

# Catalog of Control Systems Security: Recommendations for Standards Developers

*January 2008*



**Homeland  
Security**

## **National Cyber Security Division**

**Control Systems  
Security Program**





## **ACKNOWLEDGEMENT**

This document was developed for the U.S. Department of Homeland Security to help facilitate the development of control system cyber security industry standards. The author team consisted of representatives from the National Institute of Standards and Technology and Department of Energy National Laboratories (Argonne National Laboratory, Idaho National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories).

For additional information or comments please send inquires to the Control Systems Security Program at [cssp@hq.dhs.gov](mailto: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 18 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 but can be used by all sectors to develop a framework needed to produce a sound cyber security program. It should be viewed as a collection of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security 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 cyber security standards specific to their individual security needs.



# CONTENTS

1.	INTRODUCTION.....	1
2.	Recommendations for Standards Developers.....	3
2.1	Security Policy.....	3
2.1.1	Security Policy and Procedures.....	3
2.2	Organizational Security.....	5
2.2.1	Management Policy and Procedures.....	5
2.2.2	Management Accountability.....	5
2.2.3	Baseline Practices.....	5
2.2.4	Coordination of Threat Mitigation.....	6
2.2.5	Security Policies for Third Parties.....	6
2.2.6	Termination of Third-Party Access.....	7
2.3	Personnel Security.....	8
2.3.1	Personnel Security Policy and Procedures.....	8
2.3.2	Position Categorization.....	8
2.3.3	Personnel Screening.....	9
2.3.4	Personnel Termination.....	9
2.3.5	Personnel Transfer.....	9
2.3.6	Access Agreements.....	10
2.3.7	Third-Party Personnel Security.....	10
2.3.8	Personnel Accountability.....	10
2.3.9	Personnel Roles.....	11
2.4	Physical and Environmental Security.....	12
2.4.1	Physical and Environmental Security Policy and Procedures.....	12
2.4.2	Physical Access Authorizations.....	12
2.4.3	Physical Access Control.....	13
2.4.4	Monitoring Physical Access.....	13
2.4.5	Visitor Control.....	14
2.4.6	Visitor Records.....	14
2.4.7	Physical Access Log Retention.....	14
2.4.8	Emergency Shutoff.....	15
2.4.9	Emergency Power.....	15
2.4.10	Emergency Lighting.....	15
2.4.11	Fire Protection.....	15
2.4.12	Temperature and Humidity Controls.....	16
2.4.13	Water Damage Protection.....	16
2.4.14	Delivery and Removal.....	16
2.4.15	Alternate Work Site.....	17
2.4.16	Portable Media.....	17
2.4.17	Personnel and Asset Tracking.....	17
2.4.18	Location of Control System Assets.....	18
2.4.19	Information Leakage.....	18
2.4.20	Power Equipment and Power Cabling.....	18
2.4.21	Physical Device Access Control.....	19
2.5	System and Services Acquisition.....	20
2.5.1	System and Services Acquisition Policy and Procedures.....	20
2.5.2	Allocation of Resources.....	20

2.5.3	Life-Cycle Support.....	21
2.5.4	Acquisitions .....	21
2.5.5	Control System Documentation .....	21
2.5.6	Software License Usage Restrictions.....	22
2.5.7	User-Installed Software.....	22
2.5.8	Security Engineering Principles.....	23
2.5.9	Outsourced Control System Services.....	23
2.5.10	Vendor Configuration Management .....	23
2.5.11	Vendor Security Testing .....	24
2.5.12	Vendor Life Cycle Practices .....	24
2.6	Configuration Management .....	25
2.6.1	Configuration Management Policy and Procedures.....	25
2.6.2	Baseline Configuration .....	25
2.6.3	Configuration Change Control.....	26
2.6.4	Monitoring Configuration Changes .....	27
2.6.5	Access Restrictions for Configuration Change .....	27
2.6.6	Configuration Settings .....	27
2.6.7	Configuration for Least Functionality.....	28
2.6.8	Configuration Assets.....	28
2.6.9	Addition, Removal, and Disposal of Equipment .....	29
2.6.10	Factory Default Authentication Management.....	29
2.7	Strategic Planning .....	30
2.7.1	Strategic Planning Policy and Procedures.....	30
2.7.2	Control System Security Plan .....	30
2.7.3	Interruption Identification and Classification .....	31
2.7.4	Roles and Responsibilities .....	31
2.7.5	Planning Process Training .....	32
2.7.6	Testing.....	32
2.7.7	Investigate and Analyze .....	32
2.7.8	Corrective Action.....	33
2.7.9	Risk Mitigation .....	33
2.7.10	System Security Plan Update .....	33
2.7.11	Rules of Behavior.....	33
2.7.12	Security-Related Activity Planning.....	34
2.8	System and Communication Protection .....	35
2.8.1	System and Communication Protection Policy and Procedures .....	35
2.8.2	Management Port Partitioning .....	35
2.8.3	Security Function Isolation .....	36
2.8.4	Information Remnants.....	36
2.8.5	Denial-of-Service Protection.....	36
2.8.6	Resource Priority.....	37
2.8.7	Boundary Protection .....	37
2.8.8	Communication Integrity .....	38
2.8.9	Communication Confidentiality.....	38
2.8.10	Trusted Path .....	39
2.8.11	Cryptographic Key Establishment and Management.....	39
2.8.12	Use of Validated Cryptography .....	39
2.8.13	Collaborative Computing.....	40
2.8.14	Transmission of Security Parameters.....	40
2.8.15	Public Key Infrastructure Certificates.....	40



2.8.16	Mobile Code.....	41
2.8.17	Voice-Over Internet Protocol.....	41
2.8.18	System Connections.....	41
2.8.19	Security Roles.....	42
2.8.20	Message Authenticity.....	42
2.8.21	Architecture and Provisioning for Name/Address Resolution Service.....	42
2.8.22	Secure Name / Address Resolution Service (Authoritative Source).....	43
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver).....	43
2.9	Information and Document Management.....	45
2.9.1	Information and Document Management Policy and Procedures.....	45
2.9.2	Information and Document Retention.....	45
2.9.3	Information Handling.....	46
2.9.4	Information Classification.....	46
2.9.5	Information Exchange.....	46
2.9.6	Information and Document Classification.....	47
2.9.7	Information and Document Retrieval.....	47
2.9.8	Information and Document Destruction.....	48
2.9.9	Information and Document Management Review.....	48
2.9.10	Automated Marking.....	48
2.9.11	Automated Labeling.....	48
2.10	System Development and Maintenance.....	50
2.10.1	System Maintenance Policy and Procedures.....	50
2.10.2	Legacy System Upgrades.....	50
2.10.3	System Monitoring and Evaluation.....	50
2.10.4	Backup and Recovery.....	51
2.10.5	Unplanned System Maintenance.....	51
2.10.6	Periodic System Maintenance.....	52
2.10.7	Maintenance Tools.....	52
2.10.8	Maintenance Personnel.....	53
2.10.9	Remote Maintenance.....	53
2.10.10	Timely Maintenance.....	54
2.11	Security Awareness and Training.....	55
2.11.1	Security Awareness and Training Policy and Procedures.....	55
2.11.2	Security Awareness.....	55
2.11.3	Security Training.....	56
2.11.4	Security Training Records.....	56
2.11.5	Contact with Security Groups and Associations.....	56
2.11.6	Security Responsibility Testing.....	57
2.12	Incident Response.....	58
2.12.1	Incident Response Policy and Procedures.....	58
2.12.2	Continuity of Operations Plan.....	58
2.12.3	Continuity of Operations Roles and Responsibilities.....	59
2.12.4	Incident Response Training.....	59
2.12.5	Continuity of Operations Plan Testing.....	59
2.12.6	Continuity of Operations Plan Update.....	60
2.12.7	Incident Handling.....	60
2.12.8	Incident Monitoring.....	61
2.12.9	Incident Reporting.....	61
2.12.10	Incident Response Assistance.....	61
2.12.11	Incident Response Investigation and Analysis.....	62

2.12.12	Corrective Action.....	62
2.12.13	Alternate Storage Sites.....	62
2.12.14	Alternate Command/Control Methods.....	63
2.12.15	Alternate Control Center.....	63
2.12.16	Control System Backup.....	64
2.12.17	Control System Recovery and Reconstitution.....	64
2.12.18	Fail-Safe Response.....	65
2.13	Media Protection.....	66
2.13.1	Media Protection Policy and Procedures.....	66
2.13.2	Media Access.....	66
2.13.3	Media Classification.....	67
2.13.4	Media Labeling.....	67
2.13.5	Media Storage.....	68
2.13.6	Media Transport.....	68
2.13.7	Media Sanitization and Disposal.....	68
2.14	System and Information Integrity.....	70
2.14.1	System and Information Integrity Policy and Procedures.....	70
2.14.2	Flaw Remediation.....	70
2.14.3	Malicious Code Protection.....	71
2.14.4	System Monitoring Tools and Techniques.....	71
2.14.5	Security Alerts and Advisories.....	72
2.14.6	Security Functionality Verification.....	73
2.14.7	Software and Information Integrity.....	73
2.14.8	Spam Protection.....	74
2.14.9	Information Input Restrictions.....	74
2.14.10	Information Input Accuracy, Completeness, Validity, and Authenticity.....	74
2.14.11	Error Handling.....	75
2.14.12	Information Output Handling and Retention.....	75
2.15	Access Control.....	76
2.15.1	Access Control Policy and Procedures.....	76
2.15.2	Identification and Authentication Policy and Procedures.....	76
2.15.3	Account Management.....	77
2.15.4	Identifier Management.....	77
2.15.5	Authenticator Management.....	78
2.15.6	Supervision and Review.....	79
2.15.7	Access Enforcement.....	79
2.15.8	Separation of Duties.....	80
2.15.9	Least Privilege.....	80
2.15.10	User Identification and Authentication.....	80
2.15.11	Permitted Actions Without Identification or Authentication.....	81
2.15.12	Device Identification and Authentication.....	81
2.15.13	Authenticator Feedback.....	82
2.15.14	Cryptographic Module Authentication.....	82
2.15.15	Information Flow Enforcement.....	82
2.15.16	Passwords.....	83
2.15.17	System Use Notification.....	84
2.15.18	Concurrent Session Control.....	84
2.15.19	Previous Logon Notification.....	84
2.15.20	Unsuccessful Login Attempts.....	85
2.15.21	Session Lock.....	85

2.15.22	Remote Session Termination .....	85
2.15.23	Remote Access Policy and Procedures .....	86
2.15.24	Remote Access .....	86
2.15.25	Access Control for Portable and Mobile Devices .....	87
2.15.26	Wireless Access Restrictions .....	87
2.15.27	Personally Owned Information .....	88
2.15.28	External Access Protections .....	88
2.15.29	Use of External Information Control Systems .....	89
2.16	Audit and Accountability .....	90
2.16.1	Audit and Accountability Policy and Procedures .....	90
2.16.2	Auditable Events .....	90
2.16.3	Content of Audit Records .....	91
2.16.4	Audit Storage Capacity .....	92
2.16.5	Response to Audit Processing Failures .....	92
2.16.6	Audit Monitoring, Analysis, and Reporting .....	92
2.16.7	Audit Reduction and Report Generation .....	93
2.16.8	Time Stamps .....	93
2.16.9	Protection of Audit Information .....	93
2.16.10	Audit Record Retention .....	94
2.16.11	Conduct and Frequency of Audits .....	94
2.16.12	Auditor Qualification .....	94
2.16.13	Audit Tools .....	95
2.16.14	Security Policy Compliance .....	95
2.17	Monitoring and Reviewing Control System Security Policy .....	97
2.17.1	Monitoring and Reviewing Control System Security Management Policy and Procedures .....	97
2.17.2	Continuous Improvement .....	97
2.17.3	Monitoring of Security Policy .....	97
2.17.4	Best Practices .....	98
2.17.5	Security Accreditation .....	98
2.17.6	Security Certification .....	99
2.18	Risk Management and Assessment .....	100
2.18.1	Risk Assessment Policy and Procedures .....	100
2.18.2	Risk Management Plan .....	100
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures .....	101
2.18.4	Security Assessments .....	101
2.18.5	Control System Connections .....	102
2.18.6	Plan of Action and Milestones .....	102
2.18.7	Continuous Monitoring .....	102
2.18.8	Security Categorization .....	103
2.18.9	Risk Assessment .....	104
2.18.10	Risk Assessment Update .....	104
2.18.11	Vulnerability Assessment and Awareness .....	104
2.18.12	Identify, Classify, Prioritize, and Analyze Potential Security Risks .....	105

3.	CONCLUSIONS .....	107
4.	GLOSSARY: DEFINITIONS OF TERMS.....	108
5.	DOCUMENTS REFERENCED.....	120
	Appendix A.....	122

## ACRONYMS

AGA	American Gas Association
ARP	Address Resolution Protocol
CD	Compact Disc
CI/KR	Critical Infrastructures and Key Resources
CM	Cryptographic Module
CNSS	Committee on National Security Systems
CPU	Central Processing Unit
CSP	Collaborative Signal Processing
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FISMA	Federal Information Security Management Act
FLASH	Flash memory
FTP	File Transfer Protocol
HMI	Human-Machine Interface
HTTP	HyperText Transfer Protocol
ICCP	Inter-Control Center Communication Protocol
ICMP	Internet Control Message Protocol
ID	Identification
IDet	Intrusion Detection
IEEE	Institute of Electrical and Electronics Engineers
IEFT	Internet Engineering Task Force
IP	Internet Protocol

IPSec	IP Security
ISA	Instrumentation, Systems, and Automation Society
IT	Information Technology
Key	Cryptographic key
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OSI	Open System Interconnection
PC	Personal Computer
PDF	Portable Document Format
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PUB	Publication
RFC	Request for Comments
SCADA	Supervisory Control and Data Acquisition
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TSP	Telecommunications Service Priority
UHF	Ultra High Frequency
UPS	Uninterruptible Power Source
USB	Universal Serial Bus
VHF	Very High Frequency
VOIP	Voice-Over Internet Protocol
VPN	Virtual Private Network
WiFi	Wireless Fidelity

# Catalog of Control Systems Security: Recommendations for Standards Developers

## 1. INTRODUCTION

Protecting critical infrastructures and key resources (CI/KR) is essential to the security, public health and safety, economic vitality, and way of life for a nation's citizens. Fundamental to the protection of CI/KR 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 CI/KR 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. The objective of this document is to provide 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 there are differences in these systems, their similarities enable a common framework for discussing and defining security controls. Control system security standards are currently being developed by a variety of standards development groups to meet the needs of different industry sectors and regulatory environments. However, the standards developed for a specific sector may not always be consistent or comparable with similar standards developed in another sector. These developing standards often have differing emphases and levels of detail concerning specific security controls.

This document is intended to encompass these differences and provide a way to clarify security programs for control systems. Use of this document is not limited to a specific industry sector. It should be viewed as a catalog of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security 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 control system hardware and software is proprietary. However, some vendors are moving toward marketing products that utilize non-proprietary, off-the-shelf technologies. Control system networks may also use proprietary or industry-specific protocols. The proprietary nature of control systems also requires professionals with system-specific knowledge to operate them.

**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 CI/KR 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. This

presents a unique challenge for securing these systems because security cannot compromise the reliable operation of the control system.

The goal of a control system 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 upon NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, but modified to convey control system language. The following recommended controls are organized into Families primarily based upon NIST SP 800-53 but with 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 *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 pre-determined level of protection required for the control system used for the critical process. Not all of 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. The following recommendations were obtained from a review of the controls found in various industry standards. Similar controls were identified, and a single recommendation prepared that addressed the intent of the original controls. A cross reference of the standards used to develop the recommendations can be found in Appendix A.

### 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 to 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 the organizational staff and third-party contractors;
  - c. The roles, responsibilities, and management accountability structure 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 of the families 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.

## 2.2 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 utilized 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 includes 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.

### 2.2.2 Management Accountability

#### 2.2.2.1 *Requirement:*

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

### 2.2.3 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 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.

## **2.2.4 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:**

Expand relationships with local emergency response personnel to include information sharing and coordination of contingency plans as well as coordinated response to cyber security incidents.

**2.2.4.3 Requirement Enhancements:**

None.

## **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. Ensure security policies and procedures of second- and third-tier suppliers comply with corporate cyber security 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. Clearly define confidentiality or nondisclosure agreements and intellectual property rights. The organization also clearly defines change management procedures.

**2.2.5.3 Requirement Enhancements:**

None.

## **2.2.6 Termination of Third-Party Access**

### **2.2.6.1 Requirement:**

Establish procedures to remove external supplier access at the conclusion/termination of the contract.

### **2.2.6.2 Supplemental Guidance:**

Clearly define the timeliness for removal of external supplier access in the contract.

### **2.2.6.3 Requirement Enhancements:**

None.

## 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, and management accountability structure 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 procedure to review and document 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.

### 2.3.2 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.

**2.3.3 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:**

None.

**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/or data files relating to the control system that are in the employee's possession be 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, for example, keys, identification cards, building passes, computers, cell phones, and personal data assistants. Organization-owned documents include, for example, field device configuration and operational information, control system network documentation, etc.

**2.3.4.3 Requirement Enhancements:**

The organization implements automated processes to revoke access permissions that are initiated by the termination.

**2.3.5 Personnel Transfer**

**2.3.5.1 Requirement:**

The organization reviews logical 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:**

None.

**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 desire access to the control system. The organization reviews and updates access agreements periodically.

**2.3.6.2 Supplemental Guidance:**

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. 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.

**2.3.7 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, for example, 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.

**2.3.8 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.

**2.3.9 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.

## 2.4 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 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 from fire, water, and other possible environmental threats is important.

### 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 and management accountability structure 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. Include the physical and environmental protection policy as part of the general control system security policy for the organization. Develop 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.

### 2.4.2 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.

#### 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:**

None.

**2.4.3 Physical Access Control**

**2.4.3.1 Requirement:**

The organization limits physical access to all control system facilities and assets and verifies individual access authorizations before granting access. The organization limits access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

**2.4.3.2 Supplemental Guidance:**

The organization utilizes physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to control system facilities and assets. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys periodically and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated. The organization considers access requirements in emergency situations. During an emergency-related event, the organization should restrict access to control system facilities and assets to authorized individuals only.

This requirement applies to all control system facilities and assets. The organization considers control system safety and security interdependencies. Control systems often contain devices that either do not have, or cannot use, comprehensive access control capabilities. The organization uses physical access security mechanisms and defense-in-depth measures when necessary to supplement control system security when electronic mechanisms cannot fulfill the security requirements of the organization's security plan.

**2.4.3.3 Requirement Enhancements:**

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

**2.4.4 Monitoring Physical Access**

**2.4.4.1 Requirement:**

The organization monitors physical access to the control system facilities to detect and respond to physical security incidents.

**2.4.4.2 Supplemental Guidance:**

The organization considers the requirement for access to assets in emergency situations. The organization considers asset location technologies to track and monitor the movements of personnel and vehicles within hazardous areas.

**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 initiate appropriate response actions.

## 2.4.5 Visitor Control

### 2.4.5.1 *Requirement:*

The organization limits physical access to control systems by authenticating visitors before authorizing access to facilities or areas 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 required per security policies and procedures.

## 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 closeout and periodically review access logs based on an organization approved frequency.

### 2.4.6.3 *Requirement Enhancements:*

1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.
2. The organization maintains a record of all physical access, both visitor and authorized individuals, as long as dictated by any applicable laws or based on an organization-defined period and approved policy.

## 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.

## **2.4.8 Emergency Shutoff**

### **2.4.8.1 Requirement:**

For specific locations within a facility containing concentrations of control system resources (e.g., control centers, server rooms), the organization provides the capability of shutting off power to any component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without compromising personnel safety.

### **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 of 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.

## **2.4.9 Emergency Power**

### **2.4.9.1 Requirement:**

The organization provides a short-term Uninterruptible Power Supply (UPS) to facilitate an orderly shutdown of non-critical control system components in the event of a primary power source loss.

### **2.4.9.2 Supplemental Guidance:**

None.

### **2.4.9.3 Requirement Enhancements:**

1. The organization provides an alternate power source for the control system that is self-contained and does not rely on external power generation.
2. The organization provides a long-term UPS for critical control system assets.

## **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:**

None.

### **2.4.10.3 Requirement Enhancements:**

None.

## **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, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

**2.4.11.3 Requirement Enhancements:**

1. Electrical power to the control system, when interrupted, allows for controlled shutdown of the control system assets before the fire suppression system activates without jeopardizing personnel safety;
2. The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire;
3. The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders;
4. The organization employs an automatic fire suppression capability in facilities that are not staffed continuously.

**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:**

None

**2.4.12.3 Requirement Enhancements:**

None.

**2.4.13 Water Damage Protection**

**2.4.13.1 Requirement:**

The organization protects the control systems from water damage resulting from broken plumbing lines, fire control systems or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

**2.4.13.2 Supplemental Guidance:**

None.

**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 significant water leak within facilities containing control system.

**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.

**2.4.15 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 worksite. The organization implements appropriate management, operational, and technical security measures at alternate control centers.

**2.4.15.2 Supplemental Guidance:**

None.

**2.4.15.3 Requirement Enhancements:**

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

**2.4.16 Portable Media**

**2.4.16.1 Requirement:**

The organization monitors and prohibits the use of unapproved portable media use on the control system.

**2.4.16.2 Supplemental Guidance:**

The organization monitors and prevents personnel from entering secured control system facilities and areas with unapproved portable media. Portable media includes, but is not limited to, Universal Serial Bus (USB) drives, writeable compact disks (CDs) or digital versatile disks/digital video disks (DVDs), and floppy disks.

**2.4.16.3 Requirement Enhancements:**

1. The organization implements sensors to detect rogue access points and ad hoc wireless-enabled devices within control systems;
2. The organization ensures that devices cannot connect to external networks via physical or wireless connections.

**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.

**2.4.18 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, for example, 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.

**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.

**2.4.19 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.

**2.4.19.3 Requirement Enhancements:**

None.

**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:**

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

**2.4.20.3 Requirement Enhancements:**

None.

**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:**

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

**2.4.21.3 Requirement Enhancements:**

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 are used;
3. Tamper detection/ response envelopes with tamper response.

## 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/updates:

1. A formal, documented, system and services acquisition 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 and management accountability structure 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 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.

### 2.5.2 Allocation of Resources

#### 2.5.2.1 Requirement:

The organization implements a process to determine, document, approve, and allocate the resources required to adequately 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.

## 2.5.3 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.

## 2.5.4 Acquisitions

### 2.5.4.1 *Requirement:*

The organization includes security requirements and/or security specifications, either explicitly or by reference, in control system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

### 2.5.4.2 *Supplemental Guidance:*

Solicitation documents (e.g., requests for proposals) for control systems and services include, either explicitly or by reference, security requirements that describe:

1. The required security capabilities;
2. The required design and development processes;
3. The required test and evaluation procedures;
4. The required documentation.

The requirements in the solicitation documents permit updating security measures as new threats/vulnerabilities are identified and as new technologies are implemented. The Supervisory Control and Data Acquisition (SCADA) and control system procurement project, <http://www.msisac.org/scada/>, provides an example set of common control system procurement language.

### 2.5.4.3 *Requirement Enhancements:*

1. The organization requires that appropriate documentation be provided describing the functional properties of the security mechanisms employed within the control system with sufficient detail to enable the security mechanisms in the bid from the control system vendor to be analyzed and tested.
2. The organization requires that appropriate documentation be provided describing the design and implementation details of the security mechanisms employed within the control system with sufficient detail to enable the security mechanisms (including functional interfaces among control components) in the bid from the control system vendor to be analyzed and tested.

## 2.5.5 Control System Documentation

### 2.5.5.1 *Requirement:*

The organization ensures that adequate documentation for the control system and its constituent components are available, protected when required, and are accessible to authorized personnel.

**2.5.5.2 Supplemental Guidance:**

Administrator and user guides need to include information on:

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

**2.5.5.3 Requirement Enhancements:**

1. The organization develops documentation describing the functional properties of the security mechanisms employed within the control system with sufficient detail to enable analysis and testing of the security mechanisms.
2. The organization develops documentation describing the design and implementation specifications of the security mechanisms employed within the control system with sufficient detail to enable analysis and testing of the security mechanisms (including functional interfaces among control components).

## **2.5.6 Software License Usage Restrictions**

**2.5.6.1 Requirement:**

The organization's security program deploys policy and procedures to enforce compliance with software license usage restrictions.

**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.

## **2.5.7 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.

## 2.5.8 Security Engineering Principles

### 2.5.8.1 *Requirement:*

The organization designs and implements the control system using security engineering principles and best practices.

### 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.

## 2.5.9 Outsourced Control System Services

### 2.5.9.1 *Requirement:*

The organization ensures that third-party providers of control system services employ adequate security mechanisms in accordance with established service-level agreements and monitor compliance.

### 2.5.9.2 *Supplemental Guidance:*

Third-party providers are subject to the same control system security policies and procedures of the organization. All of 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.

## 2.5.10 Vendor Configuration Management

### 2.5.10.1 *Requirement:*

The control system vendor creates and implements a configuration management plan and procedures that limit changes to the control system during design and installation. This plan tracks

security flaws. The vendor obtains the organization's written approval for any changes to the plan. The vendor provides documentation of the plan and its implementation.

**2.5.10.2 Supplemental Guidance:**

None.

**2.5.10.3 Requirement Enhancements:**

None.

## **2.5.11 Vendor Security Testing**

**2.5.11.1 Requirement:**

The control system vendor develops a security test and evaluation plan. The vendor submits the plan to the organization for approval and implements the plan once written approval is obtained. The vendor then documents the results of the testing and evaluation and submits them to the organization for approval.

**2.5.11.2 Supplemental Guidance:**

The organization does not perform developmental security tests on the production control system network.

**2.5.11.3 Requirement Enhancements:**

None.

## **2.5.12 Vendor Life Cycle Practices**

**2.5.12.1 Requirement:**

The control system vendor adopts appropriate software development life-cycle practices to eliminate common coding errors that affect security, particularly with respect to input data validation and buffer management.

**2.5.12.2 Supplemental Guidance:**

Unsafe coding styles, with respect to string handling and buffer management, can result in applications which are vulnerable to crashing on deliberate malicious input due to a buffer overflow.

Appropriate software development life-cycle practices include:

1. The use of commercially available tools during development to check for unsafe conditions;
2. The use of a robust set of data validation and sanity checking tools;
3. Selecting a language that does not have unsafe buffer operations;
4. Not hard-coding database tables, but using configuration files instead;
5. Ensuring strict file system access.

**2.5.12.3 Requirement Enhancements:**

None.

## 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 non-production 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 and management accountability structure 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.

#### 2.6.1.3 *Requirement Enhancements:*

None.

### 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.

**2.6.2.3 Requirement Enhancements:**

1. The organization 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.

## **2.6.3 Configuration Change Control**

**2.6.3.1 Requirement:**

The organization authorizes, documents, and manages changes to the control 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. Due to 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, etc.) 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 off-line, or replicated to the extent feasible, before the testing can be conducted. If a control system must be taken off-line 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.

## **2.6.4 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. The organization should audit activities associated with configuration changes to the control system. The organization audits activities associated with configuration changes to the information system. The organization considers control system safety and security interdependencies.

### **2.6.4.3 Requirement Enhancements:**

None.

## **2.6.5 Access Restrictions for Configuration Change**

### **2.6.5.1 Requirement:**

The organization:

1. 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 have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals should 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, etc.).

### **2.6.5.3 Requirement Enhancements:**

The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

## **2.6.6 Configuration Settings**

### **2.6.6.1 Requirement:**

The organization:

1. Establishes mandatory configuration settings for IT 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.

**2.6.6.2 Supplemental Guidance:**

Configuration settings are the configurable parameters of the IT products that compose the control system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

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

**2.6.6.3 Requirement Enhancements:**

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

## **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 prohibit and/or restrict 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, instant messaging, file transfer protocol, hypertext transfer protocol, 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).

**2.6.7.3 Requirement Enhancements:**

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

## **2.6.8 Configuration Assets**

**2.6.8.1 Requirement:**

The organization creates and maintains a list of all end-user configurable assets and the configurations of those assets used by the organization.

**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). 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 as an integral part of component installations.
2. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of control system components.

**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 their 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 needs to be tracked, documented, and verified as sanitized. The organization periodically verifies the media sanitization process.

**2.6.9.3 Requirement Enhancements:**

None.

**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. Do not embed passwords into tools, source code, scripts, aliases or shortcuts.

**2.6.10.3 Requirement Enhancements:**

None.

## 2.7 Strategic Planning

The purpose of strategic planning is to maintain optimal operations and to prevent or recover 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, 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.

### 2.7.2 Control System Security Plan

#### 2.7.2.1 *Requirement:*

The organization develops and implements a security plan for the control system that provides an overview of the security requirements for the system and a description of the security measures in place or planned for meeting those requirements. Designated officials within the organization review and approve the control system security plan.

#### 2.7.2.2 *Supplemental Guidance:*

The security plan is aligned with the organization's control system architecture and information security architecture. To properly develop the control system security plan, it is essential for a cross-functional cyber security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the control system. The cyber security team considers control system safety and security interdependencies. The cyber security 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 cyber security team consults with the control system vendor(s) as well.

**2.7.2.3 Requirement Enhancements:**

None.

## **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 to automatically identify attacks during their early stages are determined. 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 post interruption 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.

## **2.7.4 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.

**2.7.4.3 Requirement Enhancements:**

None.

## 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:*

Training needs are to be provided to individuals in the control system community so that all understand the content, purpose, and implementation of the security plans. The organization's planning process must account for training in the implementation of the organization's security plan. Different levels of training might be prepared for personnel with different levels of responsibility. Cross-training might also be considered. Additional training controls are addressed in individual families.

### 2.7.5.3 *Requirement Enhancements:*

None.

## 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.

## 2.7.7 Investigate and Analyze

### 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.

## **2.7.8 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 cyber security 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.

## **2.7.9 Risk Mitigation**

### **2.7.9.1 Requirement:**

Risk-reduction mitigation measures are planned and implemented and the results 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 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.

## **2.7.10 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.

## **2.7.11 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 regards to control system usage. The organization obtains signed acknowledgement 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:**

None.

## **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 advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

**2.7.12.3 Requirement Enhancements:**

None.



## 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 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.

### 2.8.2 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:*

None.

## 2.8.3 Security Function Isolation

### 2.8.3.1 *Requirement:*

The control system isolates security functions from non-security functions.

### 2.8.3.2 *Supplemental Guidance:*

The control system isolates security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those 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 critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions;
2. The control system minimizes the number of non – security 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.

## 2.8.4 Information Remnants

### 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 information 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 information system.

### 2.8.4.3 *Requirement Enhancements:*

None.

## 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 exist 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.

## **2.8.6 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.

### **2.8.6.3 Requirement Enhancements:**

None.

## **2.8.7 Boundary Protection**

### **2.8.7.1 Requirement:**

The organization defines the external boundary(ies) 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:**

Any connection to the Internet or other external network or control system needs to occur through managed interfaces (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). Control system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site.

### **2.8.7.3 Requirement Enhancements:**

1. The organization physically allocates publicly accessible control system components to separate sub networks with separate, physical network interfaces. Publicly accessible control system components include, for example, 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 of the control system boundary or any unauthorized communication through the control system boundary when there is an operational failure of the boundary protection mechanisms.

## **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.

## **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 due to 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:**

None.

## **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).

It is recommended that login-to-operator interface 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 trusted computing base to correctly enforce 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.

## **2.8.11 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 the key generation process is in accordance with a specified algorithm and key sizes are based on an assigned standard. Key generation needs to 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:**

None.

## **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 Federal Information Processing Standard (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/cryptval>.

**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.

## **2.8.13 Collaborative Computing**

**2.8.13.1 Requirement:**

The use of collaborative computing mechanisms on control system is strongly discouraged and provides an explicit indication of use to the local users.

**2.8.13.2 Supplemental Guidance:**

Collaborative computing mechanisms include, for example, video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

**2.8.13.3 Requirement Enhancements:**

If collaborative computing mechanisms are utilized on the control system, they are disconnected and powered down when not in use.

## **2.8.14 Transmission of Security Parameters**

**2.8.14.1 Requirement:**

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

**2.8.14.2 Supplemental Guidance:**

Security parameters may be explicitly or implicitly associated with the information contained within the control system.

**2.8.14.3 Requirement Enhancements:**

None.

## **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.

**2.8.16 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 should authorize the use of mobile code.

**2.8.16.2 Supplemental Guidance:**

Mobile code technologies include, for example, Java, JavaScript, ActiveX, 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>.

**2.8.16.3 Requirement Enhancements:**

None.

**2.8.17 Voice-Over Internet Protocol**

**2.8.17.1 Requirement:**

The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and limits the use of VOIP within the control system.

**2.8.17.2 Supplemental Guidance:**

Generally, VOIP technologies should not be employed on control systems.

**2.8.17.3 Requirement Enhancements:**

None.

**2.8.18 System Connections**

**2.8.18.1 Requirement:**

All external control system and communication connections are identified and adequately 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 information 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.

**2.8.19 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.

**2.8.20 Message Authenticity**

**2.8.20.1 Requirement:**

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

**2.8.20.2 Supplemental Guidance:**

Message authentication provides protection from malformed traffic from misconfigured devices and malicious entities.

**2.8.20.3 Requirement Enhancements:**

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

**2.8.21 Architecture and Provisioning for Name/Address Resolution Service**

**2.8.21.1 Requirement:**

The control system's 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, it is recommended to 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. Additionally, 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.

## **2.8.22 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. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

### **2.8.22.3 Requirement Enhancements:**

None.

## **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. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

### **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 or not local DNS clients (i.e., stub resolvers) explicitly request this function.

## 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, 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 needs to be protected. Security measures, philosophy, and implementation strategies are other examples. Additionally, 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/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.

### 2.9.2 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.

#### 2.9.2.3 *Requirement Enhancements:*

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

### **2.9.3 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 being 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.

### **2.9.4 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:**

It is recommended that a minimum of three levels of classification 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.

### **2.9.5 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 through the use of 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.

## **2.9.6 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, etc.);
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 cyber security 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, etc.) 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, etc.) 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.

## **2.9.7 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, etc.). 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.

## **2.9.8 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.

## **2.9.9 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.

## **2.9.10 Automated Marking**

### **2.9.10.1 Requirement:**

The control system automatically marks data output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

### **2.9.10.2 Supplemental Guidance:**

Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the control system). The markings used in external marking are distinguished from the labels used on internal data structures described in 2.9.11.

### **2.9.10.3 Requirement Enhancements:**

None.

## **2.9.11 Automated Labeling**

### **2.9.11.1 Requirement:**

The control system automatically labels information in storage, in process, and in transmission.

**2.9.11.2 Supplemental Guidance:**

Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the control system. Information labeling is accomplished in accordance with:

1. Access control requirements;
2. Special dissemination, handling, or distribution instructions;
3. Requirements to enforce control system security policy.

**2.9.11.3 Requirement Enhancements:**

None.

## 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/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.

### 2.10.2 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 there was a concern about system security, 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.

### 2.10.3 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.

## **2.10.4 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.

## **2.10.5 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.

## **2.10.6 Periodic System Maintenance**

### **2.10.6.1 Requirement:**

The organization schedules, performs, and documents routine preventive and regular maintenance on the components of the control system in accordance with manufacturer or vendor specifications and/or organizational policies and procedures.

### **2.10.6.2 Supplemental Guidance:**

Maintenance procedures that require the physical removal of any control system component needs 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 official(s). 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 keeps a maintenance record for the control system that includes the date and time of maintenance, the name of the individual(s) performing the maintenance, the name of the escort, if necessary, a description of the maintenance performed, and a list of equipment removed or replaced (including identification numbers, if applicable).
2. The organization employs automated mechanisms to schedule and conduct maintenance as required and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.

## **2.10.7 Maintenance Tools**

### **2.10.7.1 Requirement:**

The organization approves, manages, protects, and monitors the use of control system maintenance tools and maintains the integrity of tools on an ongoing basis.

### **2.10.7.2 Supplemental Guidance:**

The intent of this requirement is to address hardware and software brought into the control system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer introduced for a particular maintenance activity). Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the control system. Hardware and/or software components that may support control 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 requirement.

### **2.10.7.3 Requirement Enhancements:**

1. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications;
3. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the control system;

4. The organization checks all maintenance equipment that can retain information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed unless an appropriate organization official explicitly authorizes an exception;
5. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only;
6. Maintenance tools are used with care on control system networks to ensure that control system operations will not be degraded by their use.

## **2.10.8 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.

## **2.10.9 Remote Maintenance**

### **2.10.9.1 Requirement:**

The organization authorizes, manages, and monitors remotely executed maintenance and diagnostic activities on the control system. When remote maintenance is completed, the organization (or control system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the password following each remote maintenance service.

### **2.10.9.2 Supplemental Guidance:**

Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools needs to be consistent with organizational policy and documented in the security plan for the control system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or security mechanisms to consider for improving the security of remote maintenance include:

1. Encryption and decryption of communications;
2. Strong identification and authentication techniques;
3. Remote disconnect verification.

### **2.10.9.3 Requirement Enhancements:**

1. The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions;
2. The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the control system;
3. The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own control system a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the control system and sanitized (for organizational information) before the service begins and also sanitized (for potentially malicious software) after the service is performed and before being reconnected to the control system.

## **2.10.10 Timely Maintenance**

### **2.10.10.1 Requirement:**

The organization acquires maintenance support and spare parts for key control system components within a specified time period of failure.

### **2.10.10.2 Supplemental Guidance:**

System reliability considerations dictate that replacement parts be readily available (from vendor inventory, operator stock, or other) to avoid or minimize system downtime. To obtain spare parts for key components in a timely manner, it is prudent to have a supply of key components on hand.

### **2.10.10.3 Requirement Enhancements:**

None.

## 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 demonstrate management's commitment to cyber and control system security programs. Feedback from staff can be valuable for refining the security program.

Following are the controls for awareness and training that need to be supported and implemented by the organization to protect the control system.

### 2.11.1 Security Awareness and Training Policy and Procedures

#### 2.11.1.1 *Requirement:*

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

1. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

#### 2.11.1.2 *Supplemental Guidance:*

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

#### 2.11.1.3 *Requirement Enhancements:*

None.

### 2.11.2 Security Awareness

#### 2.11.2.1 *Requirement:*

The organization provides basic security awareness training to all control system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter. The effectiveness of security awareness training, at the organization level, needs to be reviewed at a minimum once a year.

#### 2.11.2.2 *Supplemental Guidance:*

The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the control system(s) to which personnel have authorized access. The security awareness training program includes initial and periodic review of policies, standard operating procedures, security trends, and vulnerabilities. The control system security awareness program is consistent with the requirements of the security awareness policy

established by the organization. The effectiveness of the security awareness training can be measured by the number of security related items logged in the organizations corrective action program.

**2.11.2.3 Requirement Enhancements:**

All control system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training.

**2.11.3 Security Training**

**2.11.3.1 Requirement:**

The organization identifies and trains personnel with significant control system security roles and responsibilities. The organization documents those roles and responsibilities and provides appropriate control system security training before authorizing access to the system, when required by system changes, and with periodic training thereafter.

**2.11.3.2 Supplemental Guidance:**

The organization determines the appropriate content of security training based on the specific requirements of the organization and the control system to which personnel have authorized access. In addition, the organization ensures that the system managers, system and network administrators, and other third-party personnel having access to system-level software have adequate technical training to perform their assigned duties. The organization's security training program needs to be consistent with the requirements contained in the organization's security training policy. Users should be notified when their training is scheduled and informed as to how it will be conducted. The security training includes initial and periodic review of policies, standard operating procedures, security trends, and vulnerabilities. The control system security training program is consistent with the requirements of the security training policy established by the organization.

**2.11.3.3 Requirement Enhancements:**

None.

**2.11.4 Security Training Records**

**2.11.4.1 Requirement:**

The organization documents, maintains, and monitors individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization's records retention policy.

**2.11.4.2 Supplemental Guidance:**

The organization maintains a record of training requirements for each user in accordance with the provisions of the organization training and records retention policy.

**2.11.4.3 Requirement Enhancements:**

None.

**2.11.5 Contact with Security Groups and Associations**

**2.11.5.1 Requirement:**

The organization establishes, participates with, and maintains contacts with special interest groups, industry vendor forums, specialized public or governmental forums, or professional associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

**2.11.5.2 Supplemental Guidance:**

It is in the best interest of the organization to establish contacts with industry and professional forums to stay abreast of new technologies, techniques, security issues, and mitigation solutions. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to control systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

**2.11.5.3 Requirement Enhancements:**

None.

## **2.11.6 Security Responsibility Testing**

**2.11.6.1 Requirement:**

The organization documents and tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system.

**2.11.6.2 Supplemental Guidance:**

The organization maintains a list of security responsibilities for each user. These need to be used to test each user in accordance with the provisions of the organization training policy. Users need to be notified when their testing is scheduled, informed as to how it will be conducted, and notified as to their results. The security responsibility testing needs to be conducted at least annually and/or as warranted by technology/procedural changes.

**2.11.6.3 Requirement Enhancements:**

None.

## 2.12 Incident Response

Incident response addresses the capability to continue or resume operations of a control system in the event of disruption of normal system operation. Incident response entails the preparation, testing, and maintenance of specific policies and procedures to enable the organization to recover the control system's operational status after the occurrence of a disruption. Disruptions can come from natural disasters such as earthquakes, tornados, floods, or from man made events such as riots, terrorism, or vandalism. The ability for the control system to function after such an event is directly dependent on implementing policies, procedures, training and resources in place ahead of time using the organizations planning process. The security controls that are recommended under the incident response family provide policies and procedures for incident response monitoring, handling, reporting, testing, training, recovery, and reconstitution of the control systems for an organization.

### 2.12.1 Incident Response Policy and Procedures

#### 2.12.1.1 *Requirement:*

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

1. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

#### 2.12.1.2 *Supplemental Guidance:*

The organization ensures the incident response policy and procedures are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

#### 2.12.1.3 *Requirement Enhancements:*

None.

### 2.12.2 Continuity of Operations Plan

#### 2.12.2.1 *Requirement:*

The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or re-establishing production in case of an undesirable interruption for a control system. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring system operations after a disruption or failure. Designated officials within the organization review and approve the continuity of operations plan.

#### 2.12.2.2 *Supplemental Guidance:*

A continuity of operations plan addresses both business continuity planning and recovery of control system operations. Development of a continuity of operations plan is a process to identify procedures for safe control system operation while recovering from a significant system disruption. The plan requires documentation of critical control system functions that need to be recovered.

#### 2.12.2.3 *Requirement Enhancements:*

The continuity of operations plan delineates that at the time of the disruption to normal control system operations, the organization executes its incident response policies and procedures to place the control system in a safe configuration and initiates the necessary notifications to regulatory



authorities. The organization initiates a root cause analysis for the event and submits any findings from the analysis to the organizations corrective action program. The organization then resumes normal operation of the control system in accordance with its policies and procedures.

### **2.12.3 Continuity of Operations Roles and Responsibilities**

#### **2.12.3.1 Requirement:**

The organization's continuity of operations plan defines and communicates the specific roles and responsibilities for each part of the plan in relation to various types of control system incidents.

#### **2.12.3.2 Supplemental Guidance:**

The continuity of operations plan defines the roles and responsibilities of the various employees and contractors in the event of a significant incident. The plans identify responsible personnel to lead the recovery and response effort if an incident occurs.

#### **2.12.3.3 Requirement Enhancements:**

None.

### **2.12.4 Incident Response Training**

#### **2.12.4.1 Requirement:**

The organization trains personnel in their continuity of operations plan roles and responsibilities with respect to the control system. The organization provides refresher training at least annually. The training covers employees, contractors, and stakeholders in the implementation of the continuity of operations plan.

#### **2.12.4.2 Supplemental Guidance:**

Training needs to be provided to individuals in the control system community so that all the users of the control system understand the content, purpose, and implementation of the plans. The organization provides continuity of operations training and refresher sessions annually.

#### **2.12.4.3 Requirement Enhancements:**

1. The organization incorporates control system simulated events into continuity of operations training to facilitate effective response by personnel in crisis situations;
2. The organization employs automated mechanisms to provide a thorough and realistic control system training environment.

### **2.12.5 Continuity of Operations Plan Testing**

#### **2.12.5.1 Requirement:**

The organization tests the continuity of operations plan to determine its effectiveness and documents the results. Appropriate officials within the organization review the documented test results and initiate corrective actions if necessary. The organization tests the continuity of operations plan for the control system at least annually, using organization prescribed tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.

#### **2.12.5.2 Supplemental Guidance:**

The organization maintains a list of incident response activities and mitigations for each user in accordance with the provisions of the organization incident response policy and procedures. Users need to be notified when their testing is scheduled and informed as to how it will be conducted. There are several methods for testing and/or exercising continuity of operations plans to identify potential weaknesses (e.g., full-scale business continuity plan testing, functional/tabletop exercises, etc.). Following the preparation of the various plans, a schedule needs to be developed to review and test each plan and ensure that each still meets the objectives.

**2.12.5.3 Requirement Enhancements:**

The organization coordinates continuity of operations plan testing and/or exercises with organizational elements responsible for related plans.

1. The organization tests/exercises the continuity of operations plan at the alternate processing site to familiarize control system operations personnel with the facility and available resources and to evaluate the site's capabilities to support continuity of operations.
2. The organization employs automated mechanisms to thoroughly and effectively test/exercise the continuity of operations plan by providing complete coverage of operational issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the control system and supported missions.

## **2.12.6 Continuity of Operations Plan Update**

**2.12.6.1 Requirement:**

The organization reviews the continuity of operations plan for the control system at least annually and updates the plan to address system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing.

**2.12.6.2 Supplemental Guidance:**

Organizational changes include changes in mission, functions, or business processes supported by the control system. The organization communicates the changes to appropriate organizational elements responsible for related plans.

**2.12.6.3 Requirement Enhancements:**

None.

## **2.12.7 Incident Handling**

**2.12.7.1 Requirement:**

The organization implements control system incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

**2.12.7.2 Supplemental Guidance:**

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Incidents need to be analyzed in light of trends and recorded so they can be used for subsequent trend analyses.

**2.12.7.3 Requirement Enhancements:**

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

## **2.12.8 Incident Monitoring**

### **2.12.8.1 Requirement:**

The organization tracks and documents control system network security incidents on an ongoing basis.

### **2.12.8.2 Supplemental Guidance:**

None.

### **2.12.8.3 Requirement Enhancements:**

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

## **2.12.9 Incident Reporting**

### **2.12.9.1 Requirement:**

The organization promptly reports cyber and control system security incident information to the appropriate authorities.

### **2.12.9.2 Supplemental Guidance:**

The organization develops guidance to determine what is a reportable incident and the granularity of the information reported (e.g., aggregation of common malicious activity) and who to report to (e.g., management, IT security, process safety, control systems engineering, law enforcement agencies). Reporting documents include the details of the incident, the lessons learned, and the course of action to prevent it from occurring again. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. In addition to incident information, weaknesses and vulnerabilities in the control system need to be reported to appropriate organizational officials in a timely manner to prevent security incidents. Each organization establishes reporting criteria, to include sharing information through appropriate channels. The United States Computer Emergency Readiness Team maintains the Industrial Control System Security Center at [http://www.uscert.gov/control\\_systems](http://www.uscert.gov/control_systems).

### **2.12.9.3 Requirement Enhancements:**

The organization employs automated mechanisms to assist in the reporting of security incidents.

## **2.12.10 Incident Response Assistance**

### **2.12.10.1 Requirement:**

The organization provides an incident response support resource that offers advice and assistance to users of the control system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

### **2.12.10.2 Supplemental Guidance:**

Possible implementations of incident response support resources in an organization include a help desk and/or an assistance group and access to forensics services when required. The incident

response procedures allow for an effective response to any attack on the control system up to and including assigning qualified personnel to manually manipulate control system functions if necessary.

**2.12.10.3 Requirement Enhancements:**

The organization employs automated mechanisms to increase the availability of incident response-related information and support.

**2.12.11 Incident Response Investigation and Analysis**

**2.12.11.1 Requirement:**

The organization documents its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that the control system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps. The organization ensures that a dedicated group of personnel is assigned to periodically review the data at a minimum monthly.

**2.12.11.2 Supplemental Guidance:**

The organization develops an incident response investigation and analysis program, either internally or externally, to investigate incidents. These investigations consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber incident may include intentional and unintentional incidents.

**2.12.11.3 Requirement Enhancements:**

1. The organization develops, tests, deploys, and fully documents an incident response investigation and analysis process;
2. The program specifies roles and responsibilities with respect to local law enforcement and/or other critical stakeholders in an internal and shared incident response investigation and analysis program.

**2.12.12 Corrective Action**

**2.12.12.1 Requirement:**

The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of a cyber security incident are fully implemented.

**2.12.12.2 Supplemental Guidance:**

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

**2.12.12.3 Requirement Enhancements:**

None.

**2.12.13 Alternate Storage Sites**

**2.12.13.1 Requirement:**

The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of control system configuration information.

### **2.12.13.2 Supplemental Guidance:**

The frequency of control system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

### **2.12.13.3 Requirement Enhancements:**

The organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

1. The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards;
2. The organization configures the alternate storage site to facilitate timely and effective recovery operations;
3. The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

## **2.12.14 Alternate Command/Control Methods**

### **2.12.14.1 Requirement:**

The organization identifies alternate command/control methods for the control system and initiates necessary agreements to permit the resumption of operations for the safe operation of the control system within an organization-defined time period when the primary system capabilities are unavailable.

### **2.12.14.2 Supplemental Guidance:**

Alternate command/control methods required to resume operations within the organization-defined time period are either available at alternate organization sites or contracts with vendors need to be in place to support alternate command/control methods for the control system. Time frames to resume system operations need to be consistent with organization-established recovery time objectives.

### **2.12.14.3 Requirement Enhancements:**

1. Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements;
2. Alternate telecommunications services do not share a single point of failure with primary telecommunications services;
3. Alternate telecommunications service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards;
4. Primary and alternate telecommunications service providers need to have adequate contingency plans.

## **2.12.15 Alternate Control Center**

### **2.12.15.1 Requirement:**

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

### **2.12.15.2 Supplemental Guidance:**

Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site.

**2.12.15.3 Requirement Enhancements:**

1. The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards;
2. The organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;
3. The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements;
4. The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability.

**2.12.16 Control System Backup**

**2.12.16.1 Requirement:**

The organization conducts backups of critical control system information, including state of the user-level and system level information, process formulas, system inventories, etc., contained in the control system, on a regular schedule as defined by the organization, and stores the information at an appropriately secured location.

**2.12.16.2 Supplemental Guidance:**

The frequency of control system backups and the transfer rate of backup information to alternate storage sites (if so designated) needs to be consistent with the organization's recovery time objectives and recovery point objectives.

**2.12.16.3 Requirement Enhancements:**

1. The organization tests backup information periodically to verify media reliability and information integrity;
2. The organization selectively uses backup information in the restoration of control system functions as part of contingency plan testing;
3. The organization stores backup copies of the operating system and other critical control system software in a separate facility or in a fire-rated container that is not collocated with the operational software;
4. The organization protects system backup information from unauthorized modification;
5. The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hash) to protect the integrity of control system backups.

**2.12.17 Control System Recovery and Reconstitution**

**2.12.17.1 Requirement:**

The organization employs mechanisms with supporting procedures to allow the control system to be recovered and reconstituted to the system's original state after a disruption or failure.

**2.12.17.2 Supplemental Guidance:**

Control system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values; security-critical patches are reinstalled; security-related configuration settings are reestablished; system documentation and operating procedures are available; application and system software is reinstalled and configured with secure settings; information from the most recent, known secure backups is loaded; and the system is fully tested.

**2.12.17.3 Requirement Enhancements:**

The organization includes a full recovery and reconstitution of the control system as part of contingency plan testing.

**2.12.18 Fail-Safe Response**

**2.12.18.1 Requirement:**

The control system has the ability to execute an appropriate fail safe procedure upon the loss of communications with the control system or the loss of the control system itself.

**2.12.18.2 Supplemental Guidance:**

In the event of a loss of communication between the control system and the operational facilities, the onsite instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric industry, this may be to alert the operator of the failure and then do nothing (e.g., let the electric grid continue to operate). For the chemical or manufacturing industry, the fail-safe process may be to alert the operator but then safely shutdown the process. For the natural gas industry, this may be to maintain the last operational setting before communication failure. The organization defines what "loss of communications" means (i.e., 5 seconds or 5 minutes without communications, etc.). The organization then defines the appropriate fail safe process for its industry.

**2.12.18.3 Requirement Enhancements:**

None.

## 2.13 Media Protection

The security controls under the media protection family provide policy and procedures for limiting access to media to authorized users. Security measures also exist for labeling media for distribution and handling requirements, as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media.

Media assets include CDs; DVDs; erasable, programmable read-only memory; tapes; printed reports; and documents. Physical security controls need to address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and destroying these assets. Security requirements could include safe storage from fire, theft, unintentional distribution, or environmental damage. If an attacker gains access to unencrypted system backup media associated with a control system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an attacker to run password-cracking tools and extract usable passwords. In addition, the backups typically contain machine names, Internet Protocol addresses, software version numbers, usernames, and other data useful in planning an attack. The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of, or connected to, the control system should not be permitted to prevent the introduction of malware or the inadvertent loss or theft of data.

### 2.13.1 Media Protection Policy and Procedures

#### 2.13.1.1 *Requirement:*

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

1. A formal, documented, media protection 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 media protection policy and associated media protection controls.

#### 2.13.1.2 *Supplemental Guidance:*

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

#### 2.13.1.3 *Requirement Enhancements:*

None.

### 2.13.2 Media Access

#### 2.13.2.1 *Requirement:*

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

#### 2.13.2.2 *Supplemental Guidance:*

The organization implements stringent access and authentication techniques for portable storage media to ensure the validity of connection. The security measures allow organizations to protect data files against unauthorized internal or semi-internal access.



Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). This requirement also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

**2.13.2.3 Requirement Enhancements:**

Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted. This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

### **2.13.3 Media Classification**

**2.13.3.1 Requirement:**

The organization reviews and classifies all removable information storage media and the control system output to determine distribution limitations (public, confidential, or classified).

**2.13.3.2 Supplemental Guidance:**

The organization reviews and classifies all removable information storage media using written and approved classification guides. The classification applied to the information storage indicates the level of sensitivity of the information contained on the media.

**2.13.3.3 Requirement Enhancements:**

None.

### **2.13.4 Media Labeling**

**2.13.4.1 Requirement:**

The organization affixes external labels to removable information system media and to the control system output that indicate the distribution limitations (public, confidential, or classified) and handling caveats of the information. The organization may exempt specific types of media or hardware components from labeling as long as they remain within a secure environment (as defined by the organization).

**2.13.4.2 Supplemental Guidance:**

The organization marks human-readable output appropriately in accordance with applicable policies and procedures. The organization affixes labels to digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.

**2.13.4.3 Requirement Enhancements:**

None.

## 2.13.5 Media Storage

### 2.13.5.1 Requirement:

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

### 2.13.5.2 Supplemental Guidance:

The information is stored in the most physically and environmentally secure repository commensurate with the security category of the information recorded on the media. The organization protects control system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. The organization protects unmarked media at the highest level for the control system until the media are reviewed and appropriately labeled.

### 2.13.5.3 Requirement Enhancements:

None.

## 2.13.6 Media Transport

### 2.13.6.1 Requirement:

The organization develops security measures for paper and digital media extracted from the control system and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

### 2.13.6.2 Supplemental Guidance:

Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

### 2.13.6.3 Requirement Enhancements:

1. The organization protects digital and non-digital media during transport outside of controlled area. Physical and technical security measures for the protection of digital and non-digital media are approved by the organization and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.
2. The organization documents, where appropriate, activities associated with the transport of information system media. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.
3. The organization employs an identified custodian at all times to transport information system media. Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

## 2.13.7 Media Sanitization and Disposal

### 2.13.7.1 Requirement:

The organization sanitizes control system digital and non-digital media, before disposal or release for reuse.

**2.13.7.2 Supplemental Guidance:**

Sanitization is the process used to remove information from control system media so there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques including clearing, purging, and destroying media information ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or to have no adverse impact on the organization if released for reuse or disposal.

**2.13.7.3 Requirement Enhancements:**

1. The organization tracks, documents, and verifies media sanitization and disposal actions;
2. The organization periodically tests sanitization equipment and procedures to verify correct performance.

## 2.14 System and Information Integrity

Maintaining a control system, including information integrity, increases assurance that sensitive data have neither been modified nor deleted in an unauthorized or undetected manner. The security controls described under the system and information integrity family provide policy and procedure for identifying, reporting, and correcting control system flaws. Controls exist for malicious code detection, spam protection, and intrusion detection tools and techniques. Also provided are controls for receiving security alerts and advisories and the verification of security functions on the control system. In addition, there are controls within this family to detect and protect against unauthorized changes to software and data, restrict data input and output, check the accuracy, completeness, and validity of data, and handle error conditions.

### 2.14.1 System and Information Integrity Policy and Procedures

#### 2.14.1.1 *Requirement:*

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

1. Formal, documented, system and control integrity 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 system and information integrity policy and associated system and information integrity controls.

#### 2.14.1.2 *Supplemental Guidance:*

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

#### 2.14.1.3 *Requirement Enhancements:*

None.

### 2.14.2 Flaw Remediation

#### 2.14.2.1 *Requirement:*

The organization identifies, reports, and remediates control system flaws (per organizational, legal, and/or regulatory policies).

#### 2.14.2.2 *Supplemental Guidance:*

The organization identifies control systems containing software affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Proprietary software can be found in either commercial/government off-the-shelf component products or in custom-developed applications. The organization (or the software developer/vendor for software developed and maintained by a vendor/contractor) promptly evaluates newly released security-relevant patches, service packs, and hot fixes and tests them for effectiveness and potential impacts on the organization's control system before installation. Flaws discovered during security assessments, continual monitoring, or under incident response activities also need to be addressed expeditiously. It is generally not recommended to shut down and restart control system components when an anomaly is identified.

#### 2.14.2.3 *Requirement Enhancements:*

1. The organization centrally manages the flaw remediation process and installs updates automatically. Organizations consider the risk of employing automated flaw remediation processes on a control system;
2. The use of automated flaw remediation processes must not degrade the operational performance of the control system;
3. The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

### **2.14.3 Malicious Code Protection**

#### **2.14.3.1 Requirement:**

The control system employs malicious code protection.

#### **2.14.3.2 Supplemental Guidance:**

The organization employs malicious code protection mechanisms at critical control system entry and exit points (e.g., firewalls, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware). The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the control system.

Updates are scheduled to occur during planned control system outages. The organization considers control system vendor recommendations for malicious code protection. To reduce malicious code, organizations remove the functions and services that should not be employed on the control system (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, electronic mail, file sharing).

#### **2.14.3.3 Requirement Enhancements:**

1. The organization centrally manages malicious code protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage malicious code protection on a control system;
2. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the control system;
3. The control system automatically updates malicious code protection mechanisms.

### **2.14.4 System Monitoring Tools and Techniques**

#### **2.14.4.1 Requirement:**

The organization employs tools and techniques to monitor security events and system activities on the control system, detect attacks, and provide identification of unauthorized use of the system.

#### **2.14.4.2 Supplemental Guidance:**

Control system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection

software, log monitoring software, network monitoring software, and network forensic analysis tools). Monitoring devices can be strategically deployed within the control system (e.g., at selected perimeter locations and/or near server farms supporting critical applications) to collect essential information. Monitoring devices can also be deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices can be used to track the impact of security changes to the control system. The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the control system to support such activities. Organizations need to consult with appropriate legal counsel with regard to all system monitoring activities. The level of system monitoring activity is heightened by organizations whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

#### **2.14.4.3 Requirement Enhancements:**

1. The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols;
2. The organization employs automated tools to support near real-time analysis of events;
3. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination;
4. The control system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external control system;
5. The control system provides a real-time alert when indications of compromise or potential compromise occur;
6. The use of monitoring tools and techniques must not adversely impact the operational performance of the control system.

### **2.14.5 Security Alerts and Advisories**

#### **2.14.5.1 Requirement:**

The organization:

1. Receives control system security alerts/advisories regularly and in response to system-based occurrences;
2. Issues alerts/advisories to appropriate personnel;
3. Takes appropriate actions in response.

#### **2.14.5.2 Supplemental Guidance:**

The organization documents the types of actions to be taken in response to security alerts and advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that:

1. Facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies);
2. Provide access to advice from security professionals;
3. Improve knowledge of security best practices.

#### **2.14.5.3 Requirement Enhancements:**

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

## **2.14.6 Security Functionality Verification**

### **2.14.6.1 Requirement:**

The organization verifies the correct operation of security functions within the control system upon system startup and restart; upon command by user with appropriate privilege; periodically; and/or at defined time periods. The control system notifies the system administrator when anomalies are discovered.

### **2.14.6.2 Supplemental Guidance:**

The need to verify security functionality applies to all security functions. For security functions that are not able to execute automated self-tests, the organization either implements compensating security measures or explicitly accepts the risk of not performing the verification as required. Generally, it is not recommended to shut down and restart control system resources upon the identification of an anomaly.

### **2.14.6.3 Requirement Enhancements:**

1. The organization employs automated mechanisms to provide notification of failed automated security tests;
2. The organization employs automated mechanisms to support management of distributed security testing.

## **2.14.7 Software and Information Integrity**

### **2.14.7.1 Requirement:**

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

### **2.14.7.2 Supplemental Guidance:**

The organization employs integrity verification techniques on the control system to look for evidence of information tampering, errors, and/or omissions. The organization employs good software engineering practices with regard to commercial-off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the IT systems, control systems, and the applications it hosts.

### **2.14.7.3 Requirement Enhancements:**

Although automated tools can be risky for use in control systems, the following can be considered as appropriate:

1. The organization reassesses the integrity of software and information by performing integrity scans of the system;
2. The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification;
3. The organization employs centrally managed integrity verification tools;
4. The use of integrity verification applications must not adversely impact the operational performance of the control system.

## 2.14.8 Spam Protection

### 2.14.8.1 *Requirement:*

The control system implements spam protection.

### 2.14.8.2 *Supplemental Guidance:*

The organization employs spam protection mechanisms at critical control system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, and/or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet access, or other common means. The organization considers using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another for workstations).

The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between control system and general IT systems, control systems do not generally employ spam protection mechanisms. Unusual traffic flow, such as during crisis situations, may be misinterpreted and caught as spam, which can cause issues with the system and possible failure of the system.

### 2.14.8.3 *Requirement Enhancements:*

1. The organization centrally manages spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on a control system. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the control system.
2. The control system automatically updates spam protection mechanisms. Organizations consider the risk of employing mechanisms to centrally manage spam protection on a control system. The use of mechanisms to centrally managed spam protection must not degrade the operational performance of the control system.

## 2.14.9 Information Input Restrictions

### 2.14.9.1 *Requirement:*

The organization implements security measures to restrict information input to the control system to authorized personnel only.

### 2.14.9.2 *Supplemental Guidance:*

Restrictions on personnel authorized to input information to the control system may extend beyond the typical access requirements employed by the system and include limitations based on specific operational or project responsibilities.

### 2.14.9.3 *Requirement Enhancements:*

None.

## 2.14.10 Information Input Accuracy, Completeness, Validity, and Authenticity

### 2.14.10.1 *Requirement:*

The control system employs mechanisms to check information for accuracy, completeness, validity, and authenticity.



#### **2.14.10.2 Supplemental Guidance:**

Organization checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of control system inputs (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Inputs passed to interpreters are pre-screened to ensure the content is not unintentionally interpreted as commands. The extent to which the control system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

#### **2.14.10.3 Requirement Enhancements:**

None.

### **2.14.11 Error Handling**

#### **2.14.11.1 Requirement:**

The control system employs mechanisms to identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries.

#### **2.14.11.2 Supplemental Guidance:**

The structure and content of error messages need to be carefully considered by the organization. Error messages generated by the control system need to provide timely and useful information without providing potentially harmful information that could be exploited by adversaries. System error messages are revealed only to authorized personnel (e.g., systems administrators, maintenance personnel). Sensitive information (e.g., account numbers, passwords, and personnel ID numbers) is not to be listed in error logs or associated administrative messages. The extent to which the control system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### **2.14.11.3 Requirement Enhancements:**

None.

### **2.14.12 Information Output Handling and Retention**

#### **2.14.12.1 Requirement:**

The organization handles and retains output from the control system in accordance with applicable laws, regulations, standards, and organizational policy, as well as operational requirements of the control process.

#### **2.14.12.2 Supplemental Guidance:**

None.

#### **2.14.12.3 Requirement Enhancements:**

None.

## 2.15 Access Control

The focus of access control is ensuring that resources are only accessed by the appropriate personnel and that personnel are correctly identified. The first step in access control is creating access control lists with access privileges for personnel. The next step is to implement security mechanisms to enforce the access control lists. Mechanisms also need to be put into place to monitor access activities for inappropriate activity. The access control lists need to be managed through adding, altering, and removing access rights as necessary.

Identification and authentication is the process of verifying the identity of a user, process, or device, as a prerequisite for granting access to resources in a control system. Identification could be a password, a token, or a fingerprint. Authentication is the challenge process to prove (validate) the identification provided. An example would be using a fingerprint (identification) to access a computer via a biometric device (authentication). The biometric device authenticates the identity of the fingerprint.

### 2.15.1 Access Control Policy and Procedures

#### 2.15.1.1 Requirement:

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

1. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

#### 2.15.1.2 Supplemental Guidance:

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

#### 2.15.1.3 Requirement Enhancements:

None.

### 2.15.2 Identification and Authentication Policy and Procedures

#### 2.15.2.1 Requirement:

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

1. A formal, documented, identification and authentication 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 identification and authentication policy and associated identification and authentication controls.

#### 2.15.2.2 Supplemental Guidance:

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

### **2.15.2.3 Requirement Enhancements:**

None.

## **2.15.3 Account Management**

### **2.15.3.1 Requirement:**

The organization manages control system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews control system accounts at least annually.

### **2.15.3.2 Supplemental Guidance:**

Account management includes the identification of account types (i.e., individual, group, role-based, device-based, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the control system and specifies access rights and privileges; i.e., access control list. The organization grants access to the control system based on:

1. A valid need-to-know/need-to-share basis that is determined by assigned official duties and that satisfies all personnel security criteria;
2. Intended system use. The organization requires proper identification for requests to establish control system accounts and must approve all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers for the control system are notified when users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' control system usage or need-to-know/need-to-share changes. In cases where accounts are role-based, i.e., the workstation, hardware, and/or field devices define a user role, access to the control system includes physical security policies and procedures based on organization risk assessment. In cases where physical access to the workstation, hardware, and/or field devices predefine privileges, the organization implements physical security policies, and procedures based on organization risk assessment. Account management may include additional account types (e.g., role-based, device-based, attribute-based). The organization removes, disables, or otherwise secures default accounts (e.g., maintenance). Default passwords are changed.

### **2.15.3.3 Requirement Enhancements:**

1. The organization employs automated mechanisms to support the management of control system accounts. For some control system components (e.g., field devices), account management may have to be performed manually, where automated mechanisms are not available.
2. The control system automatically terminates temporary and emergency accounts.
3. The control system automatically disables inactive accounts.
4. The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.
5. The organization ensures default passwords are changed.

## **2.15.4 Identifier Management**

### **2.15.4.1 Requirement:**

The organization manages user identifiers by:

1. Uniquely identifying each user;
2. Verifying the identity of each user;
3. Receiving authorization to issue a user identifier from an appropriate organization official;
4. Ensuring that the user identifier is issued to the intended party;
5. Disabling user identifier after a pre-determined defined time period of inactivity;
6. Archiving user identifiers.

#### **2.15.4.2 Supplemental Guidance:**

Identifier management is not applicable to shared control system accounts (e.g., guest and anonymous accounts).

Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based. For some control systems, the capability for immediate operator interaction is critical. Local emergency actions for the control system must not be hampered by identification requirements. Access to these systems may be restricted by appropriate physical security mechanisms.

#### **2.15.4.3 Requirement Enhancements:**

None.

## **2.15.5 Authenticator Management**

#### **2.15.5.1 Requirement:**

The organization manages control system authenticators by:

1. Defining initial authenticator content;
2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;
3. Changing default authenticators upon control system installation;
4. Changing/refreshing authenticators periodically.

#### **2.15.5.2 Supplemental Guidance:**

System authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.

Passwords should not be embedded into tools, source code, scripts, aliases or shortcuts. Many control system devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great security risk and therefore should be changed.

#### **2.15.5.3 Requirement Enhancements:**

For password-based authentication, the control system:

1. Protects passwords from unauthorized disclosure and modification when stored or transmitted;
2. Prohibits passwords from being displayed when entered;
3. Enforces password minimum and maximum lifetime restrictions;
4. Prohibits password reuse for a specified number of generations.

For PKI-based authentication, the control system:

1. Validates certificates by constructing a certification path to an accepted trust anchor;
2. Establishes control of the corresponding private key;
3. Maps the authenticated identity to the user account.

## 2.15.6 Supervision and Review

### 2.15.6.1 *Requirement:*

The organization supervises and reviews the activities of users with respect to the enforcement and usage of control system access control.

### 2.15.6.2 *Supplemental Guidance:*

The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual control system-related activities and periodically reviews changes to access authorizations. The organization reviews the activities of users with significant roles and responsibilities for the control system more frequently. The extent of the audit record reviews is based on the impact level of the control system. For example, for low-impact systems it is not intended that security logs be reviewed frequently for every workstation but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records.

### 2.15.6.3 *Requirement Enhancements:*

The organization employs automated mechanisms to facilitate the review of user activities on the control system.

## 2.15.7 Access Enforcement

### 2.15.7.1 *Requirement:*

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

### 2.15.7.2 *Supplemental Guidance:*

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, and cryptography) are employed by organizations to control access to the control system. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

### 2.15.7.3 *Requirement Enhancements:*

1. The control system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Explicitly authorized personnel include, for example, control system operators, security administrators, system and network administrators, and other privileged users who have access to system control, monitoring, or administration functions. Access to privileged functions by privileged users may also be restricted based on devices (e.g., remote terminal units and field devices).
2. The control system requires dual authorization, based on approved organization procedures, to privileged functions that have impacts on facility, human, and environmental safety. The organization does not employ dual-approval mechanisms when an immediate response is necessary to ensure human and environmental safety (e.g., a safety valve).

3. Access enforcement mechanisms must not adversely impact the operational performance of the control system.

## **2.15.8 Separation of Duties**

### **2.15.8.1 Requirement:**

The control system enforces separation of duties through assigned access authorizations.

### **2.15.8.2 Supplemental Guidance:**

The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Access control software needs to be on the control system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include 1) mission functions and distinct control system support functions are divided among different individuals/roles; 2) different individuals perform control system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and 3) security personnel who administer access control functions must not administer audit functions.

### **2.15.8.3 Requirement Enhancements:**

None.

## **2.15.9 Least Privilege**

### **2.15.9.1 Requirement:**

The control system enforces the most restrictive set of rights/privileges or accesses needed by users or workstations (or processes acting on behalf of users) for the performance of specified tasks.

### **2.15.9.2 Supplemental Guidance:**

The organization employs the concept of least privilege for specific duties and control system (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

### **2.15.9.3 Requirement Enhancements:**

None.

## **2.15.10 User Identification and Authentication**

### **2.15.10.1 Requirement:**

The control system has mechanisms to uniquely identify and authenticate users (or processes acting on behalf of users).

### **2.15.10.2 Supplemental Guidance:**

Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination of these. Remote access

is any access to an organizational control system by a user (or a control system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational control system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. In addition to identifying and authenticating users at the control system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For some control systems, the capability for immediate operator interaction is critical. Local emergency actions for the control system must not be hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security mechanisms.

**2.15.10.3 Requirement Enhancements:**

Remote user access to control system components is only enabled when necessary, approved, and authenticated.

**2.15.11 Permitted Actions Without Identification or Authentication**

**2.15.11.1 Requirement:**

The organization identifies and documents specific user actions that can be performed on the control system without identification or authentication.

**2.15.11.2 Supplemental Guidance:**

The organization may allow limited user activity without identification and authentication only for initial log on activities or monitoring remote field devices and the control system.

**2.15.11.3 Requirement Enhancements:**

The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

**2.15.12 Device Identification and Authentication**

**2.15.12.1 Requirement:**

The control system employs a mechanism to identify and authenticate specific devices before establishing a connection.

**2.15.12.2 Supplemental Guidance:**

The strength of the device authentication mechanism is based on the security categorization of the control system. Automatic equipment identification may be considered as a means to authenticate connections. When practical, field devices need to be chosen with capability to support authentication mechanisms

**2.15.12.3 Requirement Enhancements:**

None.

## **2.15.13 Authenticator Feedback**

### **2.15.13.1 Requirement:**

The authentication mechanisms in the control system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

### **2.15.13.2 Supplemental Guidance:**

The control system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the control system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.

### **2.15.13.3 Requirement Enhancements:**

None.

## **2.15.14 Cryptographic Module Authentication**

### **2.15.14.1 Requirement:**

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

### **2.15.14.2 Supplemental Guidance:**

None.

### **2.15.14.3 Requirement Enhancements:**

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

## **2.15.15 Information Flow Enforcement**

### **2.15.15.1 Requirement:**

The control system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

### **2.15.15.2 Supplemental Guidance:**

Information flow control regulates where information is allowed to travel within a control system and between control systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few general examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within control systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards,



encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict control system services or provide a packet-filtering capability.

**2.15.15.3 Requirement Enhancements:**

1. The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions. Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.
2. The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.
3. The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

**2.15.16 Passwords**

**2.15.16.1 Requirement:**

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

**2.15.16.2 Supplemental Guidance:**

1. Default passwords of applications, operating systems, database management systems, or other programs must be changed immediately after installation.
2. The organization replaces default usernames whenever possible. Passwords need to be allocated, protected, and used based on the criticality level of the systems to be accessed.
3. The organization develops policies that stipulate the complexity (min/max length, combination of lower/upper case, numerals, special characters, etc.) level of the password for each criticality level. Short or easily guessed passwords are prohibited. Passwords can be a means of system protection when properly generated and used. Although passwords are not advisable in all control system applications, there are some cases where they are of benefit such as for remote access. These passwords are developed to meet defined metrics.
4. Good security practices need to be followed in the generation of passwords. Passwords should not easily be associated with the user or the organization and follow appropriate complexity rules. Initial or default passwords are changed immediately on first log-in. Following generation, passwords are not sent across any network unless protected by encryption or salted cryptographic hash specifically designed to prevent replay attacks.
5. Passwords need to be transferred to the user via secure media and the recipient must be verified. The logon ID and password is never combined in the same communication.
6. The authority to keep and change high-level passwords is given to a trusted employee who is available during emergencies.
7. A log for master passwords needs to be maintained separately from the control system, possibly in a notebook in a vault or safe.
8. Passwords need to be changed regularly and expire when the user leaves the organization or after an extended period of inactivity.
9. Users are responsible for their passwords and are instructed not to share them or write them down, and need to be aware of their surroundings when entering passwords. If the operating system supports encryption, stored passwords are encrypted. Passwords are not to be embedded into tools, source code, scripts, aliases or shortcuts.

**2.15.16.3 Requirement Enhancements:**

None.

## **2.15.17 System Use Notification**

### **2.15.17.1 Requirement:**

The organization displays an approved, system use notification message before granting access to the control system.

### **2.15.17.2 Supplemental Guidance:**

The organization or the control system displays an approved, system-use notification message at the time of control system logon informing the user:

1. Of the organization's privacy policy before granting system access to potential users and/or workstations;
2. That system usage may be monitored, recorded, and subject to audit;
3. That unauthorized use of the system is prohibited and subject to criminal and civil penalties;
4. That use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on organization's associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to control system. Privacy and security policies are consistent with applicable federal and state laws, organization directives, policies, regulations, standards, and guidance.

### **2.15.17.3 Requirement Enhancement:**

None.

## **2.15.18 Concurrent Session Control**

### **2.15.18.1 Requirement:**

The organization limits the number of concurrent sessions for any user on the control system.

### **2.15.18.2 Supplemental Guidance:**

Some control system components may not allow concurrent sessions to be limited.

### **2.15.18.3 Requirement Enhancements:**

None.

## **2.15.19 Previous Logon Notification**

### **2.15.19.1 Requirement:**

The control system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.

### **2.15.19.2 Supplemental Guidance:**

None.

### **2.15.19.3 Requirement Enhancements:**

None.

## 2.15.20 Unsuccessful Login Attempts

### 2.15.20.1 *Requirement:*

The control system limits the number of consecutive invalid access attempts by a user during a given time period. The control system temporarily disables the user account when the maximum number of unsuccessful attempts is exceeded and logs all unsuccessful login attempts.

### 2.15.20.2 *Supplemental Guidance:*

Because of the potential for denial of service, automatic lockouts initiated by the control system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by the control system must be carefully considered before being used due to safety considerations and the potential for denial of service.

### 2.15.20.3 *Requirement Enhancements:*

The control system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

## 2.15.21 Session Lock

### 2.15.21.1 *Requirement:*

After a predetermined period of inactivity, the control system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

### 2.15.21.2 *Supplemental Guidance:*

Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the control system.

### 2.15.21.3 *Requirement Enhancements:*

None.

## 2.15.22 Remote Session Termination

### 2.15.22.1 *Requirement:*

The control system automatically terminates a remote session after a defined period of inactivity for workstations that are used for control system monitoring and maintenance activities based on the risk assessment of the control system and the organization's security policy.

### 2.15.22.2 *Supplemental Guidance:*

A remote session is initiated whenever an organizational control system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Some control systems or components may not or cannot allow sessions to be terminated.

### 2.15.22.3 *Requirement Enhancements:*

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

## 2.15.23 Remote Access Policy and Procedures

### 2.15.23.1 Requirement:

The organization develops a formal written policy and appropriate security procedures to address and protect against the risks of remote access to the control system, field devices, and communication facilities.

### 2.15.23.2 Supplemental Guidance:

In many cases, system components are not located within the boundaries of the control room or where there may be a need for access to equipment remote from the user, including telecommuting or mobile computing. A formal, written procedure is needed to address access to systems remote from the user. This policy might include system locking of an interactive session after a specified period of user inactivity, using encrypted password setting on boot up and login for computers not in the control room, encrypted file system, callback and authentication on modems, or the inactivation or disconnection from the network when connections are not required. Appropriate organization officials need to authorize each remote access method for the control system and authorize only the necessary users, based on their roles and responsibilities, for access methods identified in the risk assessment.

### 2.15.23.3 Requirement Enhancements:

None.

## 2.15.24 Remote Access

### 2.15.24.1 Requirement:

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

### 2.15.24.2 Supplemental Guidance:

The organization documents, monitors, and manages all methods of remote access (e.g., dialup, Internet, physical) to the control system. Appropriate authentication methods are needed to adequately secure remote access.

Remote access is any access to an organizational control system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access security requirements are applicable to control systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).

Remote access to control system component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated. The organization considers multifactor authentication for remote user access to the control system.

### 2.15.24.3 Requirement Enhancements:

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

2. The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. Any latency induced from the use of encryption, must not degrade the operational performance of the control system.
3. The organization provides remote accesses through a limited number of managed access control points.
4. The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the control system.

## **2.15.25 Access Control for Portable and Mobile Devices**

### **2.15.25.1 Requirement:**

The organization 1) establishes use restrictions and implementation guidance for all portable media and mobile IT devices and 2) documents, monitors, logs, and limits access of these portable media and mobile devices to organizational control system. Appropriate organizational officials authorize the use of portable and mobile devices per organization's established security policy and procedures.

### **2.15.25.2 Supplemental Guidance:**

Portable media and mobile devices (e.g., notebook computers, workstations, and personal digital assistants) are allowed access to organizational networks and control system by meeting organizational security policies and procedures. Security policies and procedures include such activities as scanning the 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). Organizations consider disabling unused or unnecessary I/O ports.

### **2.15.25.3 Requirement Enhancements:**

None.

## **2.15.26 Wireless Access Restrictions**

### **2.15.26.1 Requirement:**

The organization 1) establishes use restrictions and implementation guidance for wireless technologies and 2) authorizes, monitors, and manages wireless access to the control system.

### **2.15.26.2 Supplemental Guidance:**

The organization uses authentication and cryptography or enhanced defense mechanisms to protect wireless access to the control system.

Wireless technologies include, but are not limited to, microwave, satellite, packet radio [UHF/VHF], 802.11x and Bluetooth.

### **2.15.26.3 Requirement Enhancements:**

1. The organization uses authentication and encryption to protect wireless access to the control system. Any latency induced from the use of encryption, must not degrade the operational performance of the control system.
2. The organization scans for unauthorized wireless access points at a specified frequency and takes appropriate action if such access points are discovered. Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact

control systems. The scan is not limited to only those areas within the facility containing the high-impact control systems.

## **2.15.27 Personally Owned Information**

### **2.15.27.1 Requirement:**

The organization restricts the use of personally owned information copied to the control system or control system user workstation that is used for official organization business. This includes the processing, storage, or transmission of organization business and critical control system information. The terms and conditions need to address, at a minimum;

1. The types of applications that can be accessed from personally owned IT, either remotely or from within the organization control system;
2. The maximum security category of information that can processed, stored, and transmitted;
3. How other users of the personally owned control system will be prevented from accessing organization information;
4. The use of virtual private networking (VPN) and firewall technologies;
5. The use of and protection against the vulnerabilities of wireless technologies;
6. The maintenance of adequate physical security mechanisms;
7. The use of virus and spyware protection software; and
8. How often the security capabilities of installed software are to be updated (e.g., operating system and other software security patches, virus definitions, firewall version updates, malware definitions).

### **2.15.27.2 Supplemental Guidance:**

The organization establishes strict terms and conditions for the use of personally owned information on control systems and control systems user workstations.

### **2.15.27.3 Requirement Enhancements:**

None.

## **2.15.28 External Access Protections**

### **2.15.28.1 Requirement:**

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

### **2.15.28.2 Supplemental Guidance:**

Public access is defined as access from the enterprise system. Care should be taken to ensure data shared with the enterprise system are protected for integrity of the information and applications. Public access to the control system to satisfy business requirements needs to be limited to read only access through the corporate enterprise systems via a demilitarized zone (DMZ). The organization explicitly allows necessary network protocols in the DMZ; blocks or filters unnecessary protocols, configure firewalls to block inbound connections, limits outbound connections to only those specifically required for operations, and eliminates network connections that bypass perimeter protection Mechanisms (e.g. firewall, VPN, DMZ).

### **2.15.28.3 Requirement Enhancements:**

None.

## **2.15.29 Use of External Information Control Systems**

### **2.15.29.1 Requirement:**

The organization establishes terms and conditions for authorized individuals to:

1. Access the control system from an external system;
2. Process, store, and/or transmit organization-controlled information using an external system.

### **2.15.29.2 Supplemental Guidance:**

External systems are systems or components of systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no control over the application of required security levels or the assessment of security effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems).

### **2.15.29.3 Requirement Enhancements:**

1. The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address, as a minimum the types of applications that can be accessed on the organizational information system from the external information system.
2. The organization prohibits authorized individuals from using an external system to access the control system or to process, store, or transmit organization-controlled information except in situations where the organization: 1) can verify the employment of required security mechanisms on the external system as specified in the organization's security policy and system security plan; or 2) has approved system connection or processing agreements with the organizational entity hosting the external system.

## 2.16 Audit and Accountability

Periodic audits and logging of the control system need to be implemented to validate that the security mechanisms present during system validation testing are still installed and operating correctly. These security audits review and examine a system's records and activities to determine the adequacy of system security controls and to ensure compliance with established security policy and procedures. Audits are also used to detect breaches in security services through examination of system logs. Logging is necessary for anomaly detection as well as forensic analysis.

### 2.16.1 Audit and Accountability Policy and Procedures

#### 2.16.1.1 *Requirement:*

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

1. A formal, documented, audit and accountability 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 audit and accountability policy and associated audit and accountability controls.

#### 2.16.1.2 *Supplemental Guidance:*

The organization ensures the audit and accountability policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The audit and accountability 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 a particular control system, when required.

#### 2.16.1.3 *Requirement Enhancements:*

None.

### 2.16.2 Auditable Events

#### 2.16.2.1 *Requirement:*

The control system generates audit records, at a minimum, for the following events whether or not the attempts were successful:

1. Attempts to logon;
2. Attempts to change local account attributes such as privileges;
3. Attempts to change local security policy.

#### 2.16.2.2 *Supplemental Guidance:*

The organization specifies which control system components carry out auditing activities and ensures that certain events are included or excluded from the set of auditable events based on specified attributes. Auditing activity can affect control system performance; therefore, the organization decides, based on a risk assessment, which events require auditing continually and which events require auditing in response to specific situations. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. The targeted security functionality should be able to generate an audit record of:

1. Startup and shutdown of the audit functions;
2. All auditable events for the minimum level of audit;



3. Non-allowed port, IPSec authentication error, failed key change, or administrator authentication error.

The purpose of this requirement is to identify significant and relevant events to the security of the control system that needs to be audited. The organization specifies which control system components carry out auditing activities. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

#### **2.16.2.3 Requirement Enhancements:**

1. The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.
2. The information system provides the capability to manage the selection of events to be audited by individual components of the system.
3. The organization periodically reviews and updates the list of organization-defined auditable events.

### **2.16.3 Content of Audit Records**

#### **2.16.3.1 Requirement:**

The control system captures sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes.

#### **2.16.3.2 Supplemental Guidance:**

Two types of audits need to be tracked:

1. General quality assurance audits of the configuration and operation of the control system that verify compliance with organization's security plan;
2. Audits of operational events encountered by the system when the system operates outside its normal operating parameters.

General quality assurance audit records contain information of what was audited and the results of the audit; that is, the system is in compliance or not, and if not, what areas are out of compliance. Operational event audits are initiated by the organization's corrective action process when the control system operates outside its normal operating parameters.

Audit record content typically includes:

1. Date and time of the event;
2. The component of the control system (e.g., software or hardware component) where the event occurred;
3. Type of event;
4. User/subject/device identity;
5. The operational consequences in the case of an operational event.

#### **2.16.3.3 Requirement Enhancements:**

1. The control system provides the capability to include additional, more detailed information in the records for audit events identified by type, location, or subject;
2. The control system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

## **2.16.4 Audit Storage Capacity**

### **2.16.4.1 Requirement:**

The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

### **2.16.4.2 Supplemental Guidance:**

None.

### **2.16.4.3 Requirement Enhancements:**

None.

## **2.16.5 Response to Audit Processing Failures**

### **2.16.5.1 Requirement:**

The control system alerts appropriate organization personnel in the event of an audit failure and takes actions such as:

1. Overwrite the oldest audit records;
2. Stop generating audit records.

### **2.16.5.2 Supplemental Guidance:**

Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

### **2.16.5.3 Requirement Enhancements:**

1. The control system provides a warning when allocated audit record storage volume reaches organization-defined percentage of maximum audit record storage capacity;
2. The control system provides a real-time alert when the following organization defined audit failure events occur.

## **2.16.6 Audit Monitoring, Analysis, and Reporting**

### **2.16.6.1 Requirement:**

The organization regularly monitors, reviews, and analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

### **2.16.6.2 Supplemental Guidance:**

Organizations increase the level of audit monitoring and analysis activity within the control system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. Audit records need to be monitored regularly for inappropriate activities in accordance with organizational procedures. Audit reports need to be provided to those responsible for cyber security.

### **2.16.6.3 Requirement Enhancements:**

1. The organization has automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response of suspicious activities.
2. The organization employs automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications.

## **2.16.7 Audit Reduction and Report Generation**

### **2.16.7.1 Requirement:**

The control system provides an audit reduction and report generation capability.

### **2.16.7.2 Supplemental Guidance:**

Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

In general, audit record processing is not performed on the control system.

### **2.16.7.3 Requirement Enhancements:**

1. The control system provides the capability to automatically process audit records for events of interest based upon selectable event criteria;
2. Audit record processing must not degrade the operational performance of the control system.

## **2.16.8 Time Stamps**

### **2.16.8.1 Requirement:**

The control system provides time stamps for use in audit record generation.

### **2.16.8.2 Supplemental Guidance:**

Time stamps of audit records are generated using internal system clocks.

### **2.16.8.3 Requirement Enhancements:**

None.

## **2.16.9 Protection of Audit Information**

### **2.16.9.1 Requirement:**

The control system protects audit information and audit tools from unauthorized access, modification, and deletion.

### **2.16.9.2 Supplemental Guidance:**

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit control system activity. The logs are important for error correction, security breach recovery, investigations, and related efforts.

### **2.16.9.3 Requirement Enhancements:**

None.

## **2.16.10 Audit Record Retention**

### **2.16.10.1 Requirement:**

The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

### **2.16.10.2 Supplemental Guidance:**

Logs containing computer or communication system security relevant events need to be retained for a period as defined in the information retention policy. . The organization retains audit records until it is determined that they are no longer needed for administrative, legal, regulatory, or other operational purposes.

### **2.16.10.3 Requirement Enhancements:**

None.

## **2.16.11 Conduct and Frequency of Audits**

### **2.16.11.1 Requirement:**

The organization conducts audits at planned intervals to determine whether the security objectives, measures, processes, and procedures:

1. Conform to the requirements and relevant legislation or regulations;
2. Conform to the identified information security requirements;
3. Are effectively implemented and maintained;
4. Perform as expected;
5. Identify inappropriate activities.

### **2.16.11.2 Supplemental Guidance:**

Audits can be either in the form of internal self-assessment or independent, third-party audits. Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for internal purposes. An internal audit needs to be conducted to ensure that documentation is current with any changes to the system. Independent audits review and examine records and activities to assess the adequacy of control system security measures, ensure compliance with established policies and operational procedures, and recommend necessary changes in security requirements, policies, or procedures. For independent audits, the auditor(s) need to be accompanied by an appropriate knowledgeable control system staff person(s) to answer any questions about the particular system under review.

### **2.16.11.3 Requirement Enhancements:**

None.

## **2.16.12 Auditor Qualification**

### **2.16.12.1 Requirement:**

The organization's audit program specifies auditor qualifications in accordance with the organization's documented training program.

### **2.16.12.2 Supplemental Guidance:**

The selection of auditors and conduct of audits ensure the objectivity and impartiality of the audit process. Security auditors need to:

1. Understand the control system to be audited and be personally familiar with the systems and operating practices;
2. Understand the risk involved with the audit and the consequences associated with unintentional stimulus or denial of service to the control system;
3. Fully understand 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.

**2.16.12.3 Requirement Enhancements:**

The organization assigns auditor and system administration functions to separate personnel.

## **2.16.13 Audit Tools**

**2.16.13.1 Requirement:**

The organization under the audit program specifies strict rules and careful use of audit tools when auditing control system functions.

**2.16.13.2 Supplemental Guidance:**

As a general practice, system audits determine compliance of the control system to the organization's security plan. For new control systems, system auditing utilities need to be incorporated into the design. Appropriate security audit practices for legacy systems require appropriate precautions be taken before assessing the system. For system audits to determine inappropriate activity, information custodians ensure that system monitoring tools are installed to log system activity and security events. Auditing and log management tools need to be used cautiously in maintaining and proving the integrity of the control system from installation through the system life cycle. Access to control systems audit tools need to be protected to prevent any possible misuse or compromise.

**2.16.13.3 Requirement Enhancements:**

If automated cyber security scanning tools are used on business networks, extra care needs to be taken to ensure that they do not scan the control system network by mistake. Many installed devices do not have much processing power or sophisticated error-handling routines, and scans can overload the device and effectively create a denial-of-service interruption that could lead to equipment damage, production loss, or health, safety and environmental incidents.

## **2.16.14 Security Policy Compliance**

**2.16.14.1 Requirement:**

The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.

**2.16.14.2 Supplemental Guidance:**

Periodic audits of the control system are implemented to demonstrate compliance to the organization's security policy. These audits:

1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed;
2. Document and ensure compliance to organization policies and procedures;

3. Identify security concerns, validate the system is free from security compromises, and provide information on the nature and extent of compromises should they occur;
4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes;
5. Verify that security mechanisms and management practices present during system validation are still in place and functioning;
6. Ensure reliability and availability of the system to support safe operation;
7. Continuously improve performance.

**2.16.14.3 Requirement Enhancements:**

None.

## **2.17 Monitoring and Reviewing Control System Security Policy**

Monitoring and reviewing the performance of an organization's cyber and control system security policy provides the organization the ability to evaluate the performance of their security program. Internal checking methods, such as compliance audits and incident investigations, allow the company to determine the effectiveness of the security program and whether it is operating according to expectations. Finally, through a continuous improvement process, the organization's senior leaders regularly review compliance information on the security program, developed through the audit and corrective action process, and any deviations from the goals, targets, and objectives set in the planning process. If there are deviations or nonconformance, it may be necessary to revisit the original assumptions and implement appropriate corrective actions.

### **2.17.1 Monitoring and Reviewing Control System Security Management Policy and Procedures**

#### **2.17.1.1 Requirement:**

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

1. A formal, documented, monitoring and reviewing control system security 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 monitoring and reviewing control system security management policy and associated audit and accountability controls.

#### **2.17.1.2 Supplemental Guidance:**

The organization ensures the monitoring and reviewing of control system security management policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The monitoring and reviewing of control system security management 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 a particular control system, when required.

#### **2.17.1.3 Requirement Enhancements:**

None.

### **2.17.2 Continuous Improvement**

#### **2.17.2.1 Requirement:**

The organization's security program implements continuous improvement practices to ensure that industry lessons-learned and best practices are incorporated into control system security policies and procedures.

#### **2.17.2.2 Supplemental Guidance:**

None.

#### **2.17.2.3 Requirement Enhancements:**

None.

### **2.17.3 Monitoring of Security Policy**

#### **2.17.3.1 Requirement:**

The organization includes a process for monitoring and reviewing the performance of their cyber security policy.

**2.17.3.2 Supplemental Guidance:**

Regular review of the control system security policy needs to be done to validate its effectiveness in implementing the organization's security program and objectives. Effectiveness is measured by the results of cyber security audits, incidents, suggestions, and feedback from the organizations corrective action program.

**2.17.3.3 Requirement Enhancements:**

None.

**2.17.4 Best Practices**

**2.17.4.1 Requirement:**

The organization incorporates industry best practices into the organization's security program for control systems.

**2.17.4.2 Supplemental Guidance:**

Best practices include, but are not be limited to, industry events that identify failed and successful cyber security breaches; actions to be taken to resolve a breach of cyber security that are defined in light of the business priorities; processes employed to collect metrics (e.g., audits, incidents) that help verify that the cyber security activities (manual or automated) are performing as expected; a process that will trigger a review of the level of residual risk and acceptable risk taking when there are changes to the organization, technology, business objectives, processes and external events including identified threats and changes in social climate; and operational data analyzed, recorded, and reported to assess the effectiveness or performance of the cyber security management system.

**2.17.4.3 Requirement Enhancements:**

None.

**2.17.5 Security Accreditation**

**2.17.5.1 Requirement:**

The organization authorizes (i.e., accredits) the control system for processing before operations and periodically updates the authorization based on organization-defined frequency or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

**2.17.5.2 Supplemental Guidance:**

The organization assesses the security mechanisms employed within the control systems before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications and need to be reviewed annually.

**2.17.5.3 Requirement Enhancements:**

None.



## 2.17.6 Security Certification

### 2.17.6.1 *Requirement:*

The organization conducts an assessment of the security mechanisms in the control system to determine the extent to which the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

### 2.17.6.2 *Supplemental Guidance:*

Assessments are performed and documented by qualified assessors as authorized by the organization. External audits are outside the scope of this requirement. Ensure that the assessments do not interfere with control system functions. Care must be taken to ensure that the assessments do not interfere with control system functions. The assessor 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. A control system may need to be taken off-line, to the extent feasible, before the assessments can be conducted. If a control system must be taken off-line for assessments, assessments are scheduled to occur during planned control system outages whenever possible.

### 2.17.6.3 *Requirement Enhancements:*

1. The organization employs an independent certification agent or certification team to conduct an assessment of the security mechanisms in the control system.
2. An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational control system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the control system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization.
3. Contracted certification services are considered independent if the control system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security mechanisms in the control system.
4. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the control system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.
5. In special situations, for example when the organization that owns the control system is small or the organizational structure requires that the assessment of the security mechanisms be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results.
6. The authorizing official should consult with representatives of the appropriate regulatory bodies, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

## 2.18 Risk Management and Assessment

Risk management planning is a key aspect of ensuring that the processes and technical means of securing control systems have fully addressed the risks and vulnerabilities in the system.

An organization identifies and classifies risks to develop appropriate security measures. Risk identification and classification involves security assessments of control system and interconnections to identify critical components and any areas weak in security. The risk identification and classification process is continually performed to monitor the control system's compliance status. A documented plan is developed on how the organization will strive to stay in compliance within acceptable risk.

A comprehensive organization risk assessment process is implemented and periodically executed. Assets are categorized into security levels based on the level of security is necessary for each asset to be sufficiently protected. Risk is assessed across the organization by determining the likelihood of potential threats and cost if the threat is realized. Control system vulnerabilities need to be recognized and documented.

### 2.18.1 Risk Assessment Policy and Procedures

#### 2.18.1.1 *Requirement:*

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

1. A formal, documented risk assessment 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 risk assessment policy and associated risk assessment controls.

#### 2.18.1.2 *Supplemental Guidance:*

The organization ensures the risk assessment policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The risk assessment policy also takes into account the organization's risk tolerance level. The risk assessment policy can be included as part of the general security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular control system, when required.

#### 2.18.1.3 *Requirement Enhancements:*

None.

### 2.18.2 Risk Management Plan

#### 2.18.2.1 *Requirement:*

The organization develops a risk management plan. The risk management plan is reviewed and approved by a senior organization official.

#### 2.18.2.2 *Supplemental Guidance:*

None.

#### 2.18.2.3 *Requirement Enhancements:*

None.

## **2.18.3 Certification, Accreditation, and Security Assessment Policies and Procedures**

### **2.18.3.1 Requirement:**

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

1. Formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
2. Formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

### **2.18.3.2 Supplemental Guidance:**

The organization ensures the security assessment and certification and accreditation policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The certification, accreditation, and security assessment policies can be included as part of the general information security policy for the organization. Certification, accreditation, and security assessment procedures can be developed for the security program in general, and for a particular control system, when required. The organization defines what constitutes a significant change to the control system to achieve consistent security reaccreditations.

### **2.18.3.3 Requirement Enhancements:**

None.

## **2.18.4 Security Assessments**

### **2.18.4.1 Requirement:**

The organization regularly conducts an assessment of the security measures in the control system to determine whether the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the control system. The security assessments are, at a minimum, conducted annually or when changes occur due to change in control system processes.

### **2.18.4.2 Supplemental Guidance:**

Security measures include administrative and personnel-based requirements. Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the control system.

The organization ensures that assessments do not interfere with control system functions. The assessor 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. A production control system may need to be taken off-line, or replicated to the extent feasible, before the assessments can be conducted. If a control system must be taken off-line for assessments, assessments are scheduled to occur during planned control system outages whenever possible.

### **2.18.4.3 Requirement Enhancements:**

None.

## 2.18.5 Control System Connections

### 2.18.5.1 *Requirement:*

The organization authorizes all connections from the control system to other systems outside of the accreditation boundary. The organization monitors and manages the system interconnections on an ongoing basis.

### 2.18.5.2 *Supplemental Guidance:*

The organization carefully considers the risks that may be introduced when control systems are connected to other control or information systems with different security requirements and security mechanisms, both within and outside the organization. Risk considerations also include information systems sharing the same control system networks and communications infrastructure.

### 2.18.5.3 *Requirement Enhancements:*

None.

## 2.18.6 Plan of Action and Milestones

### 2.18.6.1 *Requirement:*

The organization develops and updates a plan of action and milestones for the control system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security measures and to reduce or eliminate known vulnerabilities in the system. The organization reviews the action plan at least annually.

### 2.18.6.2 *Supplemental Guidance:*

The plan of action and milestone updates are based on the findings from security control assessments, security impact analyses, and continual monitoring activities.

### 2.18.6.3 *Requirement Enhancements:*

None.

## 2.18.7 Continuous Monitoring

### 2.18.7.1 *Requirement:*

The organization monitors the security mechanisms in the control system on an ongoing basis. Those security mechanisms that are volatile or critical to protecting the control system are assessed at least annually. All other security mechanisms are assessed at least once during the control system's three-year accreditation cycle.

### 2.18.7.2 *Supplemental Guidance:*

Continuous monitoring activities include configuration management and monitoring of control system components, security impact analyses of changes to the system, ongoing assessment of security measures, and status reporting. The organization assesses all security measures in a control system during the initial security accreditation. Subsequent to the initial accreditation, the organization assesses a subset of the security measures annually during continuous monitoring. The selection of an appropriate subset of security measures is based on:

1. The security categorization of the control system;
2. The specific security measures selected and employed by the organization to protect the control system;

3. The level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security measures in the control system.

The organization establishes the selection criteria for control monitoring and subsequently selects a subset of the security measures employed within the control system for continuous monitoring. The organization also establishes the schedule for monitoring to ensure adequate coverage is achieved.

This requirement is closely related to and mutually supportive of the activities required in monitoring configuration changes to the control system. An effective, continuous monitoring program results in ongoing updates to the control system security plan, the security assessment report, and the plan of action and milestones—the three principal documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the control system.

**2.18.7.3 Requirement Enhancements:**

1. The organization employs an independent certification agent or certification team to monitor the security mechanisms in the control system on an ongoing basis.
2. The organization can extend and maximize the value of the ongoing assessment of security mechanisms during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security measures during the control system's three-year accreditation cycle.

## **2.18.8 Security Categorization**

**2.18.8.1 Requirement:**

The organization categorizes the control system and the information processed, stored, or transmitted by the system and all security-related information in accordance with applicable laws, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the control system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

**2.18.8.2 Supplemental Guidance:**

The organization conducts security categorization as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, control system owners, and information owners. As part of a defense-in-depth protection strategy, the organization may consider partitioning higher-impact control systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk.

This control includes, but is not limited to, the categorization of control system design information, network diagrams, process programs, and vulnerability assessments. Categorization is based on the need, priority, and level of protection required commensurate with sensitivity and impact of the loss of availability, integrity, or confidentiality. The organization periodically reviews the control system and information categorizations. The organization considers safety issues in categorizing the control system. The organization also considers potential impacts to other organizations (e.g., business partners, stakeholders), including interdependencies, and potential local, regional and national impacts in categorizing the control system.

**2.18.8.3 Requirement Enhancements:**

None.

## **2.18.9 Risk Assessment**

### **2.18.9.1 Requirement:**

The organization conducts risk assessments of the control system to identify and document the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the control systems and/or control system information and processes.

### **2.18.9.2 Supplemental Guidance:**

Risk assessments take into account vulnerabilities, threat sources, risk tolerance levels, and security mechanisms planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the control system. The organization also considers potential impacts to other organizations and, in accordance with the U.S. Patriot Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the control system. The risk assessment also considers potential impacts to other organizations (e.g., business partners, stakeholders), and potential local, regional and national level impacts of the control system including interdependencies and safety issues.

### **2.18.9.3 Requirement Enhancements:**

None.

## **2.18.10 Risk Assessment Update**

### **2.18.10.1 Requirement:**

The organization updates the risk assessment plan annually or, whenever there are significant changes to the control system, the facilities where the system resides, or other conditions that may affect the security or accreditation status of the system.

### **2.18.10.2 Supplemental Guidance:**

The organization develops and documents specific criteria for what are considered significant changes to the control system.

### **2.18.10.3 Requirement Enhancements:**

None.

## **2.18.11 Vulnerability Assessment and Awareness**

### **2.18.11.1 Requirement:**

The organization, under the vulnerability assessment and awareness process, implements systematic and ongoing processes to analyze system configurations for known vulnerabilities and to ensure system configurations are reviewed at a minimum annually or as new vulnerabilities are identified and reported.

### **2.18.11.2 Supplemental Guidance:**

Vulnerability scanning is conducted using appropriate scanning tools and techniques.

1. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk.

2. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.
3. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, and static analysis of source code).
4. Automated vulnerability scanning tools are not to be used on an operational control system unless the scanning tool has been tested sufficiently to ensure that control system functions will not be degraded by the scanning process. Automated vulnerability scanners can be used on test configurations; however, care needs to be taken to ensure that the test network accurately reflects the functional control system.
5. During factory acceptance testing and site acceptance testing, vulnerability scans can be conducted on these non-production configurations. The results are used to identify vulnerabilities.
6. Organization staff obtain written approval from senior management before vulnerability scanning activities are performed.

The organization trains selected personnel in the evaluation of newly reported vulnerabilities and assessment of their relevance to the facility control system. Vulnerability information needs to be freely shared with appropriate personnel to help eliminate similar vulnerabilities in other control systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, and static analysis of source code).

The organization provides training to all employees and contract personnel to increase awareness of situations that might lead to vulnerabilities. This training is performed when an employee or contract begins work at the organization and periodically thereafter. The vulnerability awareness program is monitored and updated to encompass new vulnerabilities.

**2.18.11.3 Requirement Enhancements:**

None.

## **2.18.12 Identify, Classify, Prioritize, and Analyze Potential Security Risks**

**2.18.12.1 Requirement:**

The organization identifies, classifies, prioritizes, and analyzes potential security threats, vulnerabilities, and consequences to their control systems assets using accepted methodologies.

**2.18.12.2 Supplemental Guidance:**

The organization begins by identifying the potential risks for its system. This is not a detailed analysis but a general identification of places and systems that might be at risk. These are then classified as to potential for harm and the organizations tolerance for risk. The risks are prioritized by which are of the most concern to the organization.

Each of the risks is then analyzed using an accepted methodology. A written plan documents the types of security incidents and the response to each type. This plan includes step-by-step actions to be taken by the various organizations. Risk reduction measures are implemented and the results monitored to ensure effectiveness of the risk management plan.

The reasons for selecting or rejecting certain security mitigation measures and the risks they address need to be documented. The security measures and countermeasures contained in the risk

mitigation plan are designed to lower the risk to an acceptable level and minimize the adverse effect of a threat-exploiting vulnerability in the control system network.

**2.18.12.3 Requirement Enhancements:**

None.



### **3. CONCLUSIONS**

The scope and purpose of this document is to present a wide sampling of best practice and controls for control systems used in all industries. Since this document is not limited to a specific industry sector, it should therefore be viewed as a listing of reference information to be used when reviewing and developing standards for control systems. The recommended controls are specifically designed to provide the standards bodies of industry sectors the framework needed to develop sound security standards within each individual industry sector.

These recommendations should be reviewed periodically to stay abreast of changing control system technologies, standards, and cyber security threats to the industry. The recommendations address control system problems of a general nature. Local, state, and federal laws and regulations should be reviewed with respect to each particular industry and control system.

The recommendations presented in this document are designed to assist in creating the appropriate security program for control system networks with awareness to the threats and vulnerabilities of the enterprise. However, each industry has its own intricacies, and therefore all the recommendation may not be appropriate. The recommendations presented can be customized by standards bodies representing each particular industry and business.

## 4. GLOSSARY: DEFINITIONS OF TERMS

The terms and definitions referenced in this glossary are specific to their use in this document. No attempt has been made to correlate the definitions of the terms in this glossary with similar terms in other documents or standards.

Term	Definition
Access Control	The control of entry or use, to all or part, of any physical, functional, or logical component of a control system.
Accountability	An obligation or willingness to accept responsibility.  A property or record that ensures that the actions of an entity may be traced uniquely to that entity.
Accreditation	The official management decision given by a senior organization official to authorize operation of a control system and to explicitly accept the risk to organization operations (including mission, functions, image, or reputation), organization assets, or individuals, based on the implementation of an agreed-upon set of security measures.
Accreditation Boundary	All components of a control system to be accredited by an authorizing official and excludes separately accredited systems, to which the control system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Activities	The performance of job functions or duties (e.g., conducting system backup operations, monitoring network traffic).  An observed physical or logical event (e.g., the output from surveillance equipment or an entry in a log file).
Adequacy	Sufficient for a specific requirement or level of security.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information of a control system.
Agency	Of or belonging to the organization (e.g., senior agency information security officer).
Agreement	A contract or arrangement, either written or verbal, and sometimes enforced by law.
Approval	To give formal or official sanction.
Asset	An entity that may have value to the organization. Assets may be tangible or intangible. Assets may be people, a facility, materials, equipment, information, business reputation, an activity or operation.
Attack	Attempt to gain unauthorized access to a system's services, resources, or information, or the attempt to compromise a control system's integrity, availability, or confidentiality.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a control system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorization	The right or a permission that is granted to a system entity to access a control

<b>Term</b>	<b>Definition</b>
	system resource.
Authorizing Official	Official with the authority to formally assume responsibility for operating a control system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
Backup	A copy of information to facilitate recovery of operations or data restoration, if necessary.  Redundant control system equipment which is available to continue control system operations in the event that the primary equipment fails.
Bandwidth	The rate at which a data path (e.g., a channel) carries data, measured in bits per second.
Bluetooth	A short-range wireless standard developed to create cable-less connections between devices.
Business Network	An organization's data communications network used for general purpose business activities, typically connecting a wide variety of non-critical assets and users.
Can	The word "can," equivalent to "is able to," is used to indicate possibility and capability, whether material or physical.
Certificate	See "public key certificate."
Certification	A comprehensive assessment of the management, operational and technical security mechanisms in a control system, made in support of security accreditation, to determine the extent to which the security measures are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Chief Information Officer	An organization official responsible for: providing advice and other assistance to the head of the organization and other senior management personnel of the organization to ensure that control system technology is acquired and control system resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the organization; developing, maintaining, and facilitating the implementation of a sound and integrated control system technology architecture for the organization; and promoting the effective and efficient design and operation of all major control system resources management processes for the organization, including improvements to work processes of the organization.
Client	A device or program requesting a service.
Compromise	The unauthorized disclosure, modification, substitution, or use of data or equipment.
Confidential	Spoken, written, or electronic information that must be kept secret or in the confidence of a trusted employee; secret; private, entrusted with another's confidence or secret affairs, kept hidden or separate from the knowledge of others. Information that if released could cause harm to the operator and that is only supplied on a need-to-know basis.
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices.
Contingency	A plan for how an organization will resume partially or completely interrupted

<b>Term</b>	<b>Definition</b>
	critical function(s) within a predetermined time after a disaster or disruption
Control System	A set of hardware and software acting in concert that manage the behavior of other devices.
Controlled Interface	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system).
Cost	Value impact to the organization or person that can be measured.
Countermeasure	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a control system. Synonymous with security measures and safeguards.
Cryptographic Boundary	A logical container where all the relevant security components of a control system that employ cryptography reside. It includes the processing hardware, data and memory as well as other critical components.
Cryptographic Key (key)	A parameter used in conjunction with a cryptographic algorithm that defines the transformation of plaintext data into ciphertext data, the transformation of ciphertext data into plaintext data, a digital signature computed from data, the verification of a digital signature computed from data, an authentication code computed from data, or an exchange agreement of a shared secret.
Cryptographic Module (CM)	The set of hardware, software, and/or firmware that implements an approved security function(s) (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptography	The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
Cyber	Of, relating to, or involving computers or computer networks.
Cyber Attack	Exploitation of the software vulnerabilities of IT-based control components.
Cyber Security	The protection of digital systems and their support systems from threats of: <ul style="list-style-type: none"> <li>• Cyberspace attack by adversaries who wish to disable or manipulate them.</li> <li>• Physical attack by adversaries who wish to disable or manipulate them.</li> <li>• Access by adversaries who want to obtain, corrupt, damage or destroy sensitive information. This is an aspect of information security. Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. Note that a cyberspace attack may be mounted to obtain sensitive information to plan a future physical or cyberspace attack.</li> </ul>
Cyber Security Incident	Any malicious act or suspicious event that: <ul style="list-style-type: none"> <li>• Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,</li> <li>• Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.</li> </ul>
Data	A common term used to indicate the basic elements that can be processed or produced by a computer.

<b>Term</b>	<b>Definition</b>
Demilitarized Zone (DMZ)	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.
Denial-of-Service (DOS)	The prevention of authorized access to a system resource or the delaying of system operations and functions. (See "interruption.")
Digital Signature	The result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation.
Distributed Control Systems (DCS)	A DCS is a type of plant automation system similar to a SCADA system, except that a DCS is usually employed in factories and is located within a more confined area. It uses a high-speed communications medium, which is usually a separate wire (network) from the plant LAN. A significant amount of a closed loop control is present in the system.
Domain Name	An abstraction of IP addresses using more easily remembered names.
Electronic Security Perimeter	The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
Element	Any electrical device with terminals that may be connected to other electrical devices such as a generator, transformer, circuit breaker, bus section, or transmission line. An element may be comprised of one or more components.
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state [RFC 2828].
Entity	The facility or critical asset owner, operator, etc.
Environment	The ambient natural and artificial conditions that surround a piece of operating equipment.
Facility	A plant, building, structure, or complex contiguously located on the same site, defined by a single geographical perimeter (usually determined by a fence or other barrier that surrounds and limits uncontrolled access), and used by the operator or its contractors for the performance of work under the jurisdiction of the operator. The term "facility" includes the land (soil), surface water, and groundwater contained within its geographical perimeter.
File Transfer Protocol	FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download web pages, graphics, and other files from your hard drive to a remote server which allows FTP access.
Firewall	A set of programs residing on a gateway server that protect the resources of an internal network. Basically, a firewall working closely with a router program examines each network packet to determine whether to forward it to its destination. A firewall is often installed in a specially designated computer that is separate from the rest of the network so no incoming request can get directly at private network resources. There are several firewall screening methods; a simple one is to screen requests to make sure they come from an acceptable (previously identified) domain name and Internet Protocol address on known ports. For mobile users, firewalls may allow remote access to the private network using secure logon procedures and authentication mechanisms.

<b>Term</b>	<b>Definition</b>
Firmware	Programs or instructions that are permanently stored in hardware memory devices (usually read-only memories) that control hardware at a primitive level.
Gateway	A gateway is a network point that acts as an entrance to another network. [W – Gateway]
Hardware	Physical equipment directly involved in performing industrial process measuring and controlling functions.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a control system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
Information Owner	Official with statutory or operational authority for specified information and responsibility for establishing the requirements for its generation, collection, processing, dissemination, and disposal.
Information Security	The protection of information and control systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide availability, integrity, and confidentiality.
Information Security Policy	Aggregate of directives, regulations, rules, practices and procedures that prescribe how an organization manages, protects, and distributes information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the organization. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity	Quality of a control system reflecting the logical correctness and reliability of the operation of the system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.
Interface	A logical entry or exit point of a cryptographic boundary that provides access to cryptographic modules for logical information flow.
Internal	Information that is accessible to all Employees and Contractors while providing services to the organization (See Information Distribution for more details.).
Interruption	A degradation or disruption of the communication from a device using message flooding, generation of invalid messages, or physical attacks on the communication system. Most commonly known as Denial of Service (DoS) or Distributed Denial of Service (DDoS) if multiple attackers are involved.
Intrusion	Unauthorized act of bypassing the security boundaries of a system.
Intrusion Detection	Intrusion detection (IDet) is a type of security management system for computers and networks. An IDet system gathers and analyzes information from various areas within a device or a network to identify possible security breaches, including intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

<b>Term</b>	<b>Definition</b>
IPSec	Short for “IP Security,” a set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs). IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.
Key	See cryptographic key.
Key Establishment	The process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.
Label	In data processing, a set of symbols used to identify or describe an item, record, message, or file. Occasionally it may be the same as the address in storage.
Malware	Malicious software developed to cause harm or undesirable effects to a computer or device.
Master	A device that initiates communications requests to gather data or perform control functions.
May	The word “may,” equivalent to “is permitted,” is used to indicate a course of action permissible.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, firmware, or physical devices) employed within or at the boundary of a control system.
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within a control system.  The physical interconnection between devices attached to a network. Typical media are twisted pair, baseband coax, broadband coax, and fiber optics.
Message	An arbitrary amount of information whose beginning and end are defined or implied.
Mobile Code	Software programs or parts of programs obtained from remote control systems, transmitted across a network, and executed on a local control system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Modification	The alteration of data or information; in the adverse situation, the alteration results in a condition other than intended by the originator.
Monitor	To measure a quantity continuously or at regular intervals so that corrections to a process or condition may be made without delay if the quantity varies outside of

<b>Term</b>	<b>Definition</b>
	prescribed limits. Software or hardware that observes, supervises, or verifies the operations of a system.
Monitoring	The act of observing, carrying out surveillance on, and/or recording the presence of individuals for the purpose of maintaining and improving procedural standards and security. The act of detecting the presence of unauthorized personnel, sounds, or visual signals, and the measurement thereof with appropriate measuring instruments.
Must	The use of the word “must” is deprecated and shall not be used when stating mandatory requirements. The word “must” is used to describe unavoidable situations only.
Operator	The person who initiates and monitors the operation of a computer or process.
Organization	An administrative and functional structure which pursues collective goals, which manages its own performance, and which has a boundary separating it from its environment (as a business, association, or society); also the personnel of such a structure.
Packet	A collection of data created for transmittal across a network. The data includes the data needing transmission along with control data needed to direct the data properly to its destination.
Parity	A simple error detection technique that uses an extra parity bit for blocks of data.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Patch	An update for software created to fix bugs and errors but have become synonymous with fixing security vulnerabilities.
Periodically	An amount of time not to exceed one year.
Physical Security	Measures intended to improve protection by means such as fencing, locks, vehicle barriers, area lighting, surveillance systems, guards, dogs, intrusion detection systems, alarms, access controls, vehicle control and housekeeping.
Physical Security Perimeter	A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.  The physical border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Port	A logical entry or exit point on a computer for connecting communications or peripheral devices.
Potential Impact	The loss of confidentiality, integrity, or availability could be expected to have: 1) a limited adverse effect (FIPS 199 low); 2) a serious adverse effect (FIPS 199 moderate); or 3) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Private Key	A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.
Process Control	Descriptive of systems in which computers or intelligent electronic devices are used



Term	Definition
	for automatic regulation of operations or processes. Typical are operations wherein the control is applied continuously and adjustments to regulate the operation are directed by the computer or device to keep the value of a controlled variable constant. Contrasted with numerical control.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Protocol	A set of rules used by end point devices in a telecommunication connection to facilitate data exchange.
Proxy Server	A server placed between users and the Internet to act as a filter for malicious or unwanted traffic. Proxy servers are stateful and most focus on a single application (HTTP, FTP, etc.) and therefore can detect more malicious activity than a firewall or router.
Public	Information that can be shared with the general public.
Public Key	A cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered Collaborative Signal Processing (CSP).)
Public Key Certificate	A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity.
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke public key certificates.
Recommended	The word "recommended" is used to indicate flexibility of choice with a strong preference for the referenced control.
Record	A group of related facts or fields of information treated as a unit, thus a listing of information, usually in printed or printable form. To put data into a storage device.
Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the control system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Register	High speed storage within a CPU where data or the data's address in RAM resides when being processed. Consider adding definition for a PLC register
Remote Access	Access by users (or control systems) communicating external to a control system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to a control system security perimeter.
Replay	Recording message traffic and "playing it back" to a device later in order to make it do what you want.
Residual Risk	The remaining risks after the security controls have been applied.
Restricted	Information with limited or confined distribution, which is not accessible to the general public or other company employees.

Term	Definition
Risk	<p>A measure combining the severity and likelihood of harm from an event. Alternatively, the likelihood of an adverse outcome:</p> $\text{Risk} = L \times P \times C,$ <p>L is the likelihood of attack depends on the motivation, capabilities and intent of adversaries. P is the probability of success and depends on vulnerabilities present. C is the consequence(s). Risk is also the potential for damage to or loss of an asset.</p>
Risk Assessment	<p>The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.</p>
Risk Management	<p>The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of a control system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.</p>
Role	<p>A set of transactions that a user or set of users can perform within the context of an organization.</p>
Router	<p>A network layer device that sends traffic on the quickest route to reach its destination.</p>
Safeguards	<p>Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a control system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.</p>
Sanitization	<p>Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.</p>
SCADA System	<p>Supervisory Control and Data Acquisition systems are a combination of computer hardware and software used to send commands and acquire data for the purpose of monitoring and controlling.</p>
Secret Key	<p>A cryptographic parameter that is held private by one or more entities to limit the ability to communicate or access that group or entity.</p>
Security	<p>Protection against threats and attacks.</p>
Security Category	<p>The characterization of information or a control system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or control system would have on organizational operations, organizational assets, or individuals.</p>
Security Label	<p>Explicit or implicit marking of a data structure or output media associated with a control system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.</p>
Security Performance	<p>Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, post compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods</p>

<b>Term</b>	<b>Definition</b>
	are required to evaluate security practice performance.
Security Perimeter	See Accreditation Boundary.
Security Plan	A document that describes an operator’s plan to address security issues and related events, such as security assessments and mitigation options, and includes security levels and response measures to security threats.
Security Policies	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions “what” and “why” without dealing with “how.” Policies are normally stated in terms that are technology-independent.
Security Practices	Security practices provide a means of capturing experiences and activities that help ensure system protection and reduce potential manufacturing and control systems compromise. Subject areas include physical security, procedures, organization, design, and programming. Security practices include the actual steps to be taken to ensure system protection.
Security Procedures	Security procedures define exactly how security practices and policies are implemented and executed. They are implemented through personnel training and actions using currently available and installed technology (such as disconnecting modems). Procedures and contained criteria also include more technology-dependent system requirements that need careful analysis, design, planning, and coordinated installation and implementation.
Security Program	A security program brings together all aspects of managing security, ranging from the definition and communication of guidelines through implementation of best industry practices and ongoing operation and auditing.
Security Requirements	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a control system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under (FISMA) and serving as the Chief Information Officer’s primary liaison to the agency’s authorizing officials, control system owners, and information system security officers.
Server	A device or computer system that is dedicated to providing specific facilities to other devices attached to the network.
Server Farm	A cluster of networked servers generally housed in the same location used to perform computationally intense functions by distributing the workload.
Session	Layer 5 of OSI. [ISA definition of OSI: Abbreviation for open system interconnection (a connection between one communication system and another using a standard protocol). OSI reference model, Layer 5 – Session: provides user-to-user connections.]
Shall	Equivalent to “is required to” and used to indicate mandatory requirements strictly to be followed to conform to the standard and from which no deviation is permitted.
Should	Equivalent to “is recommended that,” is used to indicate several possibilities recommended as particularly suitable, without mentioning or excluding other, that a certain course of action is preferred but not required, that (in the negative form) a certain course of action is deprecated but not prohibited.

<b>Term</b>	<b>Definition</b>
Software	A set of programs, procedures, rules, and possibly associated documentation concerned with the operation of a computer system, for example, compilers, library routines, manuals, circuit diagrams.
Spam	Unsolicited and often unwanted email.
Specifications	An assessment object that includes document-related artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with a control system.
Spyware	Software that is secretly or surreptitiously installed into a control system to gather information on individuals or organizations without their knowledge.
Standard	A reference established by authority, custom, or general consent as a model or example. For the purposes of the U.S. Chemicals Sector Cyber security Strategy, a standard is considered a voluntary practice or guideline that is established by consensus of the industry.
Supervisory Control	A term used to imply that a controller output or computer program output is used as an input to other controllers, e.g., generation of setpoints in cascaded control systems. Used to distinguish from direct digital control.
Supervisory Control and Data Acquisition (SCADA)	A computer control system used in real time to monitor and control one or more remote facilities. The system collects data and/or sends control instructions, either automatically or by operators at other locations. SCADA is used to control facilities in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.
Switch	A network device that interconnects devices and creates separate paths for communication.
System	<p>An assembly of procedures, processes, methods, routines, or techniques united by some form of regulated interaction to form an organized whole.</p> <p>An assemblage of equipment, machines, or control devices, interconnected mechanically, hydraulically, pneumatically or electrically, and intended to act together to perform a predetermined function.</p> <p>A combination of generation, transmission, and distribution components.</p>
System Security Plan	Formal document that provides an overview of the security requirements for the control system and describes the security mechanisms in place or planned for meeting those requirements.
System Software	The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.
Technical Measures	The security mechanisms (i.e., safeguards or countermeasures) for a control system that are primarily implemented and executed by the control system through mechanisms contained in the hardware, software, or firmware components of the system.
Third Party	Refers to vendors, support personnel, other companies.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), assets, or individuals through a control system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential

<b>Term</b>	<b>Definition</b>
	for a threat source to successfully exploit control system vulnerabilities.
Threat Source	The intent and method targeted at the intentional exploitation of vulnerabilities or a situation and method that may accidentally trigger a specific vulnerability. Synonymous with term threat agent.
Unauthorized Disclosure	An event involving the exposure of information to entities not authorized access to the information.
User	Individual or (system) process authorized to access a control system.
Utility	A generic term that, when qualified, identifies the business entity including all its operating and business functions; e.g., electric utility, gas utility, water utility, wastewater utility, pipeline utility.  Any general-purpose computer program included in an operating system to perform common functions.  Any of the systems in a process plant, manufacturing facility not directly involved in production; may include any or all of the following – steam, water, refrigeration, heating, compressed air, electric power, instrumentation, waste treatment and effluent systems.
Virtual Private Network	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.
Vulnerability	A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.
Vulnerability Analysis	The identification of the ways in which assailants may attack a facility to cause harm. It can include qualitative risk analysis.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in a control system.

## 5. DOCUMENTS REFERENCED

The following documents were referenced in the preparation of this catalog. It is recognized that many of these are still in draft or do not apply directly to control systems, but still supply information useful for the cyber security of control systems. In addition, several of the NIST Special Publications and some federal documents were referenced for additional guidance.

### **Documents Used in Preparation of the Catalog Recommendations:**

1. American Gas Association, Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (AGA 12, Part 1), March 14, 2006.
2. American Gas Association, Cryptographic Protection of SCADA Communications Part 2: Retrofit link encryption for asynchronous serial communications (AGA 12, Part 2), March 31, 2006.
3. American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.01-2004), Security Technologies for Manufacturing and Control Systems, 11 March 2004.
4. American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.02-2004), Integrating Electronic Security into the Manufacturing and Control Systems Environment, 12 April 2004.
5. American Petroleum Institute, API 1164: Pipeline SCADA Security, First Edition, September, 2004.
6. American Petroleum Institute, Security Guidelines for the Petroleum Industry, April 2005
7. Chemical Industry Data Exchange, Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1, May 2005 (Note: This document has been superseded by Guidance for Addressing Cybersecurity in the Chemical Sector, Version 3.0, Chemical Sector Cyber Security Program, May 2006).
8. Department of Homeland Security, Control System Security Program, Control System Cyber Security Self-Assessment Tool, Beta Release 1.7, December 2006.
9. Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, Issued May 25, 2001, Updated December 03, 2002.
10. International Electrotechnical Commission 62351-1, Data and Communication Security, Committee Draft Version 1, April 2005.
11. International Electrotechnical Commission 62443, Security for Industrial Process Measurement and Control, Draft.
12. International Organization for Standardization 17799, Code of Practice for Information Security Management, June 10, 2005.

13. International Organization for Standardization 27001, Information Security Management Systems Requirements, October 14, 2005.
14. Institute of Electrical and Electronics Engineers 1402, Guide for Electric Power Substation Physical and Electronic Security, January 30, 2000.
15. Instrumentation, Systems, and Automation Society Standards Committee, DRAFT dISA-99.00.01 Manufacturing and Control Systems Security Part 1: Concepts, Models and Terminology Draft 2, Edit 3 October 2005.
16. Instrumentation, Systems, and Automation Society Standards Committee, DRAFT dISA-99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 5 September 20, 2005.
17. National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Revision 1 Final Public Draft, October, 2006.
18. North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-1 through CIP 009-1), May 2006.
19. North American Electric Reliability Council, Security Guidelines for the Electricity Sector, Version 1.0, June 14, 2002.

## Appendix A

# Cross Reference of Standards

The cross reference correlates the requirements contained in the referenced source documents with the recommendations in the Catalog of Control Systems Security. This correlation is meant to depict a general relationship between multiple documents. The cross reference does not imply an exact match between specific requirement details.

The source documents in the cross reference are evolving. New versions may have been released since the cross reference was developed. As a result, the cross reference may not be current. The reader is encouraged to obtain current copies of all pertinent source documents. The versions of the documents used in the cross reference are listed below:

AGA 12-1	<a href="#"><u>Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan, Draft 5, April 14, 2005</u></a>
AGA 12-2	<a href="#"><u>Cryptographic Protection of SCADA Communications Part 2: Retrofit link encryption for asynchronous serial communications, March 31, 2006</u></a>
FIPS 140-2	<a href="#"><u>Security Requirements for Cryptographic Modules, Issued May 25, 2001</u></a>
API 1164	<a href="#"><u>Security Guidelines for the Petroleum Industry</u></a>
CIDX	<a href="#"><u>Guidance for Addressing Cybersecurity , Version 1.0, May 1, 2003</u></a>
ISO 17799	<a href="#"><u>Information technology — Security techniques — Code of practice for information security management, Second edition, 2005-06-15</u></a>
ISO 27001	<a href="#"><u>Information technology — Security techniques — Information security management systems — Requirements, First edition, 2005-10-15</u></a>
IEC 62351	<a href="#"><u>Data and Communications Security – Introduction, Committee Draft (CD) Version 1, April, 2005</u></a>
IEEE 1402	<a href="#"><u>IEEE Guide for Electric Power Substation Physical and Electronic Security, 30 January 2000</u></a>
ISA 99-1	<a href="#"><u>Manufacturing and Control Systems Security, Part 1: Models and Terminology, Draft 1, Edit 8 February 2005</u></a>
ISA99-2	<a href="#"><u>Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program, Draft 1, Edit 1, April 15, 2005</u></a>
NERC Security Guidelines	<a href="#"><u>Security Guidelines for the Electricity Sector, Version: 1.0, May 3, 2005</u></a>



NERC CIP

[Cyber Security, Draft 4: Board Adopted Version, June 1, 2006](#)

NIST SP800-53

[Recommended Security Controls for Federal Information Systems – Information Security, February 2005](#)

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.1.1	Security Policy and Procedures	X	---	X	X	X	X	X	X	---	---	X	X	---	X	X
2.2.1	Management Policy and Procedures	---	---	---	X	---	X	X	X	---	---	X	X	---	X	---
2.2.2	Management Accountability	X	---	---	X	---	X	X	X	---	---	X	X	---	X	---
2.2.3	Baseline Practices	---	---	---	X	---	X	X	X	---	---	X	X	---	---	---
2.2.4	Coordination of Threat Mitigation	---	---	---	X	X	X	X	---	---	---	---	X	---	X	---
2.2.5	Security Policies for Third Parties	---	---	---	X	X	X	X	---	---	---	---	X	---	X	---
2.2.6	Termination of Third-Party Access	---	---	---	X	---	X	X	---	---	---	---	X	---	X	---
2.3.1	Personnel Security Policy and Procedures	---	---	---	X	X	X	X	X	---	---	---	X	X	X	X
2.3.2	Position Categorization	---	---	---	X	X	X	X	---	---	---	---	X	---	X	X
2.3.3	Personnel Screening	X	---	---	X	X	X	X	---	---	---	---	X	X	X	X
2.3.4	Personnel Termination	X	---	---	X	---	X	X	---	---	---	---	X	---	X	X
2.3.5	Personnel Transfer	---	---	---	X	---	---	X	---	---	---	---	X	---	---	X
2.3.6	Access Agreements	---	---	X	X	---	X	X	---	---	---	---	X	X	---	X
2.3.7	Third-Party Personnel Security	---	---	---	X	---	X	X	---	---	---	---	X	---	---	X
2.3.8	Personnel Accountability	---	---	---	X	---	X	X	---	---	---	---	X	---	---	X
2.3.9	Personnel Roles	---	---	---	X	X	X	X	---	---	X	---	X	---	X	---
2.4.1	Physical and Environmental Security Policy and Procedures	X	---	X	X	X	X	X	---	---	X	---	X	---	X	X
2.4.2	Physical Access Authorizations	---	---	X	X	X	X	X	---	---	X	---	X	X	X	X
2.4.3	Physical Access Control	---	---	---	X	X	X	X	---	---	X	---	X	X	X	X
2.4.4	Monitoring Physical Access	---	---	---	X	X	---	X	---	X	X	---	X	X	X	X
2.4.5	Visitor Control	---	---	---	X	X	X	X	---	---	X	---	---	---	X	X
2.4.6	Visitor Records	---	---	---	---	---	X	X	---	---	---	---	---	---	---	X
2.4.7	Physical Access Log Retention	---	---	---	---	---	X	X	---	---	---	---	---	---	X	---
2.4.8	Emergency Shutoff	---	---	---	X	---	X	X	---	---	---	---	---	---	---	X
2.4.9	Emergency Power	---	---	---	---	X	X	X	---	---	---	---	X	---	---	X
2.4.10	Emergency Lighting	---	---	---	---	X	---	X	---	---	---	---	X	---	---	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.4.11	Fire Protection	--	--	--	X	--	X	X	--	--	--	--	X	--	--	X
2.4.12	Temperature and Humidity Controls	--	--	--	--	--	X	X	--	--	--	--	X	--	--	--
2.4.13	Water Damage Protection	--	--	--	X	--	X	X	--	--	--	--	X	--	--	X
2.4.14	Delivery and Removal	--	--	--	--	--	--	X	--	--	--	--	X	--	--	X
2.4.15	Alternate Work Site	--	--	--	--	--	X	--	--	--	--	--	--	X	--	X
2.4.16	Portable Media	X	--	--	--	--	--	X	--	--	--	--	--	--	X	X
2.4.17	Personnel and Asset Tracking	--	--	--	--	--	X	X	--	--	--	--	X	--	--	--
2.4.18	Location of Control System Assets	--	--	--	--	--	X	X	--	--	--	--	X	--	X	X
2.4.19	Information Leakage	--	--	--	X	X	X	X	X	--	--	--	--	X	--	X
2.4.20	Power Equipment and Power Cabling	--	--	--	X	--	X	--	--	--	--	X	--	--	--	X
2.4.21	Physical Device Access Control	X	--	X	--	--	X	--	--	--	--	X	--	--	--	X
2.5.1	System and Services Acquisition Policy and Procedures	--	--	--	--	--	--	X	X	--	--	--	--	--	--	X
2.5.2	Allocation of Resources	X	--	--	--	X	X	X	X	--	--	--	--	--	--	X
2.5.3	Life-Cycle Support	--	--	--	X	X	X	--	--	--	--	--	--	--	--	X
2.5.4	Acquisitions	--	--	X	--	--	--	X	--	--	--	--	--	--	--	X
2.5.5	Control System Documentation	X	--	X	X	--	--	X	X	--	--	--	--	--	--	X
2.5.6	Software License Usage Restrictions	--	--	--	--	X	--	X	--	--	--	--	--	--	--	X
2.5.7	User-Installed Software	X	--	--	X	X	--	X	--	--	--	--	--	--	--	X
2.5.8	Security Engineering Principles	X	--	--	X	X	--	X	X	--	--	--	--	X	--	X
2.5.9	Outsourced Control System Services	--	--	--	X	X	X	X	--	--	--	--	--	--	--	X
2.5.10	Vendor Configuration Management	X	--	X	X	X	X	--	--	--	--	--	--	--	--	X
2.5.11	Vendor Security Testing	--	--	--	X	--	--	X	--	--	--	--	--	--	--	X
2.5.12	Vendor Life Cycle Practices	X	--	X	X	--	--	X	--	--	--	--	--	--	--	--
2.6.1	Configuration Management Policy and Procedures	X	--	X	X	--	X	X	--	--	--	X	X	--	X	X
2.6.2	Baseline Configuration	X	--	X	X	--	--	--	--	--	--	--	--	--	--	X
2.6.3	Configuration Change Control	X	--	X	X	--	X	X	--	--	--	X	X	--	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.6.4	Monitoring Configuration Changes	---	---	---	X	X	---	X	---	---	---	---	X	---	X	X
2.6.5	Access Restrictions for Configuration Change	---	---	---	X	X	---	X	---	---	---	---	X	---	X	X
2.6.6	Configuration Settings	---	---	---	X	X	---	X	---	---	---	---	---	---	X	X
2.6.7	Configuration for Least Functionality	---	---	---	X	---	X	X	---	---	---	---	---	---	X	X
2.6.8	Configuration Assets	---	---	---	X	---	X	X	X	---	---	---	---	---	X	---
2.6.9	Addition, Removal, and Disposal of Equipment	---	---	---	---	---	X	X	---	---	---	---	X	---	X	X
2.6.10	Factory Default Authentication Management	---	---	X	X	---	X	X	---	---	---	---	X	X	---	---
2.7.1	Strategic Planning Policy and Procedures	---	---	---	X	X	X	X	X	---	X	---	X	X	---	X
2.7.2	Control System Security Plan	X	---	---	X	X	X	X	X	---	X	---	X	X	X	X
2.7.3	Interruption Identification and Classification	---	---	---	X	X	X	X	X	---	---	---	X	X	---	X
2.7.4	Roles and Responsibilities	X	---	---	X	X	X	X	X	---	X	---	X	X	X	X
2.7.5	Planning Process Training	X	---	---	X	X	X	X	X	---	---	X	X	X	X	X
2.7.6	Testing	X	---	---	X	X	X	X	X	---	---	---	X	X	X	---
2.7.7	Investigate and Analyze	---	---	---	X	X	X	X	X	---	---	---	X	X	X	---
2.7.8	Corrective Action	---	---	---	X	X	X	X	X	---	---	---	X	X	X	X
2.7.9	Risk Mitigation	---	---	---	X	X	X	X	X	---	---	---	X	---	X	X
2.7.10	System Security Plan Update	X	---	---	X	X	X	X	X	---	---	---	X	---	X	X
2.7.11	Rules of Behavior	---	---	X	X	X	X	X	---	---	---	---	X	---	---	X
2.7.12	Security-Related Activity Planning	---	---	---	---	---	---	X	---	---	---	---	---	X	X	X
2.8.1	System and Communication Protection Policy and Procedures	X	---	X	---	X	---	X	---	---	---	---	X	---	---	X
2.8.2	Management Port Partitioning	X	---	---	X	---	---	X	---	---	---	---	---	---	---	X
2.8.3	Security Function Isolation	---	---	X	X	---	---	X	---	---	---	---	---	---	---	X
2.8.4	Information Remnants	---	---	---	X	X	---	X	---	---	---	---	---	---	---	X
2.8.5	Denial-of-Service Protection	---	X	---	X	X	X	---	---	X	---	---	X	X	---	X
2.8.6	Resource Priority	X	---	---	X	X	---	X	---	---	---	---	X	---	---	X
2.8.7	Boundary Protection	---	---	---	X	X	X	X	---	---	---	---	X	---	---	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.8.8	Communication Integrity	X	---	---	X	X	X	X	---	---	---	---	---	---	---	X
2.8.9	Communication Confidentiality	X	---	X	X	X	X	X	---	---	---	---	X	---	---	X
2.8.10	Trusted Path	X	---	X	X	---	---	X	---	---	---	---	---	---	---	X
2.8.11	Cryptographic Key Establishment and Management	X	---	X	X	---	X	X	---	---	---	---	---	X	---	X
2.8.12	Use of Validated Cryptography	X	---	X	X	---	X	X	---	---	---	---	---	X	---	X
2.8.13	Collaborative Computing	---	---	---	X	---	---	---	---	---	---	---	---	---	---	X
2.8.14	Transmission of Security Parameters	X	---	---	---	---	---	X	---	---	---	---	---	---	---	X
2.8.15	Public Key Infrastructure Certificates	X	---	---	---	---	---	X	---	---	---	---	---	---	---	X
2.8.16	Mobile Code	---	---	---	---	---	---	X	---	---	---	---	---	---	---	X
2.8.17	Voice-Over Internet Protocol	---	---	---	---	---	---	---	---	---	---	---	---	---	---	X
2.8.18	System Connections	X	---	---	X	X	X	X	---	---	---	---	X	---	X	X
2.8.19	Security Roles	X	---	---	X	X	X	X	---	---	---	---	X	---	X	X
2.8.20	Message Authenticity	X	---	---	---	---	---	X	X	X	---	X	---	X	---	X
2.8.21	Architecture and Provisioning for Name/Address Resolution Service	---	---	---	---	---	---	---	---	---	---	---	---	X	---	X
2.8.22	Secure Name / Address Resolution Service (Authoritative Source)	---	---	---	---	---	---	---	---	---	---	---	---	---	---	X
2.8.23	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	---	---	---	---	---	---	---	---	---	---	---	---	---	---	X
2.9.1	Information and Document Management Policy and Procedures	---	---	---	X	X	X	X	---	---	---	---	X	X	X	---
2.9.2	Information and Document Retention	X	---	---	X	X	X	X	---	---	---	---	X	---	X	---
2.9.3	Information Handling	X	---	---	X	---	X	X	X	---	---	---	X	---	X	X
2.9.4	Information Classification	X	---	X	X	X	X	X	---	---	---	---	X	---	---	X
2.9.5	Information Exchange	X	---	---	X	---	X	X	---	---	---	---	X	---	---	---
2.9.6	Information and Document Classification	X	---	X	X	---	X	X	---	---	---	---	X	---	X	---
2.9.7	Information and Document Retrieval	X	---	---	X	X	---	X	X	---	---	---	X	---	---	---
2.9.8	Information and Document Destruction	X	---	---	X	---	X	X	X	---	---	---	X	---	---	---

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.9.9	Information and Document Management Review	X	---	---	---	X	X	X	---	---	---	---	X	---	---	---
2.9.10	Automated Marking	---	---	---	---	---	---	---	---	---	---	---	---	---	---	X
2.9.11	Automated Labeling	---	---	---	---	X	---	---	---	---	---	---	---	---	---	X
2.10.1	System Maintenance Policy and Procedures	X	---	X	---	---	X	X	X	---	X	---	X	---	X	X
2.10.2	Legacy System Upgrades	X	---	---	X	---	---	---	---	---	---	---	X	---	X	---
2.10.3	System Monitoring and Evaluation	X	---	---	X	X	X	X	---	---	---	X	X	---	X	X
2.10.4	Backup and Recovery	X	---	X	X	X	X	X	---	---	---	X	X	---	X	X
2.10.5	Unplanned System Maintenance	X	---	X	X	---	X	X	---	---	---	X	X	---	X	X
2.10.6	Periodic System Maintenance	X	---	X	---	---	---	X	---	---	---	---	X	---	---	X
2.10.7	Maintenance Tools	X	---	X	---	---	---	X	---	---	---	---	---	---	---	X
2.10.8	Maintenance Personnel	---	---	---	X	---	---	X	---	---	---	---	---	---	---	X
2.10.9	Remote Maintenance	---	---	---	---	---	---	X	---	---	---	X	---	X	---	X
2.10.10	Timely Maintenance	---	---	X	---	---	X	X	---	---	---	---	---	---	X	X
2.11.1	Security Awareness and Training Policy and Procedures	---	---	X	X	X	X	X	---	X	---	X	X	X	X	X
2.11.2	Security Awareness	X	---	X	X	X	X	X	---	X	---	X	X	X	X	X
2.11.3	Security Training	---	---	---	X	X	X	X	---	X	---	X	X	X	X	X
2.11.4	Security Training Records	---	---	---	X	X	X	---	X	---	---	---	X	---	X	X
2.11.5	Contact with Security Groups and Associations	X	---	---	---	X	X	X	---	---	---	---	---	---	---	X
2.11.6	Security Responsibility Testing	---	---	---	---	X	X	---	X	---	---	---	X	X	---	---
2.12.1	Incident Response Policy and Procedures	X	---	---	X	X	X	X	---	X	---	X	X	X	X	X
2.12.2	Continuity of Operations Plan	X	---	---	X	X	X	X	---	---	---	---	X	X	X	X
2.12.3	Continuity of Operations Roles and Responsibilities	---	---	X	X	X	X	X	---	---	---	---	X	X	X	X
2.12.4	Incident Response Training	---	---	---	X	X	X	X	---	---	---	---	X	X	X	X
2.12.5	Continuity of Operations Plan Testing	---	---	---	X	X	X	X	---	---	---	---	X	X	X	X
2.12.6	Continuity of Operations Plan Update	---	---	---	X	X	X	X	---	---	---	---	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.12.7	Incident Handling	--	--	--	X	X	X	X	X	--	--	--	X	X	X	X
2.12.8	Incident Monitoring	--	--	--	X	X	X	X	X	--	--	--	--	X	X	X
2.12.9	Incident Reporting	--	--	--	X	X	X	X	--	--	--	--	X	X	X	X
2.12.10	Incident Response Assistance	--	--	--	X	X	X	X	--	--	--	--	--	X	X	X
2.12.11	Incident Response Investigation and Analysis	--	--	--	X	X	X	X	X	--	--	--	X	X	X	X
2.12.12	Corrective Action	X	--	--	X	X	X	X	X	--	--	--	X	--	X	X
2.12.13	Alternate Storage Sites	--	--	--	X	--	X	X	--	--	--	--	X	--	X	X
2.12.14	Alternate Command/Control Methods	--	--	--	X	X	X	X	--	--	X	--	X	X	--	X
2.12.15	Alternate Control Center	X	--	--	X	X	X	X	--	--	--	--	X	--	--	X
2.12.16	Control System Backup	--	--	--	X	X	X	--	--	--	--	--	X	--	X	X
2.12.17	Control System Recovery and Reconstitution	--	--	--	X	X	X	X	--	--	--	--	X	--	X	X
2.12.18	Fail-Safe Response	--	--	--	X	--	--	--	--	--	--	--	--	--	--	--
2.13.1	Media Protection Policy and Procedures	X	--	--	--	--	--	--	X	--	--	--	--	X	--	X
2.13.2	Media Access	--	--	--	X	--	X	X	X	--	--	--	--	--	X	X
2.13.3	Media Classification	--	--	--	X	X	X	X	X	--	--	--	--	--	X	X
2.13.4	Media Labeling	--	--	--	X	--	--	X	--	--	--	--	--	--	--	X
2.13.5	Media Storage	--	--	--	X	--	X	X	X	--	--	--	--	--	--	X
2.13.6	Media Transport	--	--	--	--	--	--	X	X	--	--	--	--	--	--	X
2.13.7	Media Sanitization and Disposal	X	--	--	X	--	X	X	X	--	--	--	--	--	X	X
2.14.1	System and Information Integrity Policy and Procedures	--	--	--	--	X	X	--	X	--	--	--	--	X	--	X
2.14.2	Flaw Remediation	--	--	--	X	X	X	X	X	--	--	--	--	--	X	X
2.14.3	Malicious Code Protection	X	--	--	X	X	X	X	--	--	--	--	--	X	X	X
2.14.4	System Monitoring Tools and Techniques	X	--	--	X	--	X	X	--	--	--	--	--	X	X	X
2.14.5	Security Alerts and Advisories	X	--	--	--	X	X	X	--	--	--	--	--	X	X	X
2.14.6	Security Functionality Verification	--	X	X	--	--	X	X	--	--	--	--	--	--	--	X
2.14.7	Software and Information Integrity	--	X	X	--	--	--	X	--	--	--	--	--	--	--	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.14.8	Spam Protection	--	--	--	--	X	--	X	--	--	--	--	--	--	X	X
2.14.9	Information Input Restrictions	--	--	--	X	X	--	X	--	--	--	--	--	--	--	X
2.14.10	Information Input Accuracy, Completeness, Validity, and Authenticity	--	--	--	X	--	--	X	--	--	--	--	--	--	--	X
2.14.11	Error Handling	--	X	--	X	--	--	X	--	--	--	--	--	--	--	X
2.14.12	Information Output Handling and Retention	--	--	--	X	X	X	X	X	--	--	--	--	--	--	X
2.15.1	Access Control Policy and Procedures	X	--	X	X	X	X	X	X	--	X	--	X	X	--	X
2.15.2	Identification and Authentication Policy and Procedures	X	X	X	X	X	X	X	X	--	X	--	X	X	--	X
2.15.3	Account Management	X	--	--	X	X	X	X	--	--	--	--	X	X	X	X
2.15.4	Identifier Management	X	--	X	X	X	X	X	--	--	--	--	X	--	X	X
2.15.5	Authenticator Management	--	--	X	--	--	X	X	--	--	--	--	X	X	X	X
2.15.6	Supervision and Review	X	--	X	X	--	X	X	X	--	--	--	X	--	X	X
2.15.7	Access Enforcement	X	--	--	X	--	X	X	--	--	--	--	X	--	X	X
2.15.8	Separation of Duties	X	--	X	X	X	X	X	--	--	--	--	X	--	--	X
2.15.9	Least Privilege	X	--	--	X	--	X	X	--	--	--	--	X	--	--	X
2.15.10	User Identification and Authentication	X	--	--	X	X	X	X	--	--	--	--	X	X	--	X
2.15.11	Permitted Actions Without Identification or Authentication	--	--	--	--	--	--	X	--	--	--	--	--	--	--	X
2.15.12	Device Identification and Authentication	--	--	--	--	--	--	X	--	--	--	--	X	--	--	X
2.15.13	Authenticator Feedback	--	--	X	--	--	--	X	--	--	--	--	--	--	--	X
2.15.14	Cryptographic Module Authentication	X	--	X	--	--	--	X	--	--	--	--	--	--	--	X
2.15.15	Information Flow Enforcement	--	--	X	--	--	--	X	--	--	--	--	--	X	X	X
2.15.16	Passwords	X	--	X	X	--	X	X	--	--	--	--	X	X	X	X
2.15.17	System Use Notification	--	--	--	X	X	--	X	--	--	--	--	--	--	X	X
2.15.18	Requirement Enhancement: None. Concurrent Session Control	X	--	--	--	--	--	X	--	--	--	--	--	--	--	X



		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.15.19	Previous Logon Notification	--	--	--	--	--	--	X	--	--	--	--	--	--	--	X
2.15.20	Unsuccessful Login Attempts	--	--	--	X	--	--	X	--	--	--	--	X	X	--	X
2.15.21	Session Lock	--	--	--	--	--	--	X	--	--	--	--	--	--	--	X
2.15.22	Remote Session Termination	X	--	--	X	--	--	X	--	--	--	--	--	--	--	X
2.15.23	Remote Access Policy and Procedures	X	--	--	--	X	--	X	--	--	--	--	X	X	X	X
2.15.24	Remote Access	X	--	--	X	X	X	X	--	--	--	--	X	X	--	X
2.15.25	Access Control for Portable and Mobile Devices	--	--	--	--	--	--	X	--	--	--	--	X	--	--	X
2.15.26	Wireless Access Restrictions	X	--	--	X	X	X	X	--	--	--	--	--	--	--	X
2.15.27	Personally Owned Information	--	--	--	X	--	--	--	--	--	--	--	--	--	--	X
2.15.28	External Access Protections	--	--	--	X	X	--	X	--	--	--	--	--	--	--	X
2.15.29	Use of External Information Control Systems	X	X	--	X	X	X	--	--	--	--	--	X	--	--	X
2.16.1	Audit and Accountability Policy and Procedures	X	--	X	X	X	X	X	X	--	X	--	X	X	X	X
2.16.2	Auditable Events	X	--	X	X	--	--	X	--	--	--	--	--	--	X	X
2.16.3	Content of Audit Records	X	--	X	X	--	--	X	--	--	--	--	--	--	--	X
2.16.4	Audit Storage Capacity	--	--	--	--	--	--	X	--	--	--	--	--	--	--	X
2.16.5	Response to Audit Processing Failures	--	--	--	--	--	--	X	--	--	--	--	--	--	--	X
2.16.6	Audit Monitoring, Analysis, and Reporting	X	--	X	X	X	X	X	X	--	--	--	--	--	X	X
2.16.7	Audit Reduction and Report Generation	X	--	X	X	X	--	X	X	--	--	--	--	--	--	X
2.16.8	Time Stamps	--	--	--	X	--	--	X	--	--	--	--	--	--	--	X
2.16.9	Protection of Audit Information	X	--	--	X	--	--	X	X	--	--	--	--	--	X	X
2.16.10	Audit Record Retention	X	--	--	X	X	--	X	X	--	--	--	--	--	X	X
2.16.11	Conduct and Frequency of Audits	X	--	--	X	X	X	X	X	--	--	--	X	--	X	X
2.16.12	Auditor Qualification	--	--	--	--	--	X	--	--	--	--	--	X	--	--	X
2.16.13	Audit Tools	X	--	--	--	--	--	X	--	--	--	--	X	--	--	X
2.16.14	Security Policy Compliance	--	--	--	--	X	X	X	X	--	--	--	--	--	X	--
2.17.1	Monitoring and Reviewing Control System Security Management Policy and Procedures	--	--	--	X	X	X	X	X	--	--	--	X	X	X	X

		AGA12-1	AGA12-2	FIPS 140-2	API 1164	Security Guidelines for the Petroleum Industry	CIDX	ISO 17799	ISO 27001	IEC 62351	IEEE 1402	ISA99-1	ISA99-2	NERC Security Guidelines	NERC CIP	NIST SP800-53
2.17.2	Continuous Improvement	--	--	--	X	X	X	X	X	--	--	X	X	--	X	X
2.17.3	Monitoring of Security Policy	--	--	--	X	X	X	--	X	--	--	--	X	--	X	X
2.17.4	Best Practices	--	--	--	X	X	X	--	X	--	--	--	X	--	--	X
2.17.5	Security Accreditation	X	--	--	X	--	--	--	--	--	--	--	--	--	--	X
2.17.6	Security Certification	X	--	--	X	X	X	--	X	--	--	--	--	--	--	X
2.18.1	Risk Assessment Policy and Procedures	X	--	--	X	X	X	X	X	--	X	X	X	X	X	X
2.18.2	Risk Management Plan	X	--	--	X	X	X	X	X	--	X	--	X	X	X	X
2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures	X	--	--	--	--	--	X	--	--	X	--	X	X	--	X
2.18.4	Security Assessments	--	--	--	X	X	X	X	X	--	--	--	X	--	--	X
2.18.5	Control System Connections	--	--	--	X	X	X	X	--	--	--	--	--	--	X	X
2.18.6	Plan of Action and Milestones	--	--	--	X	X	--	--	X	--	--	--	X	--	X	X
2.18.7	Continuous Monitoring	--	--	--	X	X	X	X	X	--	--	--	X	--	X	X
2.18.8	Security Categorization	--	--	--	X	--	X	X	--	--	--	--	X	--	--	X
2.18.9	Risk Assessment	--	--	--	X	X	X	X	X	--	X	X	X	X	X	X
2.18.10	Risk Assessment Update	--	--	--	X	X	X	X	X	--	--	--	X	--	X	X
2.18.11	Vulnerability Assessment and Awareness	--	--	--	X	--	X	X	--	--	--	--	X	X	X	X
2.18.12	Identify, Classify, Prioritize, and Analyze Potential Security Risks	--	--	--	X	X	X	X	X	--	--	--	X	--	X	--