administrator and user guidance for the control system that includes information on: (a) configuring, installing, and operating the system and (b) using the system's security features

2. Documents attempts to obtain control system documentation when such documentation is either unavailable or nonexistent (e.g., because of the age of the system or lack of support from the vendor/contractor) and provides compensating security controls, if needed.

2.5.5.2 Supplemental Guidance

Administrator and user guides need to include information on:

- The configuration, installation, operation, and trouble-shooting of the control system
- The operation and trouble-shooting of the control system's security features.

2.5.5.3 Requirement Enhancements

1. The organization obtains, if available from the vendor/contractor, information describing the functional properties of the security controls employed within the control system.
2. The organization obtains, if available from the vendor/contractor, information describing the design and implementation details of the security controls employed within the control system (including functional interfaces among control components).
3. The organization obtains, if available from the vendor/contractor, information that describes the security-relevant external interfaces to the control system.

2.5.5.4 References

NIST SP 800-53r3	SA-5
API 1164r2	Annex A, Annex B.1
NERC CIPS	CIP 002-3, B.R1-R4
NRC RG 5.71	C.4.2, C.4.2.1, C.5, App. A.3

2.5.6 Software License Usage Restrictions

2.5.6.1 Requirement

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws
2. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution
3. Controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

2.5.6.2 Supplemental Guidance

The organization uses software and associated documentation in accordance with the software licensing agreement and applicable copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization limits and documents the use of publicly accessible peer-to-peer file-sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

2.5.6.3 Requirement Enhancements

None

2.5.6.4 References

NIST SP 800-53r3	SA-6
CAG	CC-2
API 1164r2	3.8
NRC RG 5.71	App. B.1.1, App. B.1.16, App. B.1.17, App. B.1.19, App. B.3.14, App. C.11.6

2.5.7 User-Installed Software

2.5.7.1 Requirement

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

2.5.7.2 Supplemental Guidance

If provided the necessary privileges, users have the ability to install software. The organization's security program identifies the types of software permitted to be downloaded and installed (e.g., updates and security patches to existing software) and types of software prohibited (e.g., software that is free only for personal, not government or corporate use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

2.5.7.3 Requirement Enhancements

None

2.5.7.4 References

NIST SP 800-53r3	SA-7
CAG	CC-2
API 1164r2	3.8, Annex A
NRC RG 5.71	App. C.3.7, App. C.13.1

2.5.8 Security Engineering Principles

2.5.8.1 Requirement

The organization applies control system security engineering principles in the specification, design, development, and implementation of the system.

2.5.8.2 Supplemental Guidance

The application of security engineering principles is primarily targeted at new development control systems or control systems undergoing major upgrades and is integrated into the system development life cycle. For legacy control systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

2.5.8.3 Requirement Enhancements

1. The organization adopts software development standards and practices for trustworthy software throughout the development life cycle.
2. Trustworthy software reduces common design and coding errors that affect security, such as:
   a. Unsafe buffer and string management
   b. Languages that have unsafe buffer operations.

3 Trustworthy software development employs commercially available tools including a robust set of data validation and software quality assurance.

2.5.8.4 References

NIST SP 800-53r3	SA-8
CAG	CC-7, CC-16
API 1164r2	Annex A
NRC RG 5.71	C.C.8.1, C.8.4, C.10.2, C.10.3, C.12.3

2.5.9 Outsourced Control System Services

2.5.9.1 Requirement

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.

2.5.9.2 Supplemental Guidance

Third-party providers are subject to the same control system security policies and procedures of the organization. All the contractors' equipment conforms to the same requirements as the organization's internal systems. Appropriate organizational officials need to approve outsourcing of control system services to third-party providers (e.g., service bureaus, contractors, and other external organizations). The outsourced control system services' documentation includes service provider and end-user security roles, responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

2.5.9.3 Requirement Enhancements

None

2.5.9.4 References

NIST SP 800-53r3	PS-7, SA-9
API 1164r2	1.2, Annex A
NRC RG 5.71	App. B.1.1, App. B.1.2, App. B.1.21, App. B.1.22, App. C.5.2

2.5.10 Developer Configuration Management

2.5.10.1 Requirement

The organization requires that control system developers/integrators implement and document a configuration management process that (1) manages and controls changes to the system during design, development, implementation, and operation; (2) tracks security flaws; and (3) includes organizational approval of changes.

2.5.10.2 Supplemental Guidance

None

2.5.10.3 Requirement Enhancements

1. The organization requires that information system developers/integrators provide an integrity check of software to facilitate user verification of software integrity after delivery.
2. The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.
3. Enhancement Supplemental Guidance: The configuration management process includes key organizational personnel that are responsible for reviewing and approving proposed changes to the informational system and security personnel that conduct impact analyses prior to the implementation of any changes to the system.

2.5.10.4 References

NIST SP 800-53r3	SA-4, SA-10
CAG	CC-3, CC-7
API 1164r2	3.7, Annex A
NRC RG 5.71	C.3.1.3, C.4.2, App. B.5.2

2.5.11 Developer Security Testing

2.5.11.1 Requirement

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.

2.5.11.2 Supplemental Guidance

The organization does not perform developmental security tests on the production control system network. Functional acceptance and security verification checks need to be conducted on a representative testbed environment with issues documented, resolved, and retested before operational acceptance can be given. Once accepted, deployment needs to be in a controlled manner to mitigate inadvertent system upsets.

2.5.11.3 Requirement Enhancements

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

2.5.11.4 References

NIST SP 800-53r3	SA-11
API 1164r2	Annex A
NRC RG 5.71	App. C.12.5

2.5.12 Supply Chain Protection

2.5.12.1 Requirement

The organization protects against supply chain vulnerabilities employing controls defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization.

2.5.12.2 Supplemental Guidance

A supply chain is a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Products and services in the domestic and international supply chain include hardware, software, and firmware components for systems, data management services, telecommunications service providers, and Internet service providers. Domestic and international supply chains are becoming increasingly important to the national and economic security interests of the United States because of the growing dependence on products and services produced or maintained in worldwide markets. Uncertainty in the supply chain and the growing sophistication and diversity of international cyber threats increase the potential for a range of adverse effects on organizational operations and assets, individuals, other organizations, and the nation. Global commercial supply chains provide adversaries with opportunities to manipulate control system technology products that are routinely used by public and private sector organizations (e.g., suppliers, contractors) in the control systems that support U.S. critical infrastructure applications. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those control systems. To mitigate risk from the supply chain, a comprehensive security strategy should be considered that employs a strategic, organization-wide *defense-in-breadth* approach. A defense-in-breadth approach helps to protect control systems (including the technology products that compose those systems) throughout the System Development Life Cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). The identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk are important components of a successful defense-in-breadth approach.

2.5.12.3 Requirement Enhancements

1. The organization purchases all anticipated control system components and spares in the initial acquisition.
2. The organization employs trusted intermediaries for purchasing contract services, acquisitions, or logistical activities during the control system life cycle.
3. The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire control system hardware, software, firmware, or services.
4. The organization uses trusted shipping and warehousing for control systems, control system components, and technology products.
5. The organization uses a diverse set of suppliers for control systems, control system components, technology products, and control system services.
6. The organization uses standard configurations for control systems, control system components, and technology products.
7. The organization minimizes the time between purchase decisions and delivery of control systems, control system components, and technology products.
8. The organization employs independent analysis and penetration testing against delivered control systems, control system components, and technology products.

2.5.12.4 References

NIST SP 800-53r3	SA-12
CAG	CC-17
NRC RG 5.71	App. C.12.2

2.5.13 Trustworthiness

2.5.13.1 Requirement

The organization requires that the control system meet an organization-defined level of trustworthiness.

2.5.13.2 Supplemental Guidance

The level of trustworthiness for organizational control systems is defined in terms of degree of correctness for intended functionality and of degree of resilience to attack by explicitly identified levels of adversary capability. In addition, but not as a replacement for this expression of degree of correctness and resilience, the level of trustworthiness may also be described in terms of levels of developmental assurance, that is, actions taken in the specification, design, development, implementation, and operation/maintenance of the control system that impact the degree of correctness and resilience achieved. Trustworthiness may be defined as different levels on the basis of component-by-component, subsystem-by-subsystem, function-by-function, or a combination of the above. However, typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and, at a minimum, something that likely requires careful attention in order to achieve practically useful results.

2.5.13.3 Requirement Enhancements

The organization requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

2.5.13.4 References

NIST SP 800-53r3	SA-13
NRC RG 5.71	App. C.12.3

2.5.14 Critical Information System Components

2.5.14.1 Requirement

The organization:

1. Defines and documents all critical hardware and software system components that are in service
2. Upgrade existing limited legacy equipment with current or custom developed information system components.

2.5.14.2 Supplemental Guidance

The assumption is that information technology products defined by the organization cannot be trusted due to unacceptable threat potential from the supply chain. Examples would be legacy systems with no viable alternatives, or existing components that cannot be hardened or enhanced to the required level of high security assurance. The organization can deploy custom developed or compensating controls to achieve high assurance security requirements.

2.5.14.3 Requirement Enhancements

The organization:

1. Identifies information system components for which alternative sourcing is not possible

2. Employs compensating measures to ensure that critical security controls for the information system components are not compromised.

2.5.14.4 References

NIST SP 800-53r3	SA-14
API 1164r2	Annex A, Annex B.3.1.1
NRC RG 5.71	C.3.1.3, App. C.3.7, App. C.11.9

2.6 Configuration Management

The organization's security program needs to implement policies and procedures that create a process by which the organization manages and documents all configuration changes to the control system. A comprehensive change management process needs to be implemented and used to ensure that only approved and tested changes are made to the control system configuration. Control systems need to be configured properly to maintain optimal operation. Therefore, only tested and approved changes should be allowed on a control system. Vendor updates and patches need to be thoroughly tested on a nonproduction control system setup before being introduced into the production environment to ensure no adverse effects occur.

2.6.1 Configuration Management Policy and Procedures

2.6.1.1 Requirement

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.

2.6.1.2 Supplemental Guidance

The organization ensures the configuration management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general control system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular control system component when required. Configuration management should include hardware, software, versions, patches deployed, operational applications, security components, conduit schedules (for data and security items). Barcodes and RFID are commonplace means of tracking hardware and supporting elements (conduits).

2.6.1.3 Requirement Enhancements

None

2.6.1.4 References

NIST SP 800-53r3	CM-1
CAG	CC-2, CC-3, CC-4
API 1164r2	Annex A, Annex B.3.1.1
NERC CIPS	CIP 002-3, B.R6, CIP 007-3, B.R1, B.R3
NRC RG 5.71	C.3.1.4, C.4.2, App. C.11.2

2.6.2 Baseline Configuration

2.6.2.1 Requirement

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

2.6.2.2 Supplemental Guidance

This control establishes a baseline configuration for the control system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the control system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the control system is built, and deviations, if required, are documented in support of mission needs/objectives. The configuration of the control system component should be consistent with the organization's control system architecture and documentation policy. The inventory of control system components includes information (e.g., manufacturer, type, serial number, version number, and location) that uniquely identifies each component. Modern inventory control systems are frequently using radio-frequency identification (RFID) for ease of use and accuracy. Maintaining the baseline configuration involves creating a new baseline as the control system changes over time and keeping old baselines available for possible rollback.

2.6.2.3 Requirement Enhancements

1. The organization reviews and updates the baseline configuration as an integral part of control system component installations.
2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the control system.
3. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.
4. The organization employs a deny-all, permit-by-exception authorization policy to identify software allowed on organizational control systems.

2.6.2.4 References

NIST SP 800-53r3	CM-2
CAG	CC-2, CC-3, CC-4
API 1164r2	3.6, Annex B.1.1
NERC CIPS	CIP 007-3, B.R1, B.R3
NRC RG 5.71	C.4.2, App. C.11.3

2.6.3 Configuration Change Control

2.6.3.1 Requirement

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.

2.6.3.2 Supplemental Guidance

The organization manages configuration changes to the control system using an organizationally approved process (e.g., a Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the control system, including upgrades and modifications. Because of the convergence of IT and control systems, configuration change control includes changes to the configuration settings for the control system and those IT products (e.g., operating systems, firewalls, routers) that are components of the control system. Each device on the control system contains a unique identifier (e.g., serial number, device name, tag number, RFID tag) that is referenced in the configuration management process. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the control system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the control system.

A production control system may need to be taken offline, or replicated to the extent feasible, before the testing can be conducted. If a control system must be taken offline for tests, tests are scheduled to occur during planned control system outages whenever possible. In situations where the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety, reliability) to implement the live testing of the production control system, the organization documents the rationale for using a replicated system.

2.6.3.3 Requirement Enhancements

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.
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.

2.6.3.4 References

NIST SP 800-53r3	CM-3
CAG	CC-2, CC-3, CC-4
API 1164r2	3.6, Annex A, Annex B.3.1
NERC CIPS	CIP 002-3 B.R6, CIP 007-3. B.R1, B.R3

NRC RG 5.71	C.3.1.3, C.4.2, App. B.5.4, App. B.5.5, App. C.11.4

2.6.4 Monitoring Configuration Changes

2.6.4.1 Requirement

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

2.6.4.2 Supplemental Guidance

Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the control system for potential security impacts. After the control system is changed, the organization should check the security features to ensure that the features are still functioning properly. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. Security impact analysis is an important activity in the ongoing monitoring of security controls in the control system. The organization should audit activities associated with configuration changes to the control system. The organization considers control system safety and security interdependencies.

2.6.4.3 Requirement Enhancements

None

2.6.4.4 References

NIST SP 800-53r3	CM-4
CAG	CC-4
API 1164r2	3.6, Annex A, Annex B.3.1.1.1
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	C.4.3, App. C.3.4, B.5.4, App. C.11.7, App. C.11.8

2.6.5 Access Restrictions for Configuration Change

2.6.5.1 Requirement

The organization:

1. Defines, documents, and approves individual access privileges and enforces physical and logical access restrictions associated with configuration changes to the control system
2. Generates, retains, and reviews records reflecting all such changes.

2.6.5.2 Supplemental Guidance

Planned or unplanned changes to the hardware, software, and/or firmware components of the control system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to control system components for purposes of initiating changes, including upgrades, and modifications. The organization establishes strict terms and conditions for installing any hardware or software on control system devices (e.g., modems, wireless adapters, multi-function printers, games, word processing software).

In addition, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the control system. Access restrictions for change also include software libraries. Examples of access restrictions include physical and logical access controls, workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the control system component), and change windows (e.g., changes occur only

during specified times making unauthorized changes outside the window, easy to discover). Some or all the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the control system, auditing changes, and retaining and review records of changes.

2.6.5.3 Requirement Enhancements

1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
2. The organization conducts audits of control system changes at a defined frequency and when indications so warrant to determine whether unauthorized changes have occurred.
3. The control system prevents the installation of device drivers that are not signed with an organizationally recognized and approved certificate.
4. Physical security to restrict data devices (compact disc [CD]/digital video disc [DVD], tape, serial ports, network ports, USB/secure digital memory card [SD] configuration devices) is required. Security authorization including two-man policies is required.

2.6.5.4 References

NIST SP 800-53r3	CM-5
CAG	CC-2, CC-3, CC-4
API 1164r2	Annex A, Annex B.5
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	C.4.2.1, C.4.3, App. B.1.1, App. B.5.4, App. B.5.5, App. C.11.6

2.6.6 Configuration Settings

2.6.6.1 Requirement

The organization:

1. Establishes mandatory configuration settings for products employed within the control system
2. Configures the security settings of control systems technology products to the most restrictive mode consistent with control system operational requirements
3. Documents the changed configuration settings
4. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the control system based on explicit operational requirements
5. Enforces the configuration settings in all components of the control system
6. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

2.6.6.2 Supplemental Guidance

Configuration settings are the configurable parameters of the products that compose the control system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. In some industries, a mandated testing period is required, with separate approval needed before the test configuration settings can be deployed.

This control applies to remote assets (e.g., remote assets used to access the control system) as well as assets onsite.

2.6.6.3 Requirement Enhancements

1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings.
3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

2.6.6.4 References

NIST SP 800-53r3	CM-6
CAG	CC-3, CC-4, CC-13
NERC CIPS	CIP 007-3. B.R1, B.R3
NRC RG 5.71	App. C.11.7

2.6.7 Configuration for Least Functionality

2.6.7.1 Requirement

The organization configures the control system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list.

2.6.7.2 Supplemental Guidance

Control systems provide a wide variety of functions and services. Some of the default functions and services may not be necessary to support essential organizational operations (e.g., key missions, functions). The functions and services (e.g., voice-over internet protocol [VoIP], instant messaging, file transfer protocol, hypertext transfer protocol [HTTP], file sharing) provided by control systems should be carefully reviewed to determine which are candidates for elimination.

The organization considers disabling unused or unnecessary physical and logical ports (e.g., USB, Personal System/2, file transfer protocol [FTP]) on control system components to prevent unauthorized connection of devices (e.g., thumb drives, keystroke loggers). Organizations can use network scanning tools, intrusion detection and prevention systems, and end-point protections, such as firewalls and host intrusion detection systems, to identify and prevent the use of prohibited ports, protocols, and services. This can be third-party software or physical methods to control access.

2.6.7.3 Requirement Enhancements

1 The organization reviews the control system periodically or as deemed necessary to identify and eliminate unnecessary functions, ports, protocols, and/or services.

2. The organization employs automated mechanisms to prevent program execution in accordance with defined lists.
3. Use of configuration laptops and or removable electronic media sometimes cannot be avoided. In such cases, approved and authorized devices need to be documented, secured, and available only to specified and approved entities for use.
4. Six wall bordering requirements such as special equipment vaulting, two-man rules, and enhanced inventory control and authorization will be used.

5. In high security situations, it is necessary to separate the duties and access between the system administrator and the cybersecurity officer such that neither can make the changes by themselves. In this case, while the system administrator may have server permission, the security officer maintains and controls physical access to the server and/or dataport locking mechanisms.

2.6.7.4 References

NIST SP 800-53r3	CM-7
CAG	CC-2, CC-3, CC-4, CC-7, CC-13
API 1164r2	5.7, Annex A
NERC CIPS	CIP 007-3. B.R2, B.R2.1-2.3
NRC RG 5.71	App. 5.3, App. B.5.4, App. C.11.8

2.6.8 Configuration Assets

2.6.8.1 Requirement

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.

2.6.8.2 Supplemental Guidance

Before a configuration management program can operate, all configurable items should first be uniquely identified and recorded. The organization determines the appropriate level of granularity for any control system component included in the inventory that is subject to management control (e.g., tracking, and reporting). The inventory of control system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner, and for a networked component/device, the machine name and network address). In addition, configuration files, setpoints, alarm points, security filter rules, authorized and approved white lists, and permission files need to be documented and securely stored and backed up. This includes the current operational application files for the operational PLC elements. These files are crucial to effective disaster/incident recovery. The organization's maintenance program is responsible for configuration management tasks. Personnel performing maintenance on a control system should refer to and update the configurable assets list to ensure that all control system components are maintained and configured appropriately.

2.6.8.3 Requirement Enhancements

1. The organization updates the inventory of control system components and programming as an integral part of component installation, replacement and system updates.
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.
3. The organization employs automated mechanisms to detect the addition of unauthorized components/devices/component settings into the control system.

4. The organization disables network access by such components/devices or notifies designated organizational officials.
5. The organization includes in property accountability information for control system components, the names of the individuals responsible for administering those components.

2.6.8.4 References

NIST SP 800-53r3	CM-8
CAG	CC-1, CC-2, CC-4
API 1164r2	Annex A
NERC CIPS	CIP 007-3. B.R1
NRC RG 5.71	App. 5.3, App. B.5.4, App. B5.5, App. C.11.8, App. C.11.9

2.6.9 Addition, Removal, and Disposal of Equipment

2.6.9.1 Requirement

The organization implements policy and procedures to address the addition, removal, and disposal of all control system equipment. All control system assets and information are documented, identified, and tracked so that the location and function are known.

2.6.9.2 Supplemental Guidance

The organization sanitizes control system media, both paper and digital, before disposal or reuse. All control system media need to be tracked, documented, and verified as sanitized. The organization periodically verifies the media sanitization process.

2.6.9.3 Requirement Enhancements

1. Specialized critical digital assets must require internal registration, configuration and usage plan, and secure storage before, during and after usage.
2. Critical Digital Assets in security arenas, such as laptop and desktop computers, network gear, hard drives, removable electronic media (e.g., CD/DVD/Tape/USB/SD), must be destroyed on removal from operations, or inspected and undergo approved, documented, de-sanitization procedures (deep formatting or destruction) on being removed from service.

2.6.9.4 References

CAG	CC-2
NERC CIPS	CIP 007-3, B.R7, R7.1, R7.2, R7.3
NRC RG 5.71	App. B.5.1, App. B.5.5, App. C.1.6, App. C.11.2, App. C.11.9

2.6.10 Factory Default Authentication Management

2.6.10.1 Requirement

The organization changes all factory default authentication credentials on control system components and applications upon installation.

2.6.10.2 Supplemental Guidance

Many control system devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory defaults are often well known or easily discoverable. They present an obvious security risk and, therefore, should be changed prior to the device being put into service. In addition, do not embed passwords into tools, source code, scripts, aliases,

or shortcuts. Known legacy components with these deficiencies need to be identified and targeted for higher priority in upgrade/replacement during the next maintenance/upgrade cycle.

2.6.10.3 Requirement Enhancements

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.

2.6.10.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5.5, 5.6, Annex A
NERC CIPS	CIP 007-3. B.R5.1
NRC RG 5.71	C.3.3.1.4, App. B.1.20, App. B.4.1, App. B.4.7

2.6.11 Configuration Management Plan

2.6.11.1 Requirement

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.

2.6.11.2 Supplemental Guidance

Configuration items are the control system items (hardware, software, firmware, and documentation). Configuration management is the management of planned changes to those items. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual control system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life-cycle activities at the control system level. It includes the steps for moving a change through the change management process; how configuration settings and configuration baselines are updated; how the control system component inventory is maintained; how development, test, and operational environments are controlled; and how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system.

2.6.11.3 Requirement Enhancements

The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Enhanced Supplemental Guidance—In the absence of a dedicated configuration management team, the system integrator may be tasked with developing a configuration management process.

2.6.11.4 References

NIST SP 800-53r3	CM-9
API 1164r2	Annex A
NERC CIPS	CIP 003-3. B.R6
NRC RG 5.71	C.3.1.4, C.4.2, App. B.5.3, App. B.5.4, App. B.5.5, App. C.11.2

2.7 Strategic Planning

Strategic planning maintains optimal operations and prevents or recovers from undesirable interruptions to control system operation. Interruptions may take the form of a natural disaster (hurricane, tornado, earthquake, flood, etc.), an unintentional manmade event (accidental equipment damage, fire or explosion, operator error, etc.), an intentional manmade event (attack by bomb, firearm or vandalism, hacker or malware, etc.), or an equipment failure. The types of planning considered are security planning to prevent undesirable interruptions, continuity of operations planning to maintain system operation during and after an interruption), and planning to identify mitigation strategies. The continuity of operations planning may also be designated as incident response planning. The planning process is the same for each type of plan. The following items should be considered when developing a plan.

2.7.1 Strategic Planning Policy and Procedures

2.7.1.1 Requirement

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

1. A formal, documented, planning policy that addresses:
   a. The purpose of the strategic planning program as it relates to protecting the organization's personnel and assets
   b. The scope of the strategic planning program as it applies to all the organizational staff and third-party contractors
   c. The roles, responsibilities, coordination among organizational entities, and management accountability structure of the strategic planning program to ensure compliance with the organization's security policy and other regulatory commitments.
2. Formal, documented procedures to facilitate the implementation of the strategic planning policy and associated strategic planning controls.

2.7.1.2 Supplemental Guidance

The strategic planning policy may be included as part of the general information security policy for the organization. Strategic planning procedures may be developed for the security program in general and a control system in particular, when required.

2.7.1.3 Requirement Enhancements

None

2.7.1.4 References

NIST SP 800-53r3	PL-1
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	C.3.1, C.3.1.1, C.3.3.3, App. C.13

2.7.2 Control System Security Plan

2.7.2.1 Requirement

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.

2.7.2.2 Supplemental Guidance

The security plan is aligned with the organization's control system architecture and information security architecture. To develop properly the control system security plan, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and mitigate risk in the control system. The cybersecurity team considers control system safety and security interdependencies. The cybersecurity team includes members of the organization's IT staff, control system engineers, control system operators, members with network and system security expertise, members of the management staff, and members of the physical security department, at a minimum. In some smaller organizations, it may be necessary for personnel to perform multiple roles. For continuity and completeness, the cybersecurity team consults with the control system vendor(s) as well.

2.7.2.3 Requirement Enhancements

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.

2.7.2.4 References

NIST SP 800-53r3	PL-2
API 1164r2	3, Annex B
NERC CIPS	CIP 003-3. B.R1
NRC RG 5.71	C.2, C.3, App. B.1.2, App. C.10.4

2.7.3 Interruption Identification and Classification

2.7.3.1 Requirement

The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."

2.7.3.2 Supplemental Guidance

The various types of incidents that might be caused by system intrusion need to be identified and classified as to their effects and likelihood so that a proper response can be formulated for each potential

incident. The organization determines the impact to each system and the consequences associated with loss of one or more of the control systems. Proactive measurements are determined automatically to identify attacks during their early stages. The organization fully identifies any potential links between the corporate mission, safety, and the control system and incorporates this understanding into integrated security incident response procedures.

During postinterruption analysis activities, previously unforeseen consequences, especially those that may affect future application of the plan, need to be identified. Incidents may include risk events, near misses, and malfunctions. Also included should be any observed or suspected weaknesses in the control system or risks that may not have been previously recognized.

2.7.3.3 Requirement Enhancements

None

2.7.3.4 References

NIST SP 800-53r3	IR-8, PM-9
CAG	CC-10, CC-17
NERC CIPS	CIP 008-03 B.R1.1
NRC RG 5.71	C.2, C.3.1.2, App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8

2.7.4 Roles and Responsibilities

2.7.4.1 Requirement

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

2.7.4.2 Supplemental Guidance

The organization's control system security plan defines the roles and responsibilities of the various employees and contractors in the event of an incident. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including control system and other process owners, to reestablish operations. The response teams have a major role in the interruption identification and planning process. Several other standards and guidelines have begun separating out roles and responsibilities to separate control elements as necessary. Examples of differing roles and responsibilities would be Security Training versus Incident Management versus Patch Management.

2.7.4.3 Requirement Enhancements

None

2.7.4.4 References

NIST SP 800-53r3	AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
CAG	CC-18
API 1164r2	1.2, 3.1, Annex A, Annex B.5
NERC CIPS	CIP 008-3. B.R1.2
NRC RG 5.71	C.2, C.3.1.2, App. C.3.4, App. C.8, App. C.8.1, App. C.8.8, App. C.10.10

2.7.5 Planning Process Training

2.7.5.1 Requirement

The organization includes training on the implementation of the control system security plans for employees, contractors, and stakeholders into the organization's planning process.

2.7.5.2 Supplemental Guidance

Advanced training, documentation and testing requirements and certifications are to be provided to individuals in the control system community to understand the content, purpose, and implementation of the security plans, procedures and funtionality. The organization's planning process must account for training in the implementation of the organization's security plan. Different levels of training may be prepared for personnel with different levels of roles and responsibility. Cross-training might also be considered. Additional training controls are addressed in individual families.

2.7.5.3 Requirement Enhancements

None

2.7.5.4 References

NIST SP 800-53r3	AC-5, CP-1, CP-3
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B.5
NERC CIPS	CIP 008-3. B.R1.2
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8, App. C.10.4, App. C.10.6

2.7.6 Testing

2.7.6.1 Requirement

The organization regularly tests security plans to validate the control system objectives.

2.7.6.2 Supplemental Guidance

Following the preparation of the various plans, a schedule is developed to review and test each of the plans and ensure that it continues to meet the objectives. Additional testing requirements are addressed in individual families.

2.7.6.3 Requirement Enhancements

None

2.7.6.4 References

NIST SP 800-53r3	CP-2, CP-4, IR-3, SA-11, SI-4, SI-6
CAG	CC-17
API 1164r2	3.5, 3.7, Annex A, Annex B.4
NERC CIPS	CIP 008-3. B.R1, C, M1
NRC RG 5.71	App. B.4.9, App. C.8.3, App. C.9.3, App. C.13.1, App. C.13.2

2.7.7 Investigation and Analysis

2.7.7.1 Requirement

The organization includes investigation and analysis of control system incidents in the planning process.

2.7.7.2 Supplemental Guidance

The organization develops an incident investigation and analysis program, either internally or externally, to investigate incidents. These investigations need to consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber and control system incident may include intentional and/or unintentional incidents. The organization develops, tests, deploys, and fully documents an incident investigation process. The incident and analysis investigation program specifies the roles and responsibilities of local law enforcement and/or other critical stakeholders in an internal and shared incident investigation program. Incidents need to be analyzed in light of trends and recorded so they can be used for subsequent trend analyses.

2.7.7.3 Requirement Enhancements

None

2.7.7.4 References

NIST SP 800-53r3	IR-4
API 1164r2	3.5, Annex A, Annex B.2
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8, App. C.10.10

2.7.8 Corrective Action

2.7.8.1 Requirement

The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cybersecurity and control system incidents are fully implemented.

2.7.8.2 Supplemental Guidance

The organization reviews investigation results and determines corrective actions needed to ensure that similar events do not reoccur. The organization encourages and promotes cross-industry exchange of incident information and cooperation to learn corrective actions from the experiences of others.

2.7.8.3 Requirement Enhancements

None

2.7.8.4 References

NIST SP 800-53r3	IR-4
API 1164r2	3.5, Annex B.4
NERC CIPS	CIP 009-3. B.R3
NRC RG 5.71	App. C.3.4, App. C.8, App. C.8.1, App. C.8.4, App. C.8.8

2.7.9 Risk Mitigation

2.7.9.1 Requirement

Risk-reduction mitigation measures are planned and implemented, and the results are monitored to ensure effectiveness of the organization's risk management plan.

2.7.9.2 Supplemental Guidance

The organization's planning process develops step-by-step actions to be taken by the various organizations to implement the organization's risk mitigation plan. Risk mitigation measures need to be implemented, and the results need to be monitored against planned metrics to ensure the effectiveness of the risk management plan. The reasons for selecting or rejecting certain security mitigation mechanisms and the risks they address need to be documented by the organization's planning process.

2.7.9.3 Requirement Enhancements

None

2.7.9.4 References

NIST SP 800-53r3	PL-2, PM-9
API 1164r2	Annex B.3
NERC CIPS	CIP 007-3. B.R8
NRC RG 5.71	App. C.13.2

2.7.10 System Security Plan Update

2.7.10.1 Requirement

The organization regularly, at prescribed frequencies, reviews the security plan for the control system and revises the plan to address system/organizational changes or problems identified during system security plan implementation or security controls assessment.

2.7.10.2 Supplemental Guidance

Significant changes need to be defined in advance by the organization and identified in the configuration management process.

2.7.10.3 Requirement Enhancements

None

2.7.10.4 References

NIST SP 800-53r3	PL-2
API 1164r2	3, Annex B.4
NERC CIPS	CIP 008-3. B.R1.3, R4.3
NRC RG 5.71	C.4.1, C.4.2.2, App. B.3.1, App. C.3.1, App. C.7

2.7.11 Rules of Behavior

2.7.11.1 Requirement

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.

2.7.11.2 Supplemental Guidance

Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy.

2.7.11.3 Requirement Enhancements

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.

2.7.11.4 References

NIST SP 800-53r3	PL-4
API 1164r2	3. Annex A, Annex B.5
NERC CIPS	CIP 005-3. B.R2, R2.5, R2.6
NRC RG 5.71	C.3.3.2, C.3.3.2.7, App. C.9.1

2.7.12 Security-Related Activity Planning

2.7.12.1 Requirement

The organization plans and coordinates security-related activities affecting the control system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals.

2.7.12.2 Supplemental Guidance

Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advanced planning and coordination include both emergency and nonemergency (i.e., routine) situations.

2.7.12.3 Requirement Enhancements

None

2.7.12.4 References

NIST SP 800-53r3	PL-6
API 1164r2	3.5, 3.7, Annex A, Annex B.2
NERC CIPS	CIP 008-3. B.R1
NRC RG 5.71	C.3.3.2, C.3.3.2.7, App. C.9.1, App. C.10.3, App. C.10.4

2.8 System and Communication Protection

System and communication protection consists of steps taken to protect the control system and the communication links between system components from cyber intrusions. Although control system and communication protection might logically include both physical and cyber protection, this section addresses only cyber protection. Physical protection is addressed in Section 2.4.

2.8.1 System and Communication Protection Policy and Procedures

2.8.1.1 Requirement

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

1. A formal, documented system and communication protection policy that addresses:
   a. The purpose of the system and communication protection policy as it relates to protecting the organization's personnel and assets
   b. The scope of the system and communication protection policy as it applies to all the organizational staff and third-party contractors

c. The roles, responsibilities, coordination among organizational entities, and management accountability structure of the security program to ensure compliance with the organization's system and communications protection policy and other regulatory commitments

2. Formal, documented procedures to facilitate the implementation of the control system and communication protection policy and associated systems and communication protection controls.

2.8.1.2 Supplemental Guidance

The organization ensures the system and communication protection policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and communication protection policy needs to be included as part of the general information security policy for the organization. System and communication protection procedures can be developed for the security program in general and a control system in particular, when required.

2.8.1.3 Requirement Enhancements

None

2.8.1.4 References

NIST SP 800-53r3	SC-1
API 1164r2	Annex A, Annex B
NERC CIPS	CIP 005-3. B.R1 through R5
NRC RG 5.71	C.3.3.1.3, App. B.3.1, App. C.1.1, App. C.5.1

2.8.2 Management Port Partitioning

2.8.2.1 Requirement

The control system components separate telemetry/data acquisition services from management port functionality.

2.8.2.2 Supplemental Guidance

The control system management port needs to be physically or logically separated from telemetry/data acquisition services and information storage and management services (e.g., database management) of the system. Separation may be accomplished by using different computers, different central processing units, different instances of the operating systems, different network addresses, combinations of these methods, or other methods as appropriate.

2.8.2.3 Requirement Enhancements

In situations where the ICS cannot separate user functionality from information system management functionality, the organization employs compensating controls (e.g., providing increased auditing measures).

2.8.2.4 References

NIST SP 800-53r3	SC-2
API 1164r2	8.2, Annex B.3.1.4.4
NERC CIPS	CIP 005-3. B.R2
NRC RG 5.71	App. B.3.2, App. B.3.6, App. B.5.1, App. B.5.4, App. C.3.3, App. C.7, App. C.11

2.8.3 Security Function Isolation

2.8.3.1 Requirement

The control system isolates security functions from nonsecurity functions.

2.8.3.2 Supplemental Guidance

The control system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions, domains) that controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions. The control system maintains a separate execution domain (e.g., address space) for each executing process.

Some legacy control systems may not implement this capability. In situations where it is not implemented, the organization details its risk acceptance and mitigation in the control system security plan.

2.8.3.3 Requirement Enhancements

The control system employs the following underlying hardware separation mechanisms to facilitate security function isolation.

1 The control system isolates security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

2. The control system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

3. The control system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

4. The control system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

2.8.3.4 References

NIST SP 800-53r3	SC-3
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	5.1, Annex B.3.1.3
NERC CIPS	CIP 005-3. B.R1.1 through R1.5, R2
NRC RG 5.71	C.3.2.1, App. B.1.20, App. B.3.2

2.8.4 Information in Shared Resources

2.8.4.1 Requirement

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

2.8.4.2 Supplemental Guidance

Control of system remnants, sometimes referred to as object reuse or data remnants, prevents information, including cryptographically protected representations of information previously produced by the control system, from being available to any current user/role/process that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the system. This control does not address: (1) information remnants that refer to residual representation of data that have been in some way nominally erased or removed, (2) covert channels

where shared resources are manipulated to achieve a violation of information flow restrictions, or (3) components in the control system for which only a single user/role exists.

2.8.4.3 Requirement Enhancements

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

2.8.4.4 References

NIST SP 800-53r3	SC-4
API 1164r2	Annex B.3.1.3
NERC CIPS	CIP 005-3. B.R2
NRC RG 5.71	App. B.3.3

2.8.5 Denial-of-Service Protection

2.8.5.1 Requirement

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.

2.8.5.2 Supplemental Guidance

A variety of technologies exists to limit, or in some cases, eliminate the effects of denial-of-service attacks. For example, network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks.

2.8.5.3 Requirement Enhancements

1. The control system restricts the ability of users to launch denial-of-service attacks against other control systems or networks.
2. The control system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

2.8.5.4 References

NIST SP 800-53r3	SC-5
API 1164r2	Annex A, Annex B.2
NRC RG 5.71	App. B.3.4

2.8.6 Resource Priority

2.8.6.1 Requirement

The control system limits the use of resources by priority.

2.8.6.2 Supplemental Guidance

Priority protection helps prevent a lower-priority process from delaying or interfering with the control system servicing any higher-priority process. This control does not apply to components in the system for which only a single user/role exists.

2.8.6.3 Requirement Enhancements

None

2.8.6.4 References

NIST SP 800-53r3 SC-6

NRC RG 5.71 App. B.3.5

2.8.7 Boundary Protection

2.8.7.1 Requirement

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.

2.8.7.2 Supplemental Guidance

Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective, organization-defined security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone). Control system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services commonly are based on network components and consolidated management systems shared by all attached commercial customers and may include third-party-provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

Generally, public access to ICS information is not permitted. Allowing telecommunication and business IT traffic (e-mail, Internet access) on ICS systems is not recommended.

2.8.7.3 Requirement Enhancements

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.
2. The organization prevents public access into the organization's internal control system networks except as appropriately mediated.
3. The organization limits the number of access points to the control system to allow for better monitoring of inbound and outbound network traffic.
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.

5. The control system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
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.
7. The organization prevents the unauthorized release of information across managed interfaces.
8. The control system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
9. The control system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external systems.
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.
11. The control system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.
12. The organization selects an appropriate failure mode (e.g., fail open or fail close), depending on the critical needs of system availability.

2.8.7.4 References

NIST SP 800-53r3	SC-7
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	4, Annex A, Annex B
NERC CIPS	CIP 005-3. A, B.R1
NRC RG 5.71	C.3.2.1, App. B.1.20

2.8.8 Communication Integrity

2.8.8.1 Requirement

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

2.8.8.2 Supplemental Guidance

If the organization is relying on a commercial service provider for communication services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security measures for transmission integrity. When it is infeasible or impractical to obtain the necessary assurances of effective security through appropriate contracting vehicles, the organization either implements appropriate compensating security measures or explicitly accepts the additional risk.

2.8.8.3 Requirement Enhancements

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).
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.

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.
4. The control system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.8.4 References

NIST SP 800-53r3	SC-8
API 1164r2	8, Annex A, Annex B.3.1.1
NRC RG 5.71	App. B.3.6

2.8.9 Communication Confidentiality

2.8.9.1 Requirement

The control system design and implementation protects the confidentiality of communicated information where necessary.

2.8.9.2 Supplemental Guidance

The use of a third-party communication service provider instead of organization-owned infrastructure may warrant the use of encryption. The use of cryptographic mechanisms within a control system could introduce communications latency because of the additional time and computing resources required to encrypt, decrypt, and authenticate each message. Any latency induced from the use of cryptographic mechanisms must not degrade the operational performance of the control system.

2.8.9.3 Requirement Enhancements

1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.
2. The control system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

2.8.9.4 References

NIST SP 800-53r3	SC-9
CAG	CC-4, CC-14
API 1164r2	8
NRC RG 5.71	App. B.1.17, App. B.3.7

2.8.10 Trusted Path

2.8.10.1 Requirement

The control system establishes a trusted communications path between the user and the system.

2.8.10.2 Supplemental Guidance

A trusted path is employed for high-confidence connections between the security functions of the control system and the user (e.g., for login).

Login-to-operator interface should be protected by trusted path or a compensating control. A trusted path is a mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base (TCB) that provides the security functions of the system. This mechanism can only be activated by the person or the TCB and cannot be imitated by untrusted software. The TCB is the totality

of protection mechanisms within a computer system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to enforce correctly a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

2.8.10.3 Requirement Enhancements

None

2.8.10.4 References

NIST SP 800-53r3	SC-11
API 1164r2	8.1, Annex A
NRC RG 5.71	App. B.1.22, App. B.3.9

2.8.11 Cryptographic Key Establishment and Management

2.8.11.1 Requirement

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.

2.8.11.2 Supplemental Guidance

Organizations need to select cryptographic protection that matches the value of the information being protected and the control system operating constraints. A formal written policy needs to be developed to document the practices and procedures relating to cryptographic key establishment and management. These policies and procedures need to address, under key establishment, such items as key generation process in accordance with a specified algorithm and key sizes based on an assigned standard. Key generation must be performed using an effective random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution in accordance with defined standards.

2.8.11.3 Requirement Enhancements

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

2.8.11.4 References

NIST SP 800-53r3	SC-12
NRC RG 5.71	App. B.3.9

2.8.12 Use of Validated Cryptography

2.8.12.1 Requirement

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.

2.8.12.2 Supplemental Guidance

Any cryptographic modules deployed within a control system, at a minimum, must be able to meet the FIPS 140-2. Assessment of the modules must include validation of the cryptographic modules operating in approved modes of operation. The most effective safeguard is to use a cryptographic module

validated by the Cryptographic Module Validation Program. Additional information on the use of validated cryptography can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html.

2.8.12.3 Requirement Enhancements

1. The organization protects cryptographic hardware from physical tampering and uncontrolled electronic connections.
2. The organization selects cryptographic hardware with remote key management capabilities.

2.8.12.4 References

NIST SP 800-53r3	SC-13
CAG	CC-15
NRC RG 5.71	App. B.3.10

2.8.13 Collaborative Computing Devices

2.8.13.1 Requirement

The use of collaborative computing devices on the control system is strongly discouraged. If use is authorized and allowed by the organization, explicit indication of use is provided to users physically present at the devices.

2.8.13.2 Supplemental Guidance

Collaborative computing devices include video and audio conferencing capabilities, networked information boards, or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and microphones are activated.

2.8.13.3 Requirement Enhancements

1. If collaborative computing devices are used on the control system, they are disconnected and powered down when not in use.
2. The control system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.
3. The organization disables or removes collaborative computing devices from control systems in organization-defined secure work areas.

2.8.13.4 References

NIST SP 800-53r3	SC-15
API 1164r2	7.15, 7.3, Annex B.3.1.4.3
NRC RG 5.71	App. B.3.11

2.8.14 Transmission of Security Attributes

2.8.14.1 Requirement

The control system reliably associates security attributes (e.g., security labels and markings) with information exchanged between the enterprise systems and the control system.

2.8.14.2 Supplemental Guidance

Security attributes may be explicitly or implicitly associated with the information contained within the control system. For example, security labels are often used in data structures to associated attributes with specific information objects such as user access privileges, nationality, or affiliation as a contractor.

2.8.14.3 Requirement Enhancements

The control system validates the integrity of security parameters exchanged between systems.

2.8.14.4 References

NIST SP 800-53r3 SC-16

NRC RG 5.71 App. B.3.12

2.8.15 Public Key Infrastructure Certificates

2.8.15.1 Requirement

The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

2.8.15.2 Supplemental Guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

2.8.15.3 Requirement Enhancements

Any latency induced from the use of public key certificates must not degrade the operational performance of the control system.

2.8.15.4 References

NIST SP 800-53r3 SC-17

NRC RG 5.71 App. B.1.22, App. B.3.13

2.8.16 Mobile Code

2.8.16.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the control system if used maliciously
2. Documents, monitors, and manages the use of mobile code within the control system. Appropriate organizational officials authorize the use of mobile code.

2.8.16.2 Supplemental Guidance

Mobile code technologies include Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures need to prevent the development, acquisition, or introduction of unacceptable mobile code within the control system. Additional information on risk-based approaches for the implementation of mobile code technologies can be found at http://iase.disa.mil/mcp/index.html. This link to the Mobile Code Policy and Guidance has been moved to the Department of Defense Public Key Infrastructure (PKI)-certified protected area of Information Assurance Support Environment (IASE) A person must have the proper authority for access to this document.

2.8.16.3 Requirement Enhancements

The control system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

2.8.16.4 References

NIST SP 800-53r3	SC-18
CAG	CC-5, CC-12
NRC RG 5.71	App. B.1.22, App. B.3.14

2.8.17 Voice-Over Internet Protocol

2.8.17.1 Requirement

The organization: (1) establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the system if used maliciously and (2) authorizes, monitors, and controls the use of VoIP within the control system.

2.8.17.2 Supplemental Guidance

Generally, VoIP technologies should not be employed on control systems. Usage should be determined after careful consideration and after verification that it does not adversely impact the operational parameters of the ICS.

2.8.17.3 Requirement Enhancements

None

2.8.17.4 References

NIST SP 800-53r3	SC-19
API 1164r2	7.3.6

2.8.18 System Connections

2.8.18.1 Requirement

All external control system and communication connections are identified and protected from tampering or damage.

2.8.18.2 Supplemental Guidance

External access point connections to the control system need to be secured to protect the system. Access points include any externally connected communication end point (for example, dialup modems) terminating at any device within the electronic security perimeter. The first step in securing these connections is to identify the connections along with the purpose and necessity of the connection. This information needs to be documented, tracked, and audited periodically. After identifying these connection points, the extent of their protection needs to be determined. Policies and procedures need to be developed and implemented to protect the connection to the business or enterprise system. This might include disabling the connection except when specific access is requested for a specific need, automatic timeout for the connection, etc.

2.8.18.3 Requirement Enhancements

None

2.8.18.4 References

NIST SP 800-53r3	CA-3
CAG	CC-5
API 1164r2	3.6, Annex B.1, B.2, B.3
NERC CIPS	CIP 005-3. B.R1 through R1.3

NRC RG 5.71	C.3.1.3, C.3.1.4, App. B.1.1, App. B.1.22, App. B.4.5, App. B.5.2, App. C.3.4, App. C.7, App. C.9.1, App. C.11.3

2.8.19 Security Roles

2.8.19.1 Requirement

The control system design and implementation specifies the security roles and responsibilities for the users of the system.

2.8.19.2 Supplemental Guidance

Security roles and responsibilities for control system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals.

2.8.19.3 Requirement Enhancements

None

2.8.19.4 References

NIST SP 800-53r3	AC-5, PS-2
API 1164r2	1.2, Annex A
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	C.3.3.1.1, App. B.1.1, App. B.1.22, App. C.10.10

2.8.20 Session Authenticity

2.8.20.1 Requirement

The control system provides mechanisms to protect the authenticity of device-to-device communications sessions.

2.8.20.2 Supplemental Guidance

Message authentication provides protection from malformed traffic from misconfigured devices and malicious entities. The intent is to establish confidence at each end of a communications session with respect to the validity of the data and the identity of the sender. This is to address man-in-the middle attacks, which can include session hijacking, insertion of fake information, or instruction sets in the middle of a session.

In situations where the ICS cannot protect the authenticity of communications sessions, the organization employs compensating controls (e.g., auditing measures, isolation/segmented architecture, additional physical isolation). Enhanced auditing measures or encryption mechanisms designed to enhance session authenticity must not impact ICS operations by consuming too many available resources or by slowing down communications to an unacceptable level as to constitute a self-inflicted denial-of-service attack.

2.8.20.3 Requirement Enhancements

Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.

2.8.20.4 References

NIST SP 800-53r3	SC-23
API 1164r2	5.9, 7.2.2, 8.1, Annex A, Annex B.1, B.2, B.3

NRC RG 5.71	App. 3.1.1, App. B.3.6, App. B.3.18

2.8.21 Architecture and Provisioning for Name/Address Resolution Service

2.8.21.1 Requirement

The control system devices that collectively provide name/address resolution services for an organization are fault tolerant and implement address space separation.

2.8.21.2 Supplemental Guidance

In general, do not use domain name system (DNS) services on a control system. Host-based name resolution solutions are the recommended practice. However, if DNS services are implemented, deploy at least two authoritative DNS servers. The DNS configuration on the host will reference one DNS server as the primary source and the other as the secondary source. In addition, locate the two DNS servers on different network subnets and separate geographically. If control system resources are accessible from external networks, establish authoritative DNS servers with separate address space views (internal and external) to the control system resources. The DNS server with the internal view provides name/address resolution services within the control system boundary. The DNS server with the external view only provides name/address resolution information pertaining to control system resources accessible from external resources. The list of clients who can access the authoritative DNS server with a particular view is also specified.

2.8.21.3 Requirement Enhancements

The use of secure name/address resolution services must not adversely impact the operational performance of the control system.

2.8.21.4 References

NIST SP 800-53r3	SC-22
CAG	CC-16
NRC RG 5.71	App. B.3.6, App. B.3.17

2.8.22 Secure Name/Address Resolution Service (Authoritative Source)

2.8.22.1 Requirement

The control system resource (i.e., authoritative DNS server) that provides name/address resolution service provides additional artifacts (e.g., digital signatures and cryptographic keys) along with the authoritative DNS resource records it returns in response to resolution queries.

2.8.22.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. This requirement enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A DNS server is an example of control system resource that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data.

2.8.22.3 Requirement Enhancements

The control system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

2.8.22.4 References

NIST SP 800-53r3	SC-20
CAG	CC-16
NRC RG 5.71	App. B.3.15

2.8.23 Secure Name/Address Resolution Service (Recursive or Caching Resolver)

2.8.23.1 Requirement

The control system resource (i.e., resolving or caching name server) that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative DNS servers when requested by client systems.

2.8.23.2 Supplemental Guidance

In general, do not use DNS services on a control system. Host-based name resolution solutions are best practice. A resolving or caching DNS server is an example of a control system resource that provides name/address resolution service for local clients, and authoritative DNS servers are examples of authoritative sources.

2.8.23.3 Requirement Enhancements

The control system resource that implements DNS services performs data origin authentication and data integrity verification on all resolution responses whether local DNS clients (i.e., stub resolvers) explicitly request this function.

2.8.23.4 References

NIST SP 800-53r3	SC-21
CAG	CC-16
NRC RG 5.71	App. B.3.16, App. B.3.18, App. B.4.4

2.8.24 Fail in Known State

2.8.24.1 Requirement

The control system fails to a known state for defined failures.

2.8.24.2 Supplemental Guidance

Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the control system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property.

2.8.24.3 Requirement Enhancements

The control system preserves defined system state information in failure.

2.8.24.4 References

NIST SP 800-53r3	SC-24
CAG	CC-14
NRC RG 5.71	App. B.1.17, App. B.3.22

2.8.25 Thin Nodes

2.8.25.1 Requirement

The control system employs processing components that have minimal functionality and data storage.

2.8.25.2 Supplemental Guidance

The deployment of control system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, control systems, and services to a successful attack.

2.8.25.3 Requirement Enhancements

Use secure data transmission media, such as fiber optic technology, to minimize data loss from eavesdropping and data tapping.

2.8.25.4 References

NIST SP 800-53r3 SC-25

NRC RG 5.71 App. B.3.19

2.8.26 Honeypots

2.8.26.1 Requirement

The control system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks.

2.8.26.2 Supplemental Guidance

Not all ICS users should use honeypots. Only specialized entities using nonoperational equipment in highly isolated and protected zones should attempt deployment of honeypots. Created honeypots determine if active entities are attacking/probing the particular configuration the honeypot is mimicking. If deployed incorrectly, this technique can lead to a direct shortcut of established cybersecurity measures. This is a very specialized and limited application and should not be widely used.

2.8.26.3 Requirement Enhancements

The control system includes components that proactively seek to identify web-based malicious code.

2.8.26.4 References

NIST SP 800-53r3 SC-26

CAG CC-12

2.8.27 Operating System-Independent Applications

2.8.27.1 Requirement

The control system includes organization-defined applications that are independent of the operating system.

2.8.27.2 Supplemental Guidance

Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system.

2.8.27.3 Requirement Enhancements

None

2.8.27.4 References

NIST SP 800-53r3 SC-27

NRC RG 5.71 App. C.12.5

2.8.28 Confidentiality of Information at Rest

2.8.28.1 Requirement

The control system protects the confidentiality of information at rest. Examples of data at rest are: configuration files and settings, alarm point setting, password files, and security filter rules.

2.8.28.2 Supplemental Guidance

This control is intended to address the confidentiality of information in nonmobile devices.

2.8.28.3 Requirement Enhancements

The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

2.8.28.4 References

NIST SP 800-53r3 SC-28

CAG CC-15

API 1164r2 Annex A

NRC RG 5.71 App. B.3.20

2.8.29 Heterogeneity

2.8.29.1 Requirement

The organization employs diverse technologies in the implementation of the control system.

2.8.29.2 Supplemental Guidance

Increasing the diversity of technologies within the control system reduces the impact from the exploitation of a specific technology.

2.8.29.3 Requirement Enhancements

None

2.8.29.4 References

NIST SP 800-53r3 SC-29

NRC RG 5.71 App. B.3.21

2.8.30 Virtualization Techniques

2.8.30.1 Requirement

The organization employs virtualization techniques to present gateway components into control systems environments as other types of components or components with differing configurations.

2.8.30.2 Supplemental Guidance

Virtualization techniques provide organizations with the ability to disguise gateway components into control systems environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

2.8.30.3 Requirement Enhancements

1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications.
2. The organization changes the diversity of operating systems and applications on an organization-defined frequency.
3. The organization employs randomness in the implementation of the virtualization.

2.8.30.4 References

NIST SP 800-53r3	SC-30
CAG	CC-5

2.8.31 Covert Channel Analysis

2.8.31.1 Requirement

The organization requires that control system developers/integrators perform covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

2.8.31.2 Supplemental Guidance

Control system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when the potential exists for unauthorized information flows across security domains in the case of control systems containing export controlled information and having connections to the Internet.

2.8.31.3 Requirement Enhancements

The organization tests a subset of the vendor identified covert channel avenues to determine if they are exploitable.

2.8.31.4 References

NIST SP 800-53r3	SC-31
CAG	CC-5

2.8.32 Information System Partitioning

2.8.32.1 Requirement

The organization partitions the information system into components residing in separate physical domains (or environments) as necessary.

2.8.32.2 Supplemental Guidance

Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning when system components can be associated with different system impact levels derived from the categorizations. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components.

2.8.32.3 Requirement Enhancements

None

2.8.32.4 References

NIST SP 800-53r3 SC-32

NRC RG 5.71 App. B.3.2.2

2.8.33 Transmission Preparation Integrity

2.8.33.1 Requirement

The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

2.8.33.2 Supplemental Guidance

Information can be subjected to unauthorized changes (i.e., malicious and unintentional modification) at information aggregation or protocol transformation points.

2.8.33.3 Requirement Enhancements

None

2.8.33.4 References

NIST SP 800-53r3 SC-33

NRC RG 5.71 App. B.3.6

2.8.34 Non-Modifiable Executable Programs

2.8.34.1 Requirement

The information system:

1. Loads and executes the operating system software from hardware-enforced, read-only media
2. Loads and executes authorized applications from hardware-enforced, read-only media.

2.8.34.2 Supplemental Guidance

In this control, operating system software is defined as the base code on which applications are hosted. Hardware-enforced, read-only media include CD-R/DVD-Rs. The use of nonmodifiable storage media ensures the integrity of the software from the point of creation as a read-only image.

2.8.34.3 Requirement Enhancements

1. The organization employs system components with no writable storage that is persistent across component restart or power on/off cycles.

   Enhanced Supplemental Guidance—This control enhancement eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system component and requires that no removable storage be employed.

2. The Organization protects the integrity of the information on read-only media.

   Enhanced Supplemental Guidance—This control enhancement covers protection of the integrity of information placed on read-only media, controlling the media after information has been recorded onto the media. Measures may include a combination of prevention and detection/response.

2.8.34.4 References

NIST SP 800-53r3 SC-34

2.9 Information and Document Management

Information and document management is generally a part of the company records retention and document management system. Digital and hardcopy information associated with the development and execution of a control system is important and sensitive and needs to be managed. Control system design, operations data and procedures, risk analyses, business impact studies, risk tolerance profiles, etc., contain sensitive company information and need to be protected. Security measures, philosophy, and implementation strategies are other examples. In addition, business conditions change and require updated analyses and studies. Care is given to protect this information and verify that the appropriate versions are retained. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection.

The following are the controls for Information and Document Management that need to be supported and implemented by the organization to protect the control system.

2.9.1 Information and Document Management Policy and Procedures

2.9.1.1 Requirement

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.

2.9.1.2 Supplemental Guidance

The organization ensures the control system information and document management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system information and document management policy can be included as part of the general information security policy for the organization. System information and document management procedures can be developed for the security program in general and for a particular control system when required.

2.9.1.3 Requirement Enhancements

None

2.9.1.4 References

NIST SP 800-53r3	SI-1
API 1164r2	Annex A
NERC CIPS	CIP 002-3. through CIP 009-3
NRC RG 5.71	App. C.3.1, App. C.11

2.9.2 Information and Document Retention

2.9.2.1 Requirement

The organization manages control system-related data, including establishing retention policies and procedures for both electronic and paper data and manages access to the data based on formally assigned roles and responsibilities.

2.9.2.2 Supplemental Guidance

The organization develops policies and procedures detailing the retention of company information. These procedures address retention/destruction issues for all applicable information media. Any legal or regulatory requirements are considered when developing these policies and procedures. Information associated with the development and execution of a control system is important, sensitive, and needs to be appropriately managed. The National Archives and Records Administration provides guidance on records retention.

2.9.2.3 Requirement Enhancements

The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations.

2.9.2.4 References

NIST SP 800-53r3	SI-12
API 1164r2	Annex A
NERC CIPS	CIP 003-3.B.R4
NRC RG 5.71	C.5, App. B.2.11, App. C.3.4, App. C.3.10

2.9.3 Information Handling

2.9.3.1 Requirement

Organization implemented policies and procedures detailing the handling of information are developed and periodically reviewed and updated.

2.9.3.2 Supplemental Guidance

Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of control system information. These policies or procedures include the periodic review of all information to ensure it is properly handled. The organization protects information against unauthorized access, misuse, or corruption during transportation or transmission. The organization distributes or shares information on a need-to-know basis and considers legal and regulatory requirements when developing these policies and procedures.

2.9.3.3 Requirement Enhancements

None

2.9.3.4 References

NIST SP 800-53r3	MP-1, SI-12
API 1164r2	Annex A
NERC CIPS	CIP 002-3. B.R4.1
NRC RG 5.71	App. B.3.1, App. C.1.2

2.9.4 Information Classification

2.9.4.1 Requirement

All information is classified to indicate the protection required commensurate with its sensitivity and consequence.

2.9.4.2 Supplemental Guidance

A minimum of three levels of classification should be defined for control system information to indicate the protection required commensurate with its sensitivity and consequence. These levels may be company proprietary, restricted, or public, indicating the need, priority, and level of protection required for that information. These information classification levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required.

2.9.4.3 Requirement Enhancements

None

2.9.4.4 References

NIST SP 800-53r3	RA-2
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3. B.R4.2
NRC RG 5.71	App. C.8.4

2.9.5 Information Exchange

2.9.5.1 Requirement

Formal contractual and confidentiality agreements are established for the exchange of information and software between the organization and external parties.

2.9.5.2 Supplemental Guidance

When it is necessary for the control system to communicate information to another organization or external party system, the operators need to mutually develop a formal contractual and confidentiality agreement and use a secure method of communication. These formal exchange policies, procedures, and security controls need to be in place to protect the exchange of information using all types of communication facilities.

2.9.5.3 Requirement Enhancements

If a specific device needs to communicate with another device outside the control system network, communications need to be limited to only the devices that need to communicate. All other ports and routes need to be locked down or disabled.

2.9.5.4 References

NIST SP 800-53r3	SC-16
API 1164r2	Annex A
NERC CIPS	CIP 003-3. B.R5
NRC RG 5.71	App. B.3.12

2.9.6 Information and Document Classification

2.9.6.1 Requirement

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.

2.9.6.2 Supplemental Guidance

Companies use both comprehensive information and document management policies for their cybersecurity management system. Inherent in this is an information classification system that allows information assets to receive the appropriate level of protection. The organization defines information classification levels (e.g., restricted, classified, general) for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required. The organization also classifies all information (i.e., control system design information, network diagrams, process programs, vulnerability assessments) to indicate the need, priority, and level of protection required commensurate with its sensitivity and consequence.

2.9.6.3 Requirement Enhancements

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

2.9.6.4 References

NIST SP 800-53r3	AC-1, AC-3, MP-1, MP-3
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3. B.R4.2
NRC RG 5.71	App. B.3.1, App. C.1.3

2.9.7 Information and Document Retrieval

2.9.7.1 Requirement

The organization develops policies and procedures that provide details of the retrieval of written and electronic records, equipment, and other media for the control system in the overall information and document management policy.

2.9.7.2 Supplemental Guidance

The organization employs appropriate measures to ensure long-term records information can be retrieved (i.e., converting the data to a newer format, retaining older equipment that can read the data). Any legal or regulatory requirements are considered when developing these policies and procedures. The organization takes special care to confirm the security, availability, and usability of the control system configuration, which includes the logic used in developing the configuration or programming for the life of the control system.

2.9.7.3 Requirement Enhancements

None

2.9.7.4 References

NIST SP 800-53r3	AC-1
API 1164r2	Annex A
NRC RG 5.71	App. C.1.2

2.9.8 Information and Document Destruction

2.9.8.1 Requirement

The organization develops policies and procedures detailing the destruction of written and electronic records, equipment, and other media for the control system, without compromising the confidentiality of the data.

2.9.8.2 Supplemental Guidance

The organization develops policies and procedures detailing the destruction and disposal of written and electronic records, equipment, and other media in the overall information and document management policy. This also includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. All legal or regulatory requirements need to be considered when developing these policies and procedures.

2.9.8.3 Requirement Enhancements

None

2.9.8.4 References

API 1164r2	Annex A
NRC RG 5.71	App. C.1.2

2.9.9 Information and Document Management Review

2.9.9.1 Requirement

The organization performs periodic reviews of compliance with the control system information and document security management policy to ensure compliance with any laws and regulatory requirements.

2.9.9.2 Supplemental Guidance

The organization periodically reviews compliance in the information and document management security policy. The compliance review procedure needs to consider all legal and regulatory documentation requirements applicable to the control system.

2.9.9.3 Requirement Enhancements

None

2.9.9.4 References

API 1164r2	1.2, Annex A
NERC CIPS	CIP 003-3. D
NRC RG 5.71	App. B.2.3, App. C.1.2

2.9.10 Media Marking

2.9.10.1 Requirement

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).

2.9.10.2 Supplemental Guidance

The term marking is distinguished from the term labeling. Marking is used in security controls when referring to information that is human-readable. The term labeling is used in the context of marking internal data structures within the system for access control purposes for information in process, in storage, or in transit. Removable system media include both digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs, diskettes) and nondigital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, marking is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations may require marking for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information including monitors and printers. Marking of removable media and information system output is consistent with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance.

2.9.10.3 Requirement Enhancements

None

2.9.10.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	Annex A
NRC RG 5.71	App. C.1.3

2.9.11 Security Attributes

2.9.11.1 Requirement

The control system supports and maintains the binding of user-defined security attributes to information in storage, in process, and in transmission in accordance with:

1. Access control requirements
2. Special dissemination, handling, or distribution instructions
3. Otherwise, as required by the system security policy.

2.9.11.2 Supplemental Guidance

Security attributes are specified characteristics used on internal data structures to enable the implementation of access control, flow control, special dissemination, handling, or distribution instructions or to support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (e.g., user access privileges, nationality, and contractor affiliation). Such labels are often used to implement access control and flow control policies.

2.9.11.3 Requirement Enhancements

1. The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.
2. The information system allows authorized entities to change security attributes.

3. The information system maintains the binding of security attributes to information with sufficient assurance that the information attribute association can be used as the basis for automated policy actions.

   Enhanced Supplemental Guidance—Examples of automated policy actions include automated access control decisions (e.g., mandatory Access Control decisions) or decisions to release/or not release information (e.g., information flows via cross domain systems).

4. The information system allows authorized users to associate security attributes with information

   Enhanced Supplemental Guidance—The support provided by the information system can vary from prompting users to select security attributes to be associated with specific information objects, to ensure that the combination of attributes selected is valid.

5. The information system displays security attributes in human-readable form on each object-output from the system-to-system output devices to identify special dissemination, handling, or distribution instructions.

   Enhanced Supplemental Guidance—Objects output from the information system include pages, screens, or equivalent. Output devices include printers, video displays on computer terminals, monitors, screens on HMIs, notebooks/laptop computer, and personal digital assistants.

2.9.11.4 References

NIST SP 800-53r3 AC-16

NRC RG 5.71 App. C.1.3

2.10 System Development and Maintenance

Security is most effective when it is designed into the control system and sustained, through effective maintenance, throughout the life cycle of the system and through all future configurations. Maintenance activities encompass appropriate policies and procedures for performing routine and preventive maintenance on the components of a control system. This includes the use of both local and remote maintenance tools and management of maintenance personnel.

2.10.1 System Maintenance Policy and Procedures

2.10.1.1 Requirement

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

1. A formal, documented, control system maintenance 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 maintenance policy and associated system maintenance controls.

2.10.1.2 Supplemental Guidance

The organization ensures the control system maintenance policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The control system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular control system when required.

2.10.1.3 Requirement Enhancements

None

2.10.1.4 References

NIST SP 800-53r3	MA-1
API 1164r2	3.6, Annex A
NERC CIPS	CIP 007-3. A
NRC RG 5.71	C.3.3.2.4, C.4, App. C.4.1

2.10.2 Legacy System Upgrades

2.10.2.1 Requirement

The organization develops policies and procedures to upgrade existing legacy control systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the system and processes controlled.

2.10.2.2 Supplemental Guidance

Legacy systems are those control systems currently in place for control of the organization's processes. In some cases, these systems were installed before a concern about system security existed, and hence, security mitigation measures were not included. The organization determines the current configuration of the control system and then provides system upgrades as required to meet the organization's security requirements.

2.10.2.3 Requirement Enhancements

None

2.10.2.4 References

NIST SP 800-53r3	SA-8
CAG	CC-7, CC-16
API 1164r2	Annex B.3.1.6.2
NRC RG 5.71	App. C.12.4

2.10.3 System Monitoring and Evaluation

2.10.3.1 Requirement

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.

2.10.3.2 Supplemental Guidance

Control systems need to be monitored and evaluated according to the risk management plan periodically to identify vulnerabilities or conditions that might affect the security of a control system. The frequency of these evaluations needs to be based on the organization's risk mitigation policy. Changing security requirements and vulnerabilities necessitate a system review. These reviews need to be carefully planned and documented in accordance with the organization configuration management policy to identify any changes to the system. The organization maintains contact with other organizations that have similar systems to determine changing vulnerabilities.

2.10.3.3 Requirement Enhancements

None

2.10.3.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17
API 1164r2	3.3, Annex B.2.1
NERC CIPS	CIP 007-3. B.R6
NRC RG 5.71	C.4.1.2

2.10.4 Backup and Recovery

2.10.4.1 Requirement

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.

2.10.4.2 Supplemental Guidance

Control system operating software may be compromised due to an incident or disaster. A copy of the operating system software needs to be made, updated regularly, and stored in a secure environment so that it can be used to restore the control system to normal operations. In many instances, a backup control site can serve this purpose.

2.10.4.3 Requirement Enhancements

None

2.10.4.4 References

NIST SP 800-53r3	CP-6, CP-10
CAG	CC-13
API 1164r2	3.4, Annex A
NERC CIPS	CIP 009-3 B.R4
NRC RG 5.71	App. C.8.1, App. C.9.1, App. C.9.5, App. C.9.6, App. C.9.7

2.10.5 Unplanned System Maintenance

2.10.5.1 Requirement

The organization reviews and follows security requirements for a control system before undertaking any unplanned maintenance activities of control system components (including field devices). Documentation includes the following:

1. The date and time of maintenance
2. The name of the individual(s) performing the maintenance
3. The name of the escort, if necessary
4. A description of the maintenance performed
5. A list of equipment removed or replaced (including identification numbers, if applicable).

2.10.5.2 Supplemental Guidance

Unplanned maintenance is required to support control system operation in the event of system/component malfunction or failure. Security requirements necessitate that all unplanned

maintenance activities use approved contingency plans and document all actions taken to restore operability to the system.

2.10.5.3 Requirement Enhancements

The organization documents the decision and justification should unplanned maintenance not be performed on a control system after the identification of a security vulnerability.

2.10.5.4 References

API 1164r2	3.4, 3.8, Annex A, Annex B.3.1
NRC RG 5.71	App. C.3.11, App. C.4.1

2.10.6 Periodic System Maintenance

2.10.6.1 Requirement

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on system components in accordance with manufacturer or vendor specifications and/or organizational requirements
2. Explicitly approves the removal of the system or system components from organizational facilities for offsite maintenance or repairs
3. Sanitizes the equipment to remove all information from associated media prior to removal from organizational facilities for offsite maintenance or repairs
4. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

2.10.6.2 Supplemental Guidance

The control is intended to address the security aspects of the organization's system maintenance program. All maintenance activities to include routine, scheduled maintenance and repairs are controlled whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Maintenance procedures that require the physical removal of any control system component need to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components. These activities need to be approved by the appropriate organization officials. If the control system or component requires offsite repair, the organization removes all critical/sensitive information from associated media using approved procedures. After maintenance is performed on the control system, the organization checks the security features to ensure that they are still functioning properly.

2.10.6.3 Requirement Enhancements

1. The organization maintains maintenance records for the system that include (a) the date and time of maintenance; (b) name of the individual performing the maintenance; (c) name of escort, if necessary; (d) a description of the maintenance performed; and (e) a list of equipment removed or replaced (including identification numbers, if applicable).
2. The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

2.10.6.4 References

NIST SP 800-53r3 MA-2

NRC RG 5.71 App. C.4.1

2.10.7 Maintenance Tools

2.10.7.1 Requirement

The organization approves and monitors the use of system maintenance tools.

2.10.7.2 Supplemental Guidance

The intent of this control is to address the security-related issues arising from the hardware and software brought into the system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and software components that may support system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch), are not covered by this control.

2.10.7.3 Requirement Enhancements

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.
2. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the system.
3. The organization prevents the unauthorized removal of maintenance equipment by one of the following: (a) verifying that no organizational information is contained on the equipment, (b) sanitizing or destroying the equipment, (c) retaining the equipment within the facility, or (d) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.
4. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.
5. Maintenance tools are used with care on control system networks to ensure that control system operations will not be degraded by their use.

2.10.7.4 References

NIST SP 800-53r3 MA-3

API 1164r2 5.8, Annex B.4.11

NRC RG 5.71 App. C.4.2

2.10.8 Maintenance Personnel

2.10.8.1 Requirement

The organization documents authorization and approval policies and procedures and maintains a list of personnel authorized to perform maintenance on the control system. Only authorized and qualified organization or vendor personnel perform maintenance on the control system.

2.10.8.2 Supplemental Guidance

Maintenance personnel need to have appropriate access authorization to the control system when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the control system.

2.10.8.3 Requirement Enhancements

None

2.10.8.4 References

NIST SP 800-53r3	MP-5
API 1164r2	3.1, Annex A
NRC RG 5.71	App. B.1.22, App. C.4.3

2.10.9 Non-Local (Remote) Maintenance

2.10.9.1 Requirement

The organization:

1. Authorizes and monitors and controls remotely executed maintenance and diagnostic activities
2. Allows the use of remote maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system
3. Maintains records for remote maintenance and diagnostic activities
4. Terminates all sessions and remote connections when remote maintenance is completed
5. Changes passwords following each remote maintenance session, if password-based authentication is used to accomplish remote maintenance.

2.10.9.2 Supplemental Guidance

Individuals communicating through an external, nonorganization-controlled network (e.g., the Internet) conduct remote maintenance and diagnostic activities. Identification and authentication techniques used in remote maintenance and diagnostic sessions are consistent with Section 2.15.1, "Access Control Policy and Procedures." Strong authentication and enforcement requirements are in other controls in Section 2.8, "System and Communications Protection"; Section 2.10, "System Development and Maintenance"; Section 2.14, "System and Information Integrity"; and Section 2.15, "Access Controls."

2.10.9.3 Requirement Enhancements

1. The organization audits remote maintenance and diagnostic sessions, and designated organizational personnel review the maintenance records of the remote sessions.
2. The organization documents the installation and use of remote maintenance and diagnostic links.
3. The organization:
   a. Requires that remote maintenance or diagnostic services be performed from a system that implements a level of security at least as high as that implemented on the system being serviced or
   b. Removes the component to be serviced from the system and prior to remote maintenance or diagnostic services, sanitizes the component (e.g., clearing of set points, embedded network addresses and embedded security validation information) before removal from organizational facilities. After the service is performed and the component is returned to the facility, the organization should check or reinstall the authorized firmware code as specified by the configuration management plan and reset all authorized embedded configuration settings. This should remove potentially malicious software that may have been added via "new" firmware. This should be done before reconnecting the component to the system.

4. The organization requires that remote maintenance sessions be protected by a strong authenticator tightly bound to the user.
5. The organization requires that
   a. Maintenance personnel notify the system administrator when remote maintenance is planned (i.e., date/time)
   b. A designated organizational official with specific security/system knowledge approves the remote maintenance.
6. The organization employs cryptographic mechanisms to protect the integrity and confidentiality of remote maintenance and diagnostic communications.
7. The organization employs remote disconnect verification at the termination of remote maintenance and diagnostic sessions.

2.10.9.4 References

NIST SP 800-53r3	MA-4
API 1164r2	5, 8.1, 8.2.4, Annex A
NRC RG 5.71	App. B.1.22, App. B.3.11

2.10.10 Timely Maintenance

2.10.10.1 Requirement

The organization obtains maintenance support and spare parts for organization-defined list of security-critical system components within organization-defined period of failure.

2.10.10.2 Supplemental Guidance

The organization specifies those system components that, when not operational, result in increased risk to organizations, individuals, or the nation because the security functionality intended by that component is not being provided. Security-critical components include firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

2.10.10.3 Requirement Enhancements

None

2.10.10.4 References

NIST SP 800-53r3	MA-6
API 1164r2	Annex A
NERC CIPS	CIP 008-3 B.R8, CIP 009-3 B.R4
NRC RG 5.71	C.3.3.2.4, App. C.4.1

2.11 Security Awareness and Training

Physical and cyber control system security awareness is a critical part of control system incident prevention, particularly with regard to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information such as passwords. This information can then be used to compromise otherwise secure systems. Implementing a control system security program may change the way personnel access computer programs and applications, so organizations need to design effective training programs based on individuals' roles and responsibilities. Communication vehicles need to be developed to help employees understand why new access and control methods are required and how they can reduce risks and impacts to the organization. Training programs also need to