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 and updates:

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

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

2.11.1.4 References

NIST SP 800-53r3	AT-1
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 A, B, C, D
NRC RG 5.71	C.3.3.2.8, App. C.10.1, App. C.10.2, App. C.10.4, App. C.10.6

2.11.2 Security Awareness

2.11.2.1 Requirement

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

2.11.2.2 Supplemental Guidance

The organization determines the content of security awareness training and security awareness techniques based on the specific requirements of the organization and the systems to which personnel have authorized access. Security awareness techniques can include displaying posters, offering security-messaged items, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting security awareness events. The security awareness training program is consistent with the requirements contained in CFR Part 5 Subpart C (5 CFR 930.301).

2.11.2.3 Requirement Enhancements

1. All control system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training.
2. The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

2.11.2.4 References

NIST SP 800-53r3	AT-2
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 A, B.R1
NRC RG 5.71	App. C.10.1

2.11.3 Security Training

2.11.3.1 Requirement

The organization:

1. Defines and documents system security roles and responsibilities throughout the system development life cycle
2. Identifies individuals having system security roles and responsibilities
3. Provides security-related technical training: (a) before authorizing access to the system or performing assigned duties, (b) when required by system changes, and (c) on an organization-defined frequency, thereafter.

2.11.3.2 Supplemental Guidance

The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, security-related technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in CFR Part 5 Subpart C (5 CFR 930.301).

2.11.3.3 Requirement Enhancements

None

2.11.3.4 References

NIST SP 800-53r3	AT-3
CAG	CC-20
API 1164r2	1.2, 3.1, Annex A, Annex B
NERC CIPS	CIP 004-3 B.R2
NRC RG 5.71	C.3.3.2.8, App. C.10.2, App. C.10.4, App. C.10.6

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

2.11.4.4 References

NIST SP 800-53r3	AT-4
API 1164r2	3.1
NERC CIPS	CIP 004-3 B.R2.3
NRC RG 5.71	App. C.10.8

2.11.5 Contact with Security Groups and Associations

2.11.5.1 Requirement

The organization establishes and maintains contact with security groups and associations to stay up-to-date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

2.11.5.2 Supplemental Guidance

Security groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to systems are consistent with applicable laws, directives, policies, regulations, standards, and guidance.

2.11.5.3 Requirement Enhancements

None

2.11.5.4 References

NIST SP 800-53r3	AT-5
API 1164r2	3.4
NERC CIPS	CIP 008-3 B.R1.3
NRC RG 5.71	App. C.10.9

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 must be notified when their testing is scheduled, informed as to how it will be conducted, and notified of the 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

2.11.6.4 References

NIST SP 800-53r3	MA-6
API 1164r2	3.5
NRC RG 5.71	App. C.3.6, App. C.12.5, App. C.12.6, App. C.13.1

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 manmade events like 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 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 and updates:

1. A formal, documented, incident response 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 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. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular system, when required.

2.12.1.3 Requirement Enhancements

None

2.12.1.4 References

NIST SP 800-53r3	IR-1
CAG	CC-18
API 1164r2	3.5
NERC CIPS	CIP 008-3
NRC RG 5.71	App. C.8.1

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

1. The continuity of operations plan delineates that at the time of the disruption to normal system operations, the organization executes its incident response policies and procedures to place the system in a safe configuration and initiates the necessary notifications to regulatory authorities.
2. The organization initiates a root cause analysis for the event and submits any findings from the analysis to the organizations corrective action program.
3. The organization then resumes normal operation of the system in accordance with its policies and procedures.

2.12.2.4 References

NIST SP 800-53r3	CP-2
API 1164r2	3.4, Annex A
NERC CIPS	CIP 003-3 B.R4.1, CIP 009-3
NRC RG 5.71	App. C.9.2

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

2.12.3.4 References

NIST SP 800-53r3	CP-3
API 1164r2	3.5
NERC CIPS	CIP 009-3 B.R1.2
NRC RG 5.71	App. C.9.4

2.12.4 Incident Response Training

2.12.4.1 Requirement

The organization:

1. Trains personnel in their incident response roles and responsibilities with respect to the system
2. Provides refresher training on an organization-defined frequency, at least annually.

2.12.4.2 Supplemental Guidance

Training needs to be provided to individuals in the control system community so that all 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.

2.12.4.4 References

NIST SP 800-53r3	IR-2
CAG	CC-18
API 1164r2	3.5, Annex A, Annex B.5.1.2.4
NERC CIPS	CIP 008-3 B.R1.6
NRC RG 5.71	App. C.8.2

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. Several methods for testing and/or exercising continuity of operations plans exist for identifying potential weaknesses

(e.g., full-scale business continuity plan testing, functional/tabletop exercises). 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

1. The organization coordinates continuity of operations plan testing and exercises with organizational elements responsible for related plans.
2. The organization tests and 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.
3. The organization employs automated mechanisms to thoroughly and effectively test and 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.

2.12.5.4 References

NIST SP 800-53r3	CP-4, IR-3
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3 B.R1.6
NRC RG 5.71	App. C.9.3, App. C.9.7

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

2.12.6.4 References

NIST SP 800-53r3	CP-2
API 1164r2	3.4, Annex A
NRC RG 5.71	App. C.9.3, App. C.9.7

2.12.7 Incident Handling

2.12.7.1 Requirement

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
2. Coordinates incident handling activities with contingency planning activities

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

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.

2.12.7.4 References

NIST SP 800-53r3	IR-4
CAG	CC-16, CC-18
API 1164r2	3.5, Annex A, Annex B.2.1.3.5
NERC CIPS	CIP 008-3 B.R1.2
NRC RG 5.71	App. C.8.4

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

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.

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.

2.12.8.4 References

NIST SP 800-53r3	IR-5
CAG	CC-18
API 1164r2	3.5, Annex B.2.1.3.5
NERC CIPS	CIP 008-3 B.R1.2
NRC RG 5.71	App. C.8.5

2.12.9 Incident Reporting

2.12.9.1 Requirement

The organization promptly reports cyber and system security incident information to designated 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, 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. Current federal policy requires that organizational officials report security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within specified timeframes designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. The US-CERT phone number is 1-888-282-0870.

A sister organization, the Industrial Control System Computer Emergency Response Team (ICS-CERT) at http://www.us-cert.gov/control_systems/ics-cert/ provides free assistance specifically for ICS issues. This is a manned 24-hour center designed to receive and transmit ICS Alerts, pertaining to potential adverse cyber effects (malware and 0-day infections). It is equipped with trained specialists to assist ICS users in determining whether they are experiencing a system upset or potential malware infection effects. The phone number for this watch floor is 1-877-776-7585.

2.12.9.3 Requirement Enhancements

The organization employs automated mechanisms to assist in the reporting of security incidents. The Einstein network monitoring device from DHS is an example of an automated mechanism.

2.12.9.4 References

NIST SP 800-53r3	IR-6
CAG	CC-18
API 1164r2	3.5
NERC CIPS	CIP 008-3 B.R1.3
NRC RG 5.71	App. C.8.5

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.

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 manipulate manually control system functions if necessary.

The ICS-CERT at http://www.us-cert.gov/control_systems/ics-cert/ provides free assistance specifically for ICS issues. This is a manned 24-hour center designed to receive and transmit ICS Alerts, pertaining to potential adverse cyber effects (malware and 0-day infections). It is equipped with trained specialists to assist ICS users in determining whether they are experiencing a system upset or potential

malware infection effects. This assistance can be in the form of support for incident response and forensic analysis. The phone number for this watch floor is 1-877-776-7585.

2.12.10.3 Requirement Enhancements

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

   Enhanced Supplemental Guidance—Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to websites to query the assistance capability, or the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

2. The organization:

   a. Establishes a direct, coorperative relationship between its incident response capability and external providers of information system protection capability

   Identifies organizational incident response team members to the external providers.

   Enhanced Supplemental Guidance—External providers of information system protection capability include the Computer Network Defense program within the US Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

2.12.10.4 References

NIST SP 800-53r3 IR-7

NRC RG 5.71 App. C.8.7

2.12.11 Incident Response Plan

2.12.11.1 Requirement

The organization:

1. Develops an incident response plan that
   a. Provides the organization with a roadmap for implementing its incident response capability
   b. Describes the structure and organization of the incident response capability
   c. Provides a high-level approach for how the incident response capability fits into the overall organization
   d. Meets the unique requirements of the organization with respect to mission, function, size, and structure
   e. Defines reportable incidents
   f. Provides metrics for measuring the incident response capability within the organization
2. Distributes copies of the incident response plan to identified active incident response personnel
2. Reviews the incident response plan on a periodic frequency for relevance, changes to configuration and processes and the result of incident plan test exercises
3. Revises the incident response plan to address system/organizational/operational changes or problems encountered during plan implementation, execution, or testing
4. Communicates incident response plan changes to identified active incident response personnel.

2.12.11.2 Supplemental Guidance

The organization should have a formal, focused, and coordinated approach to responding to incidents. The time to develop an incident response investigation and analysis plans, either internally or externally, is not during such incidents, but beforehand, where calm, calculated actions and responses can be developed and tested for effectiveness. These investigations should consider incidents based on the potential outcome as well as the actual outcome, recognizing that the cyber incident may include intentional and unintentional incidents. Immediate response that is not well thought-out has the potential to be more harmful than no alternative action.

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.

2.12.11.4 References

NIST SP 800-53r3	IR-8
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3
NRC RG 5.71	App. C.8.8

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 cybersecurity incident are fully implemented.

2.12.12.2 Supplemental Guidance

The organization reviews investigation results and determines 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

2.12.12.4 References

NIST SP 800-53r3	CP-4, IR-4
API 1164r2	3.5, Annex A
NERC CIPS	CIP 008-3 C, M1
NRC RG 5.71	C2, App. C.3.2, App. C.3.9, App. C.3.11, App. C.8.1, App. C.13.3

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

1. The organization identifies potential accessibility problems at the alternative storage site in the event of an areawide disruption or disaster and outlines explicit mitigation actions.
2. 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.
3. The organization configures the alternate storage site to facilitate timely and effective recovery operations.

2.12.13.4 References

NIST SP 800-53r3	CP-6
API 1164r2	3.4, Annex A, Annex B.2.1.3.5
NRC RG 5.71	App. B.1.22

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. Timeframes 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.

2.12.14.4 References

NIST SP 800-53r3	CP-4, CP-8
API 1164r2	3.4, Annex A, Annex B.2.1.3.5
NRC RG 5.71	C.3.3, App. B.1.22, App. B.4.5

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

2.12.15.4 References

NIST SP 800-53r3	CP-7
API 1164r2	3.4, Annex A
NERC CIPS	CIP 002-3 B.R1.2.1, CIP 002-3 R3
NRC RG 5.71	App. B.1.22

2.12.16 Control System Backup

2.12.16.1 Requirement

The organization:

1. Conducts backups of user-level information contained in the system on an organization-defined frequency
2. Conducts backups of system-level information (including system state information) contained in the system on an organization-defined frequency
3. Protects the confidentiality and integrity of backup information at the storage location.

2.12.16.2 Supplemental Guidance

The frequency of system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the recovery time and recovery point objectives for the organization. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of system backups. Protecting backup information from unauthorized disclosure also is an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use

of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control.

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.

2.12.16.4 References

NIST SP 800-53r3	CP-9
CAG	CC-19
API 1164r2	3.4, Annex A, Annex B.3.1.1.1
NERC CIPS	CIP 008-3 B.R4
NRC RG 5.71	App. C.8.1, App. C.9.5, App. C.9.6

2.12.17 Control System Recovery and Reconstitution

2.12.17.1 Requirement

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

2.12.17.2 Supplemental Guidance

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. The recovery and reconstitution capability employed by the organization can be a combination of automated mechanisms and manual procedures.

2.12.17.3 Requirement Enhancements

1. The organization implements transaction recovery for systems that are transaction-based (e.g., database management systems).
2. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state.
3. The organization provides the capability to re-image system components in accordance with organization defined restoration time periods from configuration controlled and integrity protected disk images representing a secure, operational state for the components.

2.12.17.4 References

NIST SP 800-53r3	CP-10
CAG	CC-19
API 1164r2	3.4, Annex A

NERC CIPS	CIP 009-3 B.R1 through R5
NRC RG 5.71	App. C.9.3, App. C.9.7

2.12.18 Fail-Safe Response

2.12.18.1 Requirement

The system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with the 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 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 shut down 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). The organization then defines the appropriate fail-safe process for its industry.

2.12.18.3 Requirement Enhancements

The system preserves the organization-defined system state information in failure.

2.12.18.4 References

API 1164r2	8.1

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 (IP) 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 allowed.

2.13.1 Media Protection Policy and Procedures

2.13.1.1 Requirement

The organization develops, disseminates, and periodically reviews and 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

2.13.1.4 References

NIST SP 800-53r3	MP-1
API 1164r2	Annex A
NERC CIPS	CIP 003-3 B.R4, CIP 009-3 B.R5, CIP 007-3 B.R7
NRC RG 5.71	App. B.3.1

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.

System media include both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, and DVDs) and nondigital media (e.g., paper, microfilm). This requirement also applies to portable and mobile computing and communications device 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

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

2.13.2.4 References

NIST SP 800-53r3	MP-2
CAG	CC-15
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R7
NRC RG 5.71	App. C.1.2

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

2.13.3.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	6, Annex A
NERC CIPS	CIP 003-3 B.R4.2
NRC RG 5.71	App. B.1.13, App. C.1.3

2.13.4 Media Marking

2.13.4.1 Requirement

The organization:

1. Marks, in accordance with organizational policies and procedures, removable system media and system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information
2. Exempts an organization-defined list of media types or hardware components from marking as long as the exempted items remain within the organization-defined protected environment.

2.13.4.2 Supplemental Guidance

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

2.13.4.3 Requirement Enhancements

The system marks output on external media including video display devices, to identify any of the organization-identified set of special dissemination, handling, or distribution instructions that apply to system output using organization-identified human readable, standard naming conventions. Note: System markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the system). External markings are distinguished from internal markings (i.e., the labels used

on internal data structures within the system). Video display devices include computer terminals, monitors, screens on notebook computers, and personal digital assistants.

2.13.4.4 References

NIST SP 800-53r3	MP-3
CAG	CC-9
API 1164r2	Annex A
NRC RG 5.71	App. B.1.13, App. C.1.3

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 are stored.

2.13.5.2 Supplemental Guidance

System media include both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) and nondigital media (e.g., paper, microfilm). This control applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered systems and may have the capability to store information on internal media (e.g., on voicemail systems). Because telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any 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 system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, the physical access controls to the facility where the media reside provide adequate protection. The organization protects system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

2.13.5.3 Requirement Enhancements

None

2.13.5.4 References

NIST SP 800-53r3	MP-4
CAG	CC-15

API 1164r2	Annex A
NERC CIPS	CIP 009-3 B.R4
NRC RG 5.71	App. C.1.4

2.13.6 Media Transport

2.13.6.1 Requirement

The organization:

1. Protects organization-defined types of digital and nondigital media during transport outside controlled areas using organization-defined security measures
2. Maintains accountability for system media during transport outside controlled areas
3 Restricts the activities associated with transport of such media to authorized personnel.

2.13.6.2 Supplemental Guidance

System media include both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, CDs, DVDs) and nondigital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside controlled areas. Telephone systems also are considered systems and may have the capability to store information on internal media (e.g., on voicemail systems). Because telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other systems, organizational personnel exercise caution in the types of information stored on telephone voicemail systems that are transported outside controlled areas. A controlled area is any 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 system.

Physical and technical security measures for the protection of digital and nondigital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and nondigital media during transport. Cryptographic mechanisms can provide confidentiality and integrity protections depending on the mechanisms used. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of storage containers for transporting nondigital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

2.13.6.3 Requirement Enhancements

1. The organization documents activities associated with the transport of system media using organization-defined system of records. Note: Organizations establish documentation requirements for activities associated with the transport of system media in accordance with the organizational assessment of risk.
2. The organization employs an identified custodian throughout the transport of system media. Note: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

3. In situations where the ICS cannot support cryptographic mechanisms, the organization employs compensating controls.

2.13.6.4 References

NIST SP 800-53r3	MP-5
NRC RG 5.71	App. C.1.5

2.13.7 Media Sanitization and Disposal

2.13.7.1 Requirement

The organization sanitizes system digital and nondigital media, before disposal or release for reuse.

2.13.7.2 Supplemental Guidance

This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from system media such that reasonable assurance exists, 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, prevent the disclosure of organizational information to unauthorized individuals when such media are reused or disposed of. The organization employs sanitization mechanisms with strength and integrity commensurate with the security category of the information. FIPS 199 provides standards and guidance on security categories of information and systems. The organization uses its discretion on the use of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

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.

2.13.7.4 References

NIST SP 800-53r3	MP-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R7
NRC RG 5.71	App. C.1.6

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 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, controls within this family 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 and 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

2.14.1.4 References

NIST SP 800-53r3	SI-1
NERC CIPS	CIP 007-3 A, B, C, D
NRC RG 5.71	App. C.3.1

2.14.2 Flaw Remediation

2.14.2.1 Requirement

The organization:

1. Identifies, reports, and corrects system flaws
2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational systems before installation
3. Incorporates flaw remediation into the organizational configuration management process as an emergency change.

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 either in 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 organization employs automated mechanisms to determine periodically and on demand the state of system components with regard to flaw remediation.
3. The organization measures the time between flaw identification and flaw remediation, comparing with organization-defined benchmarks.
4. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined system components.
5. The use of automated flaw remediation processes must not degrade the operational performance of the control system.

2.14.2.4 References

NIST SP 800-53r3	SI-2
API 1164r2	3.7, 7.2, Annex B.3
NERC CIPS	CIP 007-3 B.R1
NRC RG 5.71	App. C.3.2

2.14.3 Malicious Code Protection

2.14.3.1 Requirement

The organization:

1. Employs malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: (a) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or (b) inserted through the exploitation of system vulnerabilities
2. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures
3. Configures malicious code protection mechanisms to: (a) perform periodic scans of the system on an organization-defined frequency and real-time scans of files from external sources as the files are downloaded, opened, or executed and (b) disinfect and quarantine infected files
4. Considers using malicious code protection software products from multiple vendors as part of defense-in-depth
5. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

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., VoIP, Instant Messaging, file transfer protocol, HTTP, electronic mail, file sharing).

2.14.3.3 Requirement Enhancements

1. The organization centrally manages malicious code protection mechanisms.
2. The system automatically updates malicious code protection mechanisms (including signature definitions).
3. The system prevents users from circumventing host-based malicious code protection capabilities.
4. The system updates malicious code protection mechanisms only when directed by a privileged user.
5. The organization does not allow users to introduce removable media into the system.
6. The system implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly (i.e., block, quarantine, send alert to administrator) when the system encounters data not explicitly allowed by the security policy.
7. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the system.

2.14.3.4 References

NIST SP 800-53r3	SI-3
CAG	CC-2, CC-4, CC-5, CC-7, CC-10, CC-12, CC-13, CC-15, CC-16, CC-17
API 1164r2	5.7, 5.8, 5.8, Annex B.3.1.2
NERC CIPS	CIP 007-3 B.R4, R4.1, R4.2
NRC RG 5.71	App. B.1.16, App. B.1.20, App. B.3.11, App. B.5.2, App. C.3.3

2.14.4 System Monitoring Tools and Techniques

2.14.4.1 Requirement

The organization:

1. Monitors events on the system
2. Detects system attacks
3. Identifies unauthorized use of the system
4. Deploys monitoring devices (a) strategically within the system to collect organization-determined essential information and (b) at ad hoc locations within the system to track specific types of transactions of interest to the organization
5. Heightens the level of system monitoring activity whenever an indication of increased risk exists to organizational operations and assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information
6. Consults legal counsel with regard to system monitoring activities.

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). It is paramount that the use of monitoring tools and techniques does not adversely impact the operation performance of the ICS. 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 also can be deployed at ad hoc locations within the system to track specific transactions. In addition, 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. An example of a specific type of transaction of interest to the organization with regard to monitoring is HTTP traffic that bypasses organizational HTTP proxies, when use of such proxies is required. 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 an indication of increased risk exists 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 systemwide intrusion detection system using common protocols.
2. In situations where the ICS cannot support the use of automated tools to support near real-time analysis of events, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.
3. The organization employs automated tools to support near real-time analysis of events.
4. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.
5. The control system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Unusual/unauthorized activities or conditions include the presence of malicious code, the unauthorized export of information, or signaling to an external control system.
6. The control system provides a real-time alert when indications of compromise or potential compromise occur.
7. The system prevents users from circumventing host-based intrusion detection and prevention capabilities.
8. In situations where the ICS cannot prevent nonprivileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls (e.g., enhanced auditing) in accordance with the general tailoring guidance.
9. The system notifies a defined list of incident response personnel of suspicious events and takes a defined list of least disruptive actions to terminate suspicious events. Note: The least disruptive actions may include initiating request for human response.
10. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.
11. The organization tests/exercises intrusion monitoring tools on a defined time-period. Note: The frequency of tests/exercises is dependent on the type and method of deployment of the intrusion monitoring tools.

12. The organization makes provisions so that encrypted traffic is visible to system monitoring tools. Note: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount, for others the mission assurance concerns are greater.
13. The system analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. Note: Anomalies within the system include large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.
14. The use of monitoring tools and techniques must not adversely impact the operational performance of the control system.

2.14.4.4 References

NIST SP 800-53r3	SI-4
CAG	CC-5, CC-6, CC-14, CC-15
API 1164r2	3.5, Annex B.0, Annex B.3.1.2
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. B.1.17, App. B.5.2, App. C.3.4

2.14.5 Security Alerts and Advisories and Directives

2.14.5.1 Requirement

The organization:

1. Receives system security alerts, advisories, and directives from designated external organizations on an ongoing basis
2. Generates internal security alerts, advisories, and directives as deemed necessary
3. Disseminates security alerts, advisories, and directives to an organization-defined list of personnel
4. Implements security directives in accordance with timeframes established by the directives, or notifies the issuing organization of the degree of noncompliance. Shutting down and restarting the ICS on the identification of an anomaly are not recommended because the event logs can be erased.

2.14.5.2 Supplemental Guidance

The US-CERT generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential because of the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the nation should the directives not be implemented in a timely manner. Preplanned segmentation and limited operational plans should be enacted to maximize operational availability if immediate untested compliance represents a greater detrimental threat to the ICS.

2.14.5.3 Requirement Enhancements

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

2.14.5.4 References

NIST SP 800-53r3 SI-5

API 1164r2	Annex B.5.1.1.5
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. C.3.5

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 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, the control system resources should not be shut down and restarted 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.

2.14.6.4 References

NIST SP 800-53r3	SI-6
API 1164r2	7.2, Annex B.4.1.2
NERC CIPS	CIP 007-3 B.R4, R6
NRC RG 5.71	App. B.3.2, App. B.4.9

2.14.7 Software and Information Integrity

2.14.7.1 Requirement

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

2.14.7.2 Supplemental Guidance

The organization employs integrity verification techniques on the system to look for evidence of information tampering, errors, and 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 monitor automatically the integrity of the IT systems, control systems, and the applications it hosts. The organization uses automated tools with extreme caution on designated high-availability systems.

2.14.7.3 Requirement Enhancements

1. The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the system and uses the scans with extreme caution on designated high-availability systems.
2. The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification and uses automated tools with extreme caution on designated high-availability systems.

3. The organization employs centrally managed integrity verification tools and uses such tools with extreme caution on designated high-availability systems.
4. The organization requires use of tamper-evident packaging for organization-defined system components during transportation from vendor to operational site, during operation, or both.

2.14.7.4 References

NIST SP 800-53r3	SI-7
CAG	CC-3
API 1164r2	3.6, 7.2.2.2, Annex A
NRC RG 5.71	App. B.1.16, App. B.3.2

2.14.8 Spam Protection

2.14.8.1 Requirement

The organization:

1. Employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means
2. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures
3. Considers using spam protection software products from multiple vendors as part of defense-in-depth.

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

2.14.8.4 References

NIST SP 800-53r3 SI-8

API 1164r2	7.2.2.1, 7.3.7
NERC CIPS	CIP 007-3 B.R4
NRC RG 5.71	App. C.3.3

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

2.14.9.4 References

NIST SP 800-53r3	SI-9
API 1164r2	6.1, Annex A
NERC CIPS	CIP 003-3 B.R5
NRC RG 5.71	App. C.3.8

2.14.10 Information Input Validation

2.14.10.1 Requirement

The control system checks the validity of information inputs by employing mechanisms to check for accuracy, completeness, validity, and authenticity.

2.14.10.2 Supplemental Guidance

Rules for checking accuracy, completeness, validity, and authenticity of information inputs should be accomplished as close to the point of origin as possible. Rules for checking the valid syntax and semantics 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 prescreened to ensure the content is not unintentionally interpreted as commands. The extent 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

2.14.10.4 References

NIST SP 800-53r3	SI-10
CAG	CC-7
API 1164r2	5, 8.1, Annex A
NRC RG 5.71	App. B.3.6, App. C.3.8

2.14.11 Error Handling

2.14.11.1 Requirement

The system:

1. Identifies error conditions
2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries
3. Reveals error messages only to authorized personnel
4. Prohibits inclusion of sensitive information in error logs or associated administrative messages.

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 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

2.14.11.4 References

NIST SP 800-53r3	SI-11
API 1164r2	7.2
NRC RG 5.71	App. C.3.9

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

The National Archives and Records Administration provides guidance on records retention.

2.14.12.3 Requirement Enhancements

None

2.14.12.4 References

NIST SP 800-53r3	SI-12
API 1164r2	3.1, 6, Annex A
NERC CIPS	CIP 005-3 B.R5 to R5.3
NRC RG 5.71	App. C.3.10

2.14.13 Predictable Failure Prevention

2.14.13.1 Requirement

The organization:

1. Protects the system from harm by considering mean time to failure for an organization-defined list of system components in specific environments of operation
2. Provides substitute system components, when needed, and a mechanism to exchange active and standby roles of the components.

2.14.13.2 Supplemental Guidance

Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry average. The transfer of responsibilities between active and standby system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress, or for maintenance reasons.

2.14.13.3 Requirement Enhancements

1. The organization takes the system component out of service by transferring component responsibilities to a substitute component no later than an organization-defined fraction or percentage of mean time to failure.
2. The organization does not allow a process to execute without supervision for more than an organization-defined time period.
3. The organization manually initiates a transfer between active and standby system components at least once per a defined frequency if the mean time to failure exceeds the defined time period.
4. The organization, if a system component failure is detected, (a) ensures that the standby system component successfully and transparently assumes its role within a defined time period and (b) activates an alarm and/or automatically shuts down the system. Note: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

2.14.13.4 References

NIST SP 800-53r3	SI-13
API 1164r2	3.4, 6, Annex A, Annex B.3, Annex B.5
NRC RG 5.71	App. B.3.22, App. C.3.11, App. C.9.2

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 in 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 and updates:

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

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

1. Public access to ICS is not permitted.
2. Business IT and general corporation access to the ICS is not permitted.

2.15.1.4 References

NIST SP 800-53r3	AC-1, SC-14
CAG	CC-9
API 1164r2	4, 5, Annex A
NERC CIPS	CIP 003-3 B.R5, CIP 005-3 B.R2
NRC RG 5.71	C.3.3.1.1, App. B.1.1

2.15.2 Identification and Authentication Policy and Procedures

2.15.2.1 Requirement

The organization develops, disseminates, and periodically reviews and 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

2.15.2.4 References

NIST SP 800-53r3 IA-1

API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R2.5
NRC RG 5.71	App. B.4.1

2.15.3 Account Management

2.15.3.1 Requirement

The organization manages system accounts, including:

1. Identifying account types (i.e., individual, group, and system)
2. Establishing conditions for group membership
3. Identifying authorized users of the system and specifying access rights and privileges
4. Requiring appropriate approvals for requests to establish accounts
5. Authorizing, establishing, activating, modifying, disabling, and removing accounts
6. Reviewing accounts on a defined frequency
7. Specifically authorizing and monitoring the use of guest/anonymous accounts
8. Notifying account managers when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes
9. Granting access to the system based on a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage.

2.15.3.2 Supplemental Guidance

The identification of authorized users of the system and the specification of access rights and privileges are consistent with the requirements in other security controls in the security plan.

2.15.3.3 Requirement Enhancements

1. The organization employs automated mechanisms to support the management of system accounts.
2. The system automatically terminates temporary and emergency accounts after a defined time period for each type of account.
3. The system automatically disables inactive accounts after a defined time period.
4. The system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.
5. The organization reviews currently active system accounts on a defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.
6. The organization prohibits the use of system account identifiers as the identifiers for user electronic mail accounts.

2.15.3.4 References

NIST SP 800-53r3	AC-2
CAG	CC-9, CC-11
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R5

NRC RG 5.71 App. B.1.2

2.15.4 Identifier Management

2.15.4.1 Requirement

The organization manages system identifiers for users and devices by:

1. Receiving authorization from a designated organizational official to assign a user or device identifier
2. Selecting an identifier that uniquely identifies an individual or device
3. Assigning the user identifier to the intended party or the device identifier to the intended device
4. Archiving previous user or device identifiers.

2.15.4.2 Supplemental Guidance

Common device identifiers include Media Access Control (MAC) or IP addresses, or device unique token identifiers. Management of user identifiers is not applicable to shared system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of a system account associated with an individual.

2.15.4.3 Requirement Enhancements

None

2.15.4.4 References

NIST SP 800-53r3 IA-4

API 1164r2 Annex A

NERC CIPS CIP 005-3 B.R5

NRC RG 5.71 App. B.4.6

2.15.5 Authenticator Management

2.15.5.1 Requirement

The organization manages system authenticators for users and devices by:

1. Verifying, as part of the initial authenticator distribution for a user authenticator, the identity of the individual receiving the authenticator
2. Establishing initial authenticator content for organization-defined authenticators
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators
5. Changing default content of authenticators upon system installation
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate)
7. Changing or refreshing authenticators periodically, as appropriate for authenticator type
8. Protecting authenticator content from unauthorized disclosure and modification
9. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

2.15.5.2 Supplemental Guidance

Device authenticators include, for example, certificates and passwords. User authenticators include tokens, PKI certificates, biometrics, passwords, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many system components are shipped with factory default user authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation.

The system supports user authenticator management requirements by enforcing organization-defined password minimum and maximum lifetime restrictions and password reuse restrictions for organization-defined number of generations. Measures to safeguard user authenticators includes maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.

2.15.5.3 Requirement Enhancements

1. The system, for PKI-based authentication:
    a. Validates certificates by constructing a certification path with status information to an accepted trust anchor
    b. Enforces authorized access to the corresponding private key
    c. Maps the authenticated identity to the user account. Note: Status information for certification paths includes certificate revocation lists or online certificate status protocol responses.
2. The organization requires that the registration process to receive a user authenticator be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
3. The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.
4. The organization requires unique authenticators be provided by vendors and manufacturers of system components.

2.15.5.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5, 5.5, Annex A
NERC CIPS	CIP 005-3 B.R5
NRC RG 5.71	App. B.4.7

2.15.6 Account Review

2.15.6.1 Requirement

The organization:

1. Reviews and analyzes system audit records on an organization-defined frequency for indications of inappropriate or unusual activity, and report findings to designated organizational officials
2. Adjusts the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

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, security logs are not intended to be reviewed frequently for every workstation but rather at central points, such as a web proxy or e-mail servers, and when specific circumstances warrant review of other audit records.

2.15.6.3 Requirement Enhancements

1. The system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.
2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
3. The system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.
4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to enhance further the ability to identify inappropriate or unusual activity.

2.15.6.4 References

NIST SP 800-53r3	AC-2, AU-6
CAG	CC-6, CC-9, CC-11
API 1164r2	5, Annex A, Annex B.4
NERC CIPS	CIP 005-3 B.R5
NRC RG 5.71	App. B.1.2, App. B.1.11, App. B.2.6

2.15.7 Access Enforcement

2.15.7.1 Requirement

The control system enforces assigned authorizations for controlling logical 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, attribute-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrixes, 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.

In addition to enforcing authorized access at the system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased security for the organization. Consideration is given to the implementation of an audited, manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant.

2.15.7.3 Requirement Enhancements

1. The system enforces dual authorization, based on organizational policies and procedures for organization-defined privileged commands. Note: The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.
2. The system enforces one or more organization-defined nondiscretionary access control policies over organization-defined set of users and resources where the policy rule set for each policy specifies:
   a. Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day)
   b. Required relationships among the access control information to permit access. Note: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, and Originator Controlled Access Control.
3. The system prevents access to organization-defined security-relevant information except during secure, nonoperable system states. Note: Security relevant information is any information within the system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, nonoperable system states are states in which the system is not performing mission/business-related processing (e.g., the system is offline for maintenance, troubleshooting, bootup, shutdown).

2.15.7.4 References

NIST SP 800-53r3	AC-3
CAG	CC-9, CC-11
API 1164r2	5.10, Annex A
NERC CIPS	CIP 003-3 B.R5
NRC RG 5.71	App. B.1.3

2.15.8 Separation of Duties

2.15.8.1 Requirement

The organization:

1. Establishes division of responsibilities and separates duties of individuals as necessary to eliminate conflicts of interest
2. Implements separation of duties through assigned system access authorizations.

2.15.8.2 Supplemental Guidance

Separation of duties prevents users from having the system access necessary to perform malevolent activity without collusion. Examples of separation of duties include (1) mission functions and distinct system support functions are divided among different individuals and roles; (2) different individuals perform 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 do not administer audit functions.

In situations where the ICS cannot support the differentiation of roles, the organization employs appropriate compensating controls. The organization carefully considers the appropriateness of single individuals or single groups performing multiple critical roles.

2.15.8.3 Requirement Enhancements

None

2.15.8.4 References

NIST SP 800-53r3	AC-5
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5.2
NRC RG 5.71	App. B.1.5

2.15.9 Least Privilege

2.15.9.1 Requirement

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

2.15.9.2 Supplemental Guidance

The organization employs the concept of least privilege for specific duties and the 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.

In situations where the ICS cannot support the differentiation of privileges, the organization employs appropriate compensating controls. The organization carefully considers the appropriateness of single individuals or single groups having multiple critical privileges.

2.15.9.3 Requirement Enhancements

1. The organization explicitly authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information. Note: Explicitly authorized personnel include security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
2. The organization requires that users of system accounts with access to organization-defined list of security functions or security-relevant information, use nonprivileged accounts when accessing other system functions, and if feasible, audits any use of privileged accounts for such functions.
3. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the system.

2.15.9.4 References

NIST SP 800-53r3	AC-6
CAG	CC-8, CC-9
API 1164r2	Annex A
NERC CIPS	CIP 003-3 B.R5, R5.2
NRC RG 5.71	App. B.1.6, App. B.5.3

2.15.10 User Identification and Authentication

2.15.10.1 Requirement

The system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational 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. Authentication of user identities is accomplished by passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Organizational users include employees and contractors. Access to organizational systems is defined as either local or network. Local access is any access to an organizational system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational system by a user (or process acting on behalf of a user) where such access is obtained across a network connection. Remote access is a type of network access which involves communication through an external, nonorganization-controlled network (e.g., the Internet). Organization-controlled networks include local area networks, wide area networks, and virtual private networks that are totally under the control of the organization. Identification and authentication requirements for system access by other than organizational users are described in other controls.

FIPS 201 specifies a PIV credential for use in the unique identification and authentication of federal employees and contractors. The identification and authentication requirements in this control are satisfied by complying with FIPS 201 as required by Homeland Security Presidential Directive (HSPD) 12. The selection of authentication mechanisms specified in FIPS 201 is constrained by whether access to the organizational system is local or network. FIPS 201 (Section 6.3.2) provides information on appropriate authentication mechanisms for local and network accesses to systems. In addition to identifying and authenticating users at the system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased security for the organization.

2.15.10.3 Requirement Enhancements

1. The system employs multifactor authentication for remote access and for access to privileged accounts.
2. The system employs multifactor authentication for network access and for access to privileged accounts.
3. The system employs multifactor authentication for local and network access.

2.15.10.4 References

NIST SP 800-53r3	IA-2, IA-8
CAG	CC-4, CC-5
API 1164r2	5, Annex A
NERC CIPS	CIP 003-3 B.R5, R5.1, R5.1.1
NRC RG 5.71	App. B.4.2, App. B.4.6

2.15.11 Permitted Actions without Identification or Authentication

2.15.11.1 Requirement

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

2.15.11.2 Supplemental Guidance

The organization may allow limited user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible systems. Organizations should also identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed.

Such bypass may be via a physical switch that is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and authentication have not yet occurred.

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.

2.15.11.4 References

NIST SP 800-53r3 AC-14

NRC RG 5.71 App. B.1.12

2.15.12 Device Identification and Authentication

2.15.12.1 Requirement

The system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection.

2.15.12.2 Supplemental Guidance

The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The system typically uses either shared known information (e.g., MAC or Transmission Control Protocol/IP [TCP/IP] addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP] or a Radius server with EAP-Transport Layer Security authentication) to identify and authenticate devices on local and wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the system with higher impact levels requiring stronger authentication.

2.15.12.3 Requirement Enhancements

1. The system authenticates devices before establishing remote network connections using bi-directional authentication between devices that are cryptographically based. Note: Remote network connection is any connection with a device communicating through an external, nonorganization-controlled network (e.g., the Internet).
2. The system authenticates devices before establishing network connections using bidirectional authentication between devices that are cryptographically based.

2.15.12.4 References

NIST SP 800-53r3 IA-3

API 1164r2 8.1, Annex B.3.1.4.2

NRC RG 5.71 App. B.4.1, App. B.4.5

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

2.15.13.4 References

NIST SP 800-53r3	IA-6
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R3.2
NRC RG 5.71	App. B.4.8

2.15.14 Cryptographic Module Authentication

2.15.14.1 Requirement

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

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.

2.15.14.4 References

NIST SP 800-53r3	IA-7
API 1164r2	8.2.2, Annex A, Annex B.23.1.6
NRC RG 5.71	App. B.4.9

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 system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions. Note: Information flow enforcement mechanisms compare labels on all information (data content and data structure) and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the information flow policy. Information flow enforcement using explicit labels can be used to control the release of certain types of information.
2. The system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.
3. The system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.
4. The system prevents encrypted data from bypassing content-checking mechanisms.
5. The system enforces organization-defined limitations on the embedding of data types within other data types.
6. The system enforces information flow control on metadata.
7. The system enforces organization-defined one-way flows using hardware mechanisms.
8. The system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions.
9. The system enforces the use of human review for organization-defined security policy filters when the system is not capable of making an information flow control decision.
10. The system provides the capability for a privileged administrator to enable and disable organization-defined security policy filters.
11. The system provides the capability for a privileged administrator to configure the organization-defined security policy filters to support different security policies.

2.15.15.4 References

NIST SP 800-53r3	AC-4
CAG	CC-4, CC-9, CC-15
API 1164r2	Annex A, Annex B.3.1.3, Annex B.3.1.4
NERC CIPS	CIP 003-3 B.R5

NRC RG 5.71	App. B.1.1, App. B.1.4

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 (minimum/maximum 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 login. 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 are 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

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

2.15.16.4 References

NIST SP 800-53r3	IA-5
CAG	CC-4
API 1164r2	5.5, 8.1, Annex A, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R4.4

NRC RG 5.71	App. B.4.3, App. B.4.7

2.15.17 System Use Notification

2.15.17.1 Requirement

The system:

1. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states that (a) users are accessing a private or government system; (b) system usage may be monitored, recorded, and subject to audit; (c) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (d) use of the system indicates consent to monitoring and recording
2. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access, the system
3. For publicly accessible systems, (a) displays the system use information, when appropriate, before granting further access; (b) ensures that any references to monitoring, recording, or auditing are consistent with privacy accommodations for such systems that generally prohibit those activities; and (c) includes in the notice given to public users of the system, a description of the authorized uses of the system.

2.15.17.2 Supplemental Guidance

System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the system. System use notification is intended only for system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

2.15.17.3 Requirement Enhancement

None

2.15.17.4 References

NIST SP 800-53r3	AC-8
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R3.2
NRC RG 5.71	App. B.1.8

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

The organization may define the maximum number of concurrent sessions for a system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given system account and does not address concurrent sessions by a single user via multiple system accounts.

2.15.18.3 Requirement Enhancements

None

2.15.18.4 References

NIST SP 800-53r3 AC-10

NRC RG 5.71 App. B.4.4

2.15.19 Previous Logon (Access) Notification

2.15.19.1 Requirement

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

2.15.19.2 Supplemental Guidance

This control is intended to cover both traditional user logons to ICS systems as well as service-related processes that automatically log on to the ICS.

2.15.19.3 Requirement Enhancements

1. The information system is capable of notifying the user the number of successful logon and access attempts as well as unsuccessful logon and access attempts.
2. The information system is capable of displaying security-related changes to the user's account within an organizational-defined time period.

2.15.19.4 References

NIST SP 800-53r3 AC-9

NRC RG 5.71 App. B.1.9

2.15.20 Unsuccessful Login Attempts

2.15.20.1 Requirement

The system:

1. Enforces a limit of an organization-defined number of consecutive invalid access attempts by a user during an organization-defined time period
2. Automatically locks the account/node for an organization-defined time period and delays the next login prompt according to an organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

2.15.20.2 Supplemental Guidance

Because of the potential for denial of service, automatic lockouts initiated by the system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may choose to employ different algorithms for different system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application level. Permanent automatic lockouts initiated by a control system must be carefully considered before being used because of safety considerations and the potential for denial of service. Operator lockouts for critical and emergency control stations must maintain maximum control. In these cases, compensatory security requirements, such as limited physical access to trusted employees, are used.

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.

2.15.20.4 References

NIST SP 800-53r3	AC-7
API 1164r2	5.5
NRC RG 5.71	App. B.1.7

2.15.21 Session Lock

2.15.21.1 Requirement

The system:

1. Prevents further access to the system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user
2. Retains the session lock until the user re-establishes access using appropriate identification and authentication procedures.

2.15.21.2 Supplemental Guidance

A session lock is not a substitute for logging out of the system. Organization-defined time periods of inactivity comply with policy. In some situations, session-lock for ICS operator workstations/nodes is not advisable (e.g., when immediate operator responses are required for emergency situations). In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures).

2.15.21.3 Requirement Enhancements

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

2.15.21.4 References

NIST SP 800-53r3	AC-11
API 1164r2	5.4
NRC RG 5.71	App. B.1.10, App. B.4.4

2.15.22 Remote Session Termination

2.15.22.1 Requirement

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

2.15.22.2 Supplemental Guidance

This control applies to both organization-controlled networks and nonorganization-controlled networks. The organization-defined time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses in accordance with an organizational assessment of risk.

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.

2.15.22.4 References

NIST SP 800-53r3	SC-10

API 1164r2	5.4
NRC RG 5.71	App. B.3.11, App. B.4.4

2.15.23 Remote Access Policy and Procedures

2.15.23.1 Requirement

The organization:

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

2.15.23.2 Supplemental Guidance

Remote access is any access to an organizational system by a user (or process acting on behalf of a user) communicating through an external, nonorganization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Virtual private network (VPN) when adequately provisioned may be treated as an organization-controlled network. With regard to wireless, radiated signals within organization-controlled facilities typically qualify as outside organizational control. Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Remote access controls are applicable to systems other than public web servers or systems specifically designed for public access.

2.15.23.3 Requirement Enhancements

None

2.15.23.4 References

NIST SP 800-53r3	AC-17
API 1164r2	8.2.4, Annex A
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.3.11

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 secure adequately remote access.

Remote access is any access to an organizational control system by a user (or a system) communicating through an external, nonorganization-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 on 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. Note: The encryption strength of mechanism is selected based on the FIPS 199 impact level of the information.
3. The system routes all remote accesses through a limited number of managed access control points.
4. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the system.
5. The system protects wireless access to the system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary.
6. The organization monitors for unauthorized remote connections to the system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered. Note: Organizations proactively search for unauthorized remote connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to those areas within the facility containing the systems. Yet, the scan is conducted outside those areas only as needed to verify that unauthorized wireless access points are not connected to the system.
7. The organization disables, when not intended for use, wireless networking capabilities internally embedded within system components prior to issue.
8. The organization does not allow users to independently configure wireless networking capabilities.
9. The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
10. The organization ensures that remote sessions for accessing an organization-defined list of security functions and security-relevant information employ additional security measures (organization-defined security measures) and are audited.
11. The organization disables peer-to-peer wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.
12. The organization disables Bluetooth wireless networking capability within the system except for explicitly identified components in support of specific operational requirements.

2.15.24.4 References

NIST SP 800-53r3	AC-17
CAG	CC-5, CC-6, CC-8, CC-14
API 1164r2	8.1, 8.2.4, Annex A, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R4.4
NRC RG 5.71	App. B.1.17, App. B.3.11, App. B.5.3

2.15.25 Access Control for Mobile Devices

2.15.25.1 Requirement

The organization:

1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices
2. Authorizes connection of mobile devices to organizational systems
3. Monitors for unauthorized connections of mobile devices to organizational systems
4. Enforces requirements for the connection of mobile devices to organizational systems
5. Disables system functionality that provides the capability for automatic execution of code on removable media without user direction
6. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures
7. Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

2.15.25.2 Supplemental Guidance

Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives), portable computing, and communications devices with storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Usage restrictions and implementation guidance related to mobile devices can include configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

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

In situations where the ICS cannot implement any or all the components of this control, the organization employs other mechanisms or procedures as compensating controls. This may involve physically locking components; specific access logs; and specific monitoring programs for locks, keys, and access logs.

2.15.25.3 Requirement Enhancements

1. The organization restricts the use of writable, removable media in organizational systems.
2. The organization prohibits the use of personally owned, removable media in organizational systems.
3. The organization prohibits the use of removable media in organizational systems when the media have no identifiable owner. Note: An identifiable owner for removable media helps reduce the risk of

employing such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

2.15.25.4 References

NIST SP 800-53r3	AC-19
CAG	CC-6, CC-8
API 1164r2	Annex A
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.1.19

2.15.26 Wireless Access Restrictions

2.15.26.1 Requirement

The organization:

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

2.15.26.4 References

NIST SP 800-53r3	AC-17
CAG	CC-4, CC-5, CC-6, CC-8, CC-14
API 1164r2	7.2.2.1, 7.3.8, Annex A, Annex B.1.1.1.1, Annex B.1.1.3, Annex B.3.1.4
NERC CIPS	CIP 005-3 B.R2
NRC RG 5.71	App. B.1.17, App. B.3.11, App. B.5.4

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 be 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 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
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

2.15.27.4 References

NIST SP 800-53r3	AC-20
CAG	CC-5
API 1164r2	Annex A
NRC RG 5.71	App. B.1.22

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. The organization explicitly allows necessary network protocols in the demilitarized zone; 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, demilitarized zone).

2.15.28.3 Requirement Enhancements

None

2.15.28.4 References

NIST SP 800-53r3	AC-20, IA-2

CAG	CC-4, CC-5
API 1164r2	7.3, 8, Annex B.3
NERC CIPS	CIP 005-3 B.R1, R2, R3
NRC RG 5.71	App. B.1.18, App. B.1.22, App. B.3.11, App. B.4.6, App. B.5.4

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 system from an external system
2. Process, store, and 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 the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External systems include, but are not limited to, (1) personally owned systems (e.g., computers, cellular telephones, or personal digital assistants), (2) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports), (3) systems owned or controlled by nonfederal governmental organizations, and (4) private or federal systems that are not owned by, operated by, or under the direct supervision and authority of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational system. This control does not apply to the use of external systems to access public interfaces to organizational systems and information. The organization establishes terms and conditions for the use of external systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum (1) the types of applications that can be accessed on the organizational system from the external system and (2) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external system.

2.15.29.3 Requirement Enhancements

1. The organization prohibits authorized individuals from using an external system to access the system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external system as specified in the organization's security policy and security plan or (b) has approved system connection or processing agreements with the organizational entity hosting the external system.
2. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external systems.

2.15.29.4 References

NIST SP 800-53r3	AC-20
CAG	CC-4, CC-5, CC-13, CC-15, CC-16
API 1164r2	7.3, 8, Annex B.3, Annex B.5
NERC CIPS	CIP 005-3 B.R1, R2, R3
NRC RG 5.71	App. B.1.20, App. B.3.11, App. B.5.4

2.15.30 User-Based Collaboration and Information Sharing

2.15.30.1 Requirement

The organization:

1. Facilitates information sharing by enabling specified authorized users to determine whether access authorization assigned to the end users match allowable access restrictions on information where limited discretion/information access is required
2. Employs automated or manual mechanisms as required to assist authorizing users in making the correct information sharing/collaboration decisions.

2.15.30.2 Supplemental Guidance

This control applies to information that may be restricted (e.g., privileged medical, business, proprietary, personally identifiable information, or special access programs/compartmentalization) based on administrative and/or legal determination. End users may be individuals, groups, or organizations, and the information may be defined by specific content, type, or security categorization.

2.15.30.3 Requirement Enhancements

The information system employs automated mechanisms to enable authorized users to make information sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.

2.15.30.4 References

NIST SP 800-53r3	AC-21
API 1164r2	7.3
NERC CIPS	CIP 008-3 B.R1.3

2.15.31 Publicly Accessible Content

2.15.31.1 Requirement

The organization:

1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information
3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system
4. Reviews the content on the publicly accessible organizational information system for nonpublic information on a routine interval
5. Removes nonpublic information from publicly accessible information systems if discovered.

2.15.31.2 Supplemental Guidance

Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, executive orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information is examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public typically without identification or authentication. The posting of information on nonorganizational information systems is covered by appropriate organizational policy.

2.15.31.3 Requirement Enhancements

None

2.15.31.4 References

NIST SP 800-53r3	AC-22
API 1164r2	6
NRC RG 5.71	App. B.1.23

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 also are 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 and 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

2.16.1.4 References

NIST SP 800-53r3	AU-1
API 1164r2	1.2, Annex A, Annex B.4, Annex B.5
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.1

2.16.2 Auditable Events

2.16.2.1 Requirement

The organization:

1. Determines, based on a risk assessment in conjunction with mission/business needs, which system-related events require auditing (e.g., an organization-defined list of auditable events and frequency of [or situation requiring] auditing for each identified auditable event)
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events
3. Ensures that auditable events are adequate to support after-the-fact investigations of security incidents
4. Adjusts, as necessary, the events to be audited within the system based on current threat information and ongoing assessments of risk.

2.16.2.2 Supplemental Guidance

The purpose of this control is for the organization to identify events that need to be auditable as significant and relevant to the security of the system. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses 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. The checklists and configuration guides at http://web.nvd.nist.gov/view/ncp/repository provide recommended lists of auditable events.

2.16.2.3 Requirement Enhancements

1. The organization reviews and updates the list of organization-defined auditable events on an organization-defined frequency.
2. The organization includes execution of privileged functions in the list of events to be audited by the system.

2.16.2.4 References

NIST SP 800-53r3	AU-2, AU-12
CAG	CC-6, CC-8
API 1164r2	7.2, Annex B.2.1, Annex B.5
NERC CIPS	CIP 007-3 B.R5.1.2
NRC RG 5.71	App. B.2.2, App. B.2.12

2.16.3 Content of Audit Records

2.16.3.1 Requirement

The system produces audit records that contain sufficient information to establish what events occurred, when the events occurred, where the events occurred, the sources of the events, and the outcomes of the events.

2.16.3.2 Supplemental Guidance

Audit record content includes (1) date and time of the event, (2) the component of the system (e.g., software component, hardware component) where the event occurred, (3) type of event, (4) user/subject identity, and (5) the outcome (success or failure) of the event.

2.16.3.3 Requirement Enhancements

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

2.16.3.4 References

NIST SP 800-53r3	AU-3, AU-12
CAG	CC-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5
NRC RG 5.71	App. B.2.3, App. B.2.12

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

The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity.

2.16.4.3 Requirement Enhancements

None

2.16.4.4 References

NIST SP 800-53r3	AU-4
CAG	CC-6
NRC RG 5.71	App. B.2.4

2.16.5 Response to Audit Processing Failures

2.16.5.1 Requirement

The system:

1. Alerts designated organizational officials in the event of an audit processing failure
2. Takes the following additional actions: an organization-defined set of actions to be taken (e.g., shutdown system, overwrite oldest audit records, and stop generating audit records).

2.16.5.2 Supplemental Guidance

Audit processing failures include 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 system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity.
2. The system provides a real-time alert when the following audit failure events occur: an organization-defined audit failure event requiring real-time alerts.
3. The system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and either rejects or delays network traffic above those thresholds.

2.16.5.4 References

NIST SP 800-53r3	AU-5

CAG	CC-6
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.5

2.16.6 Audit Monitoring, Analysis, and Reporting

2.16.6.1 Requirement

The organization:

1. Reviews and analyzes system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to designated organizational officials
2. Adjusts the level of audit review, analysis, and reporting within the system when a change in risk exists to organizational operations, organizational assets, individuals, other organizations, or the nation based on law enforcement information, intelligence information, or other credible sources of information.

2.16.6.2 Supplemental Guidance

Organizations increase the level of audit monitoring and analysis activity within the control system whenever an indication of increased risk exists 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 cybersecurity.

2.16.6.3 Requirement Enhancements

1. The system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.
2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
3. The system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system. Note: An example of an automated mechanism for centralized review and analysis is a Security Information Management product.
4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to enhance further the ability to identify inappropriate or unusual activity.

2.16.6.4 References

NIST SP 800-53r3	AU-6
CAG	CC-6
API 1164r2	Annex A, Annex B.3.1.2, Annex B.5.1.1.3
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.6

2.16.7 Audit Reduction and Report Generation

2.16.7.1 Requirement

The system provides an audit reduction and report generation capability.

2.16.7.2 Supplemental Guidance

An audit reduction, review, and reporting capability provides support for near real-time audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter 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 on selectable event criteria.
2. Audit record processing must not degrade the operational performance of the control system.

2.16.7.4 References

NIST SP 800-53r3	AU-7, AU-12
CAG	CC-6
API 1164r2	Annex A
NERC CIPS	CIP 007-3 B.R5.1.2
NRC RG 5.71	App. B.2.7, App. B.2.12

2.16.8 Time Stamps

2.16.8.1 Requirement

The system uses internal system clocks to generate time stamps for audit records.

2.16.8.2 Supplemental Guidance

Time stamps generated by the system include both date and time.

2.16.8.3 Requirement Enhancements

The system synchronizes internal system clocks on an organization-defined frequency.

2.16.8.4 References

NIST SP 800-53r3	AU-8
CAG	CC-6
NERC CIPS	CIP 007-3 B.R6, R6.3
NRC RG 5.71	App. B.2.8

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

The system produces audit records on hardware-enforced, write-once media.

2.16.9.4 References

NIST SP 800-53r3	AU-9
CAG	CC-6
API 1164r2	Annex A

NERC CIPS	CIP 007-3 D1.4
NRC RG 5.71	App. B.2.9

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

The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes retention and availability of audit records relative to subpoena and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated.

2.16.10.3 Requirement Enhancements

None

2.16.10.4 References

NIST SP 800-53r3	AU-11
API 1164r2	Annex A
NERC CIPS	CIP 007-3 D1.4
NRC RG 5.71	App. B.2.11

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 auditors need to be accompanied by an appropriate knowledgeable control system staff person to answer any questions about the particular system under review.

2.16.11.3 Requirement Enhancements

None

2.16.11.4 References

NIST SP 800-53r3	AU-1, CA-7
CAG	CC-17
API 1164r2	Annex A
NERC CIPS	CIP 002-3 through CIP 009-3, C and D
NRC RG 5.71	App. B.2.1

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 process.

2.16.12.3 Requirement Enhancements

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

2.16.12.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17
API 1164r2	Annex A
NRC RG 5.71	C.3.3.2.8

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 cybersecurity 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-handing 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.

2.16.13.4 References

NIST SP 800-53r3	AU-7
API 1164r2	Annex B.4.1.1
NRC RG 5.71	App. B.2.7, App. C.3.4

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 cybersecurity 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

2.16.14.4 References

NIST SP 800-53r3	CA-1
API 1164r2	Annex A, Annex B.4.1
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	C.3.3.3, C.3.3.2.2, App. C.2.1, App. C.5.1, App. C.7

2.16.15 Audit Generation

2.16.15.1 Requirement

The system:

1. Provides audit record generation capability for the auditable events
2. Provides audit record generation capability at the organization-defined system components
3. Allows authorized users to select which auditable events are to be audited by specific components of the system
4. Generates audit records for the selected list of auditable events.

2.16.15.2 Supplemental Guidance

Audit records can be generated from various components within the system. This control defines the specific system components providing auditing capability. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

2.16.15.3 Requirement Enhancements

The system provides the capability to compile audit records from multiple components within the system into a systemwide (logical or physical) audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail. Note: This control does not require that audit records from every component that provides auditing capability within the system be included in the systemwide audit trail. The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls.

2.16.15.4 References

NIST SP 800-53r3	AU-12
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	App. B.2.12, App. C.3.4

2.16.16 Monitoring for Information Disclosure

2.16.16.1 Requirement

The organization monitors open source information for evidence of unauthorized release or disclosure of organizational information.

2.16.16.2 Supplemental Guidance

Unauthorized sensitive protected information (proprietary, security, and configuration) can be discovered in the public domain by self searching public information sources for these types of information releases. This allows the owner to attempt to contain or remove identified sensitive information from such public sources.

2.16.16.3 Requirement Enhancements

None

2.16.16.4 References

NIST SP 800-53r3 AU-13

NERC CIPS CIP 002-3 through CIP 009-3, D

2.16.17 Session Audit

2.16.17.1 Requirement

Where legally required, the system provides the capability to:

1. Capture and record and log all content related to a user session
2. Remotely view and hear all content related to an established user session in real time.

2.16.17.2 Supplemental Guidance

Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, executive orders, directives, policies, or regulations. Very specific critical infrastructure applications in multiple industrial sectors require control room or cockpit monitoring as a part of operational regulation.

2.16.17.3 Requirement Enhancements

None

2.16.17.4 References

NIST SP 800-53r3 AU-14

API 1164r2 Annex A

NERC CIPS CIP 002-3 through CIP 009-3, D

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 its 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 deviations or nonconformance exists, 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 and 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

2.17.1.4 References

NIST SP 800-53r3	PM-1
CAG	CC-17
API 1164r2	1.2
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	App. C.3.4

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

2.17.2.4 References

NIST SP 800-53r3	CA-2, CA-7
CAG	CC-17
API 1164r2	1.2
NERC CIPS	CIP 002-3 through CIP 009-3, D
NRC RG 5.71	C.4.1

2.17.3 Monitoring of Security Policy

2.17.3.1 Requirement

The organization includes a process for monitoring and reviewing the performance of its cybersecurity 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 cybersecurity audits, incidents, suggestions, and feedback from the organizations corrective action program.

2.17.3.3 Requirement Enhancements

None

2.17.3.4 References

NIST SP 800-53r3 CA-2, CA-7

CAG CC-2, CC-3, CC-4

API 1164r2 Annex B.4.1.2

NERC CIPS CIP 002-3 through CIP 009-3, D

NRC RG 5.71 C.3.3.3.2, C.4.1, C.4.1.1, C.4.1.2, C.4.1.3

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:

1. Industry events that identify failed and successful cybersecurity breaches
2. Actions to be taken to resolve a breach of cybersecurity that are defined in light of the
   a. Business priorities
   b. Processes employed to collect metrics (e.g., audits, incidents) that help verify that the cybersecurity activities (manual or automated) are performing as expected
   c. Process that will trigger a review of the level of residual risk and acceptable risk taking when changes exist to the organization, technology, business objectives, and processes
   d. External events including identified threats and changes in social climate
   e. Operational data analyzed, recorded, and reported to assess the effectiveness or performance of the cybersecurity management system.

2.17.4.3 Requirement Enhancements

None

2.17.4.4 References

NIST SP 800-53r3 CA-7

CAG CC-17

API 1164r2 1.2

NERC CIPS CIP 002-3 through CIP 009-3

NRC RG 5.71 App. C.3.5

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 a significant change occurs 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

2.17.5.4 References

NIST SP 800-53r3	CA-6
API 1164r2	3.6, Annex A
NRC RG 5.71	C.3.3

2.17.6 Security Certification

2.17.6.1 Requirement

The organization assesses the security mechanisms in the control system to determine the extent 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 offline, to the extent feasible, before the assessments can be conducted. If a control system must be taken offline 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 assess 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 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.

4. 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.
5. 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.

2.17.6.4 References

NIST SP 800-53r3 CA-4

API 1164r2 3.7

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 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 and 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

2.18.1.4 References

NIST SP 800-53r3	RA-1
API 1164r2	3.3, Annex B.2
NERC CIPS	CIP 002-3 B.R1, R1.2
NRC RG 5.71	C.3.3

2.18.2 Risk Management Plan

2.18.2.1 Requirement

The organization develops a risk management plan. A senior organization official reviews and approves the risk management plan.

2.18.2.2 Supplemental Guidance

None

2.18.2.3 Requirement Enhancements

None

2.18.2.4 References

NIST SP 800-53r3	CA-1, RA-1, PM-9
CAG	CC-9
API 1164r2	3.3, Annex B.2
NERC CIPS	CIP 002-3 B.R1, R1.2
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.3 Certification, Accreditation, and Security Assessment Policies and Procedures

2.18.3.1 Requirement

The organization develops, disseminates, and periodically reviews and 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

2.18.3.4 References

NIST SP 800-53r3	CA-1, PM-9
API 1164r2	3.3, Annex B.2
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.4 Security Assessments

2.18.4.1 Requirement

The organization:

1. Assesses the security controls in the system on an organization-defined frequency, at least annually, to determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
2. Produces a security assessment report that documents the results of the assessment.

2.18.4.2 Supplemental Guidance

The organization assesses the security controls in a system as part of (1) security authorization or reauthorization, (2) meeting the requirement for annual assessments, (3) continuous monitoring, and (4) testing/evaluation of the system as part of the system development life-cycle process. The requirement for (at least) annual security control assessments should not be interpreted by organizations as adding assessment requirements to those requirements already in place in the security authorization process. To satisfy the annual assessment requirement, organizations can draw on the security control assessment results from any of the following sources, including but not limited to, (1) security assessments conducted as part of a system authorization or reauthorization process, (2) continuous monitoring, or (3) testing and evaluation of the system as part of the ongoing system development life-cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the system and in accordance with policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls for the system is based on (1) the security categorization of the system, (2) the specific security controls selected and employed by the organization, and (3) the level of assurance that the organization must have in determining the effectiveness of the security controls. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the system for assessment. Those security controls that are volatile or critical to protecting the system are assessed at least annually. All other controls are assessed at least once during the system's 3-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness.

2.18.4.3 Requirement Enhancements

1. The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the system.
2. The organization includes as part of security control assessments, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises.

2.18.4.4 References

NIST SP 800-53r3	CA-2
CAG	CC-17

API 1164r2	Annex B.4.1.2
NERC CIPS	CIP 003-3 B.R4, R4.3, CIP 005-3 B.R4
NRC RG 5.71	C.3.3, C.3.3.3, C.3.3.3.2, App. C.13

2.18.5 Control System Connections

2.18.5.1 Requirement

The organization:

1. Authorizes all connections from the system to other systems outside the authorization boundary through the use of system connection agreements
2. Documents the system connections and associated security requirements for each connection
3. Monitors the system connections on an ongoing basis verifying enforcement of documented security requirements.

2.18.5.2 Supplemental Guidance

Because security categorizations apply to individual systems, the organization carefully considers the risks that may be introduced when systems are connected to other systems with different security requirements and security controls, both internal to the organization and external to the organization. Each interconnection between systems must be addressed individually, documenting the interface characteristics. The level of formality for this documentation varies depending on the relationship between the systems. The relationship ranges from systems with the same owner for which there is no need of an agreement but simply a description of the interface characteristics, to systems within different organizations necessitating a formal interconnection security agreement and a Memorandum of Understanding/Agreement. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the systems. Risk considerations also include systems sharing the same networks.

2.18.5.3 Requirement Enhancements

None

2.18.5.4 References

NIST SP 800-53r3	CA-3
CAG	CC-5
API 1164r2	7.1, 7.3.1, 7.3.2, 7.3.3, 7.3.4, 8.2
NERC CIPS	CIP 005-3 B.R1, R2, R3

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 weaknesses or 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

2.18.6.4 References

NIST SP 800-53r3	CA-5
API 1164r2	Annex B.3.1.1, Annex B.5.1.1.1
NERC CIPS	CIP 002-3 through CIP 009-3, C and D

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 3-year accreditation cycle.

2.18.7.2 Supplemental Guidance

A continuous monitoring program allows an organization to maintain the security authorization of a system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management for systems. An effective continuous monitoring program includes: (1) configuration management and control of system components, (2) security impact analyses of changes to the system or its environment of operation, (3) ongoing assessment of security controls, and (4) status reporting.

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

2.18.7.3 Requirement Enhancements

The organization employs an independent assessor or assessment team to monitor the security controls in the system on an ongoing basis.

2.18.7.4 References

NIST SP 800-53r3	PM-4, PM-8, PM-9, PM-11, CA-7
CAG	CC-17
API 1164r2	7.2, Annex A, Annex B.3.1.4, Annex B.4.1
NERC CIPS	CIP 007-3 B.R6
NRC RG 5.71	C.4, C.4.1, App. C.3.4, App. C.5.8

2.18.8 Security Categorization

2.18.8.1 Requirement

The organization:

1. Categorizes information and systems in accordance with applicable laws, management orders, directives, policies, regulations, standards, and guidance

2. Documents the security categorization results (including supporting rationale) in the system security plan for the information system

3. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

2.18.8.2 Supplemental Guidance

A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of availability, integrity, or confidentiality. 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 inventories and reviews the control system and information categorizations with established configuration management plans including where the information is processed, stored, and transmitted. 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

2.18.8.4 References

NIST SP 800-53r3	RA-2
CAG	CC-9
API 1164r2	6, Annex B.2.1
NERC CIPS	CIP 007-3 A, B, C, D

2.18.9 Risk Assessment

2.18.9.1 Requirement

The organization develops, disseminates, and 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.

2.18.9.2 Supplemental Guidance

This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable laws, executive orders, directives, policies regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. 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

2.18.9.4 References

NIST SP 800-53r3	RA-3
CAG	CC-5, CC-10, CC-15, CC-16, CC-17
API 1164r2	7.2, Annex A, Annex B.3.1.4, Annex B.4.1
NERC CIPS	CIP 003-3 B.R4, R4.3, CIP 005-3 B.R4
NRC RG 5.71	C.3.3, App. C.13

2.18.10 Risk Assessment Update

2.18.10.1 Requirement

The organization updates the risk assessment plan annually or, whenever significant changes occur 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

2.18.10.4 References

NIST SP 800-53r3	RA-3
CAG	CC-10, CC-17
API 1164r2	3.3, 3.6, Annex A
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.3.3, App. C.13

2.18.11 Vulnerability Assessment and Awareness

2.18.11.1 Requirement

The organization:

1. Scans for vulnerabilities in the system on an organization-defined frequency and randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system are identified and reported
2. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations; (b) formatting and making transparent checklists and test procedures; and (c) measuring vulnerability impact
3. Analyzes vulnerability scan reports and remediates legitimate vulnerabilities within a defined timeframe based on an assessment of risk

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

2.18.11.2 Supplemental Guidance

Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms. Operational approval and care must be used when and if vulnerability scanning and penetration testing are used, to ensure ICS functions are not adversely impacted by the scanning process. Production ICS need to be taken off-line or replicated on test beds to the extent feasible. It is possible to scan ICS systems if they are off-line, but caution and approval of such scans are essential. Network scanning tools have been known to cause detrimental operational issues if not configured and tested before being used. It is not recommended to scan operational ICS systems unless absolutely required. If the risks for scanning on operational equipment are deemed too great, the organization should employ compensating controls.

2.18.11.3 Requirement Enhancements

1. The organization employs vulnerability scanning tools that include the capability to readily update the list of system vulnerabilities scanned.
2. The organization updates the list of system vulnerabilities scanned on an organization-defined frequency or when new vulnerabilities are identified and reported.
3. The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., system components scanned and vulnerabilities checked).
4. The organization attempts to discern what information about the system is discoverable by adversaries.
5. The organization performs security testing to determine the level of difficulty in circumventing the security controls of the system.
6. The organization includes privileged access authorization to organization-defined system components for selected vulnerability scanning activities to facilitate more thorough scanning.
7. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.
8. The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational systems and notify designated organizational officials.

2.18.11.4 References

NIST SP 800-53r3	RA-5
CAG	CC-4, CC-5, CC-7, CC-10, CC-17
API 1164r2	3.3, 3.6, Annex A
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.4, C.4.1.3, App. C.13.1

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 are 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

2.18.12.4 References

NIST SP 800-53r3	RA-5
CAG	CC-4, CC-5, CC-7, CC-10, CC-17
API 1164r2	Annex B.3.1
NERC CIPS	CIP 007-3 B.R8
NRC RG 5.71	C.4, C.4.1.3, App. C.13.1

2.19 Security Program Management

2.19.1 Information Security Program Plan

2.19.1.1 Requirement

The organization:

1. Develops and disseminates an organization-wide security program plan that:
   a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements
   b. Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended
   c. Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance

d. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation

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

3. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

2.19.1.2 Supplemental Guidance

The security program plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual systems and the organization-wide security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's security program plan unless the controls are included in a separate security plan for a system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational systems). The organization-wide security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a separate document or in multiple documents in situations where different organizational entities are assigned responsibility. These different entities are accountable for the implementation, assessment, and approval of the common controls that are not implemented as part of a system. In those cases, the documents describing common controls are included as attachments to the security program plan. If multiple common control documents are contained in the security program plan, the organization specifies in each document, the organizational official or officials responsible for the implementation, assessment, and approval of the common controls included in the respective documents. For example, the organization may require that the Facilities Management Office develop, implement, assess, and approve common physical and environmental protection controls or that the Human Resources Office develop, implement, assess, and approve common personnel security controls when such controls are not associated with a system.

2.19.1.3 Requirement Enhancements

None

2.19.1.4 References

NIST SP 800-53r3	PM-1
API 1164r2	1.2, 3
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. C.5.3

2.19.2 Senior Information Security Officer

2.19.2.1 Requirement

The organization appoints a senior security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.

2.19.2.2 Supplemental Guidance

The security officer described in this control is an official of the organization or an official of an appropriate subordinate organization. Organizations also may refer to this organizational official as the Senior Security Officer or Chief Security Officer.

2.19.2.3 Requirement Enhancements

None

2.19.2.4 References

NIST SP 800-53r3	PM-2
API 1164r2	1.2, Annex B.5
NERC CIPS	CIP 002-3 B.R4
NRC RG 5.71	C.3.1.2

2.19.3 Information Security Resources

2.19.3.1 Requirement

The organization:

1. Ensures that all capital planning and investment requests include the resources needed to implement the security program and documents all exceptions to this requirement
2. Employs a business case to record the resources required
3. Ensures that security resources are available for expenditure as planned and approved.

2.19.3.2 Supplemental Guidance

Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the security-related aspects of the capital planning and investment control process.

2.19.3.3 Requirement Enhancements

None

2.19.3.4 References

NIST SP 800-53r3	PM-3
API 1164r2	3.6
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.4 Plan of Action and Milestones Process

2.19.4.1 Requirement

The organization (1) implements a process for ensuring that plans of action and milestones for the security program and the associated organizational systems are maintained and (2) documents the remedial security actions (from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets, individuals, other organizations, and the nation.

2.19.4.2 Supplemental Guidance

The plan of action and milestones is a key document in the security program. The plan of action and milestones updates is based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

2.19.4.3 Requirement Enhancements

None

2.19.4.4 References

NIST SP 800-53r3	PM-4
API 1164r2	Annex B.3.1.1, Annex B.5.1.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.5 Information System Inventory

2.19.5.1 Requirement

The organization develops and maintains an inventory of its systems and critical components.

2.19.5.2 Supplemental Guidance

This control addresses the inventory requirements in Federal Information Security Management Act (FISMA). Federal organizations or organizations using information systems on behalf of a federal agency must comply with FISMA requirements. Additionally, a central tenet of the US Comprehensive National Cybersecurity Initiative states that "offense must inform defense." Or, knowledge of actual attacks that have already compromised systems is the essential foundation on how to begin to construct effective defenses. But the basic tenant in cybersecurity is that you have to know what elements you have and how they work and how they are connected before you can begin the process of protecting them.

2.19.5.3 Requirement Enhancements

None

2.19.5.4 References

NIST SP 800-53r3	CA-3, CM-3 CM-6, IA-3,PM-5
CAG	CC-1
API 1164r2	3.6, Annex B. 1.1, Annex B.2.1
NERC CIPS	CIP 002-3 through CIP 009-3
NRC RG 5.71	App. C.11.9

2.19.6 Information Security Measures of Performance

2.19.6.1 Requirement

The organization develops, monitors, and reports on the results of security measures of performance.

2.19.6.2 Supplemental Guidance

Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the security program and the security controls employed in support of the program.

2.19.6.3 Requirement Enhancements

None

2.19.6.4 References

NIST SP 800-53r3	PM-6
CAG	CC-1, CC-2, CC-3
API 1164r2	7.2.2, 8.2.4, Annex A, Annex B.1, Annex B.2.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.7 Enterprise Architecture

2.19.7.1 Requirement

The organization develops an enterprise architecture with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation.

2.19.7.2 Supplemental Guidance

The integration of security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting standards and guidelines. The Federal Enterprise Architecture Segment Architecture Methodology provides guidance on integrating security requirements and security controls into enterprise architectures.

2.19.7.3 Requirement Enhancements

None

2.19.7.4 References

NIST SP 800-53r3	PM-7
CAG	CC-16
API 1164r2	7, Annex B.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.8 Critical Infrastructure Plan

2.19.8.1 Requirement

The organization addresses security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

2.19.8.2 Supplemental Guidance

The critical infrastructure and key resources protection plan is consistent with applicable laws, directives, policies, regulations, standards, and guidance.

2.19.8.3 Requirement Enhancements

None

2.19.8.4 References

NIST SP 800-53r3	PM-8
API 1164r2	4
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.9 Risk Management Strategy

2.19.9.1 Requirement

The organization:

1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the nation associated with the operation and use of systems
2. Implements that strategy consistently across the organization.

2.19.9.2 Supplemental Guidance

An organization-wide risk management strategy should include an unambiguous expression of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy.

2.19.9.3 Requirement Enhancements

None

2.19.9.4 References

NIST SP 800-53r3	PM-9
API 1164r2	3.3
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.10 Security Authorization Process

2.19.10.1 Requirement

The organization:

1. Manages (i.e., documents, tracks, and reports) the security state of organizational systems through security authorization processes
2. Fully integrates the security authorization processes into an organization-wide risk management strategy.

2.19.10.2 Supplemental Guidance

The security authorization process for systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines.

2.19.10.3 Requirement Enhancements

None

2.19.10.4 References

NIST SP 800-53r3	PM-10
API 1164r2	7.3, Annex B. 2.1, Annex B.5.1
NERC CIPS	CIP 002-3 through CIP 009-3

2.19.11 Mission/Business Process Definition

2.19.11.1 Requirement

The organization:

1. Defines mission/business processes with consideration for security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the nation
2. Determines protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

2.19.11.2 Supplemental Guidance

Protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the nation through the compromise of information (i.e., loss of confidentiality, integrity, or

availability). Inherent in defining an organization's protection needs is an understanding of the level of adverse impact that could result if a compromise occurs and, therefore, a categorization of information in accordance with FIPS 199. Modeling and simulation techniques can help in discerning the security ramification in mission/business process definitions.

2.19.11.3 Requirement Enhancements

None

2.19.11.4 References

NIST SP 800-53r3	PM-11
API 1164r2	Annex A, Annex B.1.1
NERC CIPS	CIP 002-3 through CIP 009-3

3. CONCLUSIONS

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

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 definitions and deployment intricacies, and therefore, all recommendation may not be appropriate. In particular, definitions and institutional operations drive the language and structure of many diverse standards and guidelines, yet the convergence and similarities of industrial cybersecurity is undeniable. Various guidelines and standards cannot be compared using control family titles only, as several standards and guidelines address similar security concerns in different areas, and typically within the context of related control families. Both the CAG and RG5.71 tend to do this, in that on first look, it appears security controls may not have been addressed. In fact, they have been extensively addressed, within several control families (examples would be “roles and responsibilities,” “document retention times” and “access control.” Each of these families are widely addressed within other controls, as roles and responsibilities, document retention times and access controls change with the subject matter (i.e., visitor control, configuration management, incident control).

These recommendations should be reviewed periodically to stay abreast of changing control system technologies, standards, guidelines, and cybersecurity threats to the industry. These recommendations address control system problems of a general nature. Implementing all these controls cannot guarantee absolute safety and security against cyber threats, as the dynamic nature of threats define defense as always lagging the offensive nature of malware. However, judicious adoption of the control system elements and defenses to harden existing ICSs must be made in the attempt to protect CIKR. The recommendations presented in this document can and should be customized by standards bodies representing each particular industry and business. Local, state, and federal laws and regulations should be reviewed as having precedence with respect to each particular industry and control system deployment.

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 explicitly to 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 exclude separately accredited systems, to which the control system is connected. Synonymous with the term security perimeter defined in Committee on National Security Systems (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.

Term	Definition
Authorization	The right or a permission that is granted to a system entity to access a control 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 on 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 that is available to allow continued 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 cableless connections between devices.
Boundary Protection	Methods to protect and/or isolate the ICS from IT Business systems and outside internet capable systems.
Business Network	An organization's data communications network used for general purpose business activities, typically connecting a wide variety of noncritical 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 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.

Term	Definition
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 critical function(s) within a predetermined time after a disaster or disruption.
Control System	A set of hardware and software acting in concert that manages 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.
Covert Channel Analysis	A method to covertly analyze and identify aspects of system communication that are potential avenues for covert storage, timing channels, and unauthorized information.
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	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.

Term	Definition
Cybersecurity	The protection of digital systems and their support systems from threats of: Cyberspace attack by adversaries who wish to disable or manipulate them. Physical attack by adversaries who wish to disable or manipulate them. 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. A cyberspace attack may be mounted to obtain sensitive information to plan a future physical or cyberspace attack.
Cybersecurity Incident	Any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.
Data	A common term used to indicate the basic elements that can be processed or produced by a computer.
Demilitarized Zone	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	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 that, when properly implemented, provides the services of origin authentication, data integrity, and signer nonrepudiation.
Distributed Control Systems	A distributed control system is a type of plant automation system similar to a SCADA system, except that a distributed control system 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 composed 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.

Term	Definition
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. Several firewall screening methods are available; a simple one is to screen requests to make sure they come from an acceptable (previously identified) domain name and IP address on known ports. For mobile users, firewalls may allow remote access to the private network using secure logon procedures and authentication mechanisms.
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.
Heterogeneity	Increasing the diversity of information technologies within the information system reduces the impact of exploitation from a specific technology.
Honeypots	Devices and/or techniques designed to actively seek out, monitor, and log malicious code and exploits in the internet in a secure configuration by posing as unprotected cyber clients.
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.

Term	Definition
Information Technology (IT)	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. 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 within the electronic perimeter, while providing services to the organization.
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 or distributed denial of service if multiple attackers are involved.
Intrusion	Unauthorized act of bypassing the security boundaries of a system.
Intrusion Detection (IDet)	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).
IPSec	Short for "IP Security," a set of protocols developed by the Internet Engineering Task Force 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.
ISA	International Society of Automation – Industrial Automation Controls System standards group, associated with ANSI and IEC.
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.

Term	Definition
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.
Least Privilege	The concept of "Least Privilege" is to grant users only those permissions they need to operate and function. This reduces and eliminates the introduction of rouge or malware into cyber systems.
Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the availability, integrity, or confidentiality of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host, spyware, and some forms of adware (extortionware) are also examples of malicious code.
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.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
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. Typically used in configuration or alert pop-ups in gui interfaces.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Devices	Portable cartridge/disk-based, removable storage media (floppy disks, CDs, tape, USB flash drives, external hard drives, and other flash memory cards (SD)/drives that contain nonvolatile memory) or portable computing and communications device with information storage capability (notebook computers, personal digital assistants, cellular telephones, cameras). Used for component control system configuration.
Modification	The alteration of data or information; in the adverse situation, the alteration results in a condition other than intended by the originator.

Term	Definition
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 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.
Network Disconnect	The cyber system terminates a network connection at the end of a session or after a period of inactivity.
Nonrepudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information and receiving a message.
Operator	The person who initiates and monitors the operation of a computer or process.
Organization	An administrative and functional structure that pursues collective goals, that manages its own performance, and that 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 include 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 has become synonymous with fixing security vulnerabilities.
Penetration Testing	A test methodology in which assessors, using all available documentation (system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Periodically	An amount of time not to exceed 1 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.

Term	Definition
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.
Predictable Failure Prevention	Mean time between failure rates are defendable and based on considerations that are installation specific, not the industry average. This provides the asset owner with a list of substitute information system components when needed and a mechanism to exchange active and standby roles of the components.
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 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.)
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	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.

Term	Definition
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).
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
Register	High speed storage within a Central Processing Unit (CPU) where data or the data's address in RAM resides when being processed. Consider adding definition for a Programmable Logic Controller 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.
Risk	A measure combining the severity and likelihood of harm from an event. Alternatively, the likelihood of an adverse outcome: Risk = L × P × C, L is the likelihood of attack and 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.
Risk Assessment	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.
Risk Management	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 because of laws, directives, policies, or regulations.
Role	A set of transactions that a user or set of users can perform within the context of an organization.

Term	Definition
Role-based Access Control	Access control based on user roles (a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Router	A network layer device that sends traffic on the quickest route to reach its destination.
Safeguards	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.
Sanitization	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
SCADA System	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.
Secret Key	A cryptographic parameter held private by one or more entities to limit the ability to communicate or access that group or entity.
Security	Protection against threats and attacks.
Security Category	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.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Label	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.
Security Performance	Security performance may be evaluated in terms of a program's compliance, completeness of measures to provide specific threat protection, postcompromise 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 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.

Term	Definition
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 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" and 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.
Six-wall border	This refers to a physical, completely enclosed border such as a room, cage, safe or metal cabinet. Raised floors and drop ceilings may not constitute part of a border because they could create potentially uncontrolled access points.

Term	Definition
Software	A set of programs, procedures, rules, and possibly associated documentation concerned with the operation of a computer system compilers, library routines, manuals, circuit diagrams.
Spam	Unsolicited and often unwanted e-mail.
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.
Supply Chain Protection	A supply chain is a system of organizations, people activities, information, and resources that provides products and/or services to consumers. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those informational systems.
Switch	A network device that interconnects devices and creates separate paths for communication.
System	An assembly of procedures, processes, methods, routines, or techniques united by some form of regulated interaction to form an organized whole. An assemblage of equipment, machines, or control devices, interconnected mechanically, hydraulically, pneumatically or electrically, and intended to act together to perform a predetermined function. A combination of generation, transmission, and distribution components.
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.

Term	Definition
Thin Nodes	Information system that employs processing components that have minimal functionality and data storage.
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 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.
Trustworthiness	Defined in degrees of correctness for intended functionality and the degree of resilience to attach by explicitly identified levels of adversary capability. This is defined on different levels on a basis of component-by-component, subsystem-by-subsystem, function-by-function or a combination.
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 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, a number of systems 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 and tools were reviewed or referenced in the preparation of this catalog. Some of these documents are still in draft stage or do not apply directly to control systems. Other references are not standards, but very informative guidelines or implementation guidance documents containing timely and useful information for improving the security of ICSs. An attempt has been made to organize these references with respect to the DHS critical Infrastructure sectors. Some of the references listed below may be proprietary, designed for licensed in-house usage, and may be obtained via purchase or specific individual request. All the documents listed below are listed for user awareness. The contents of proprietary/licensed documents are not used in this document unless expressed written permission of the originator/publisher was received. Several documents such as the multiple NIST Publications, DHS publications, NERC documents, and various open source documents are freely available; and some of the content was included in the creation of this document.

General:

American National Standards Institute/Instrumentation, Systems, and Automation Society Technical Report (ANSI/ISA-TR99.00.01-2007), Security Technologies for Manufacturing and Control Systems, 2007. http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9665

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, April 12, 2004. http://www.isa.org/Template.cfm?Section=Find_Standards&Template=/Customsource/ISA/Standards/TaggedStandardsCommittee.cfm&id=4296

Department of Homeland Security, National Cyber Security Division, Control System Security Program, Cyber Security Evaluation Tool, Release 3.0. http://www.us-cert.gov/control_systems/pdf/CSET_fact_sheet.pdf

Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," issued May 25, 2001, updated December 03, 2002. FIPS-140-3 is a DRAFT Security Requirements for Cryptographic Modules and is still in draft form. FIPS 140-2 also contains the following four annexes:

A – January 4, 2011, Draft "Approved Security Functions for FIPS Pub 140-2"

B – June 14, 2007, Draft "Approved Protection Profiles for FIPS PUB 140-2"

C – November 24, 2010, Draft "Approved Random Number Generators for FIPS PUB 140-2"

D – January 4, 2011, Draft "Approved Key Establishment Techniques for FIPS PUB 140-2."

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Federal Information Processing Standards Publication 180-3, "Secure Hash Standards," issued October 2008. http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

Federal Information Processing Standards Publication 198-1, "The Keyed-Hash Message Authentication Code (HMAS)," issued July 2008. http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

International Electrotechnical Commission 62351-1, "Data and Communication Security," Committee Draft Version 1, April 2005.

International Electrotechnical Commission 62443-2-1, "Industrial Communication Networks – Network and System Security":

Part 1-1: "Terminology, concepts and models," July 2009

Part 2-1: "Establishing an industrial automation and control system security program," November 2010

Part 3-1: "Security technologies for industrial automation and control systems," July 2009

Part 3-3: "

http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/43215

http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=pro-det.p&He=IEC&Pu=62443&Pa=2&Se=1&Am=&Fr=&TR=&Ed=1"

International Organization for Standardization 17799, "Code of Practice for Information Security Management," June 10, 2005. (Note: This document has been superseded by ISO/IEC 27002:2005, Stage 90.92, April 2008.)

International Organization for Standardization 27001, "Information Security Management Systems Requirements," October 14, 2005.

International Society of Automation Society Standards Committee, ANSI/ISA-99.00.01-2007, "Manufacturing and Control Systems Security Part 1: Concepts, Models and Terminology," October 29, 2007.

International Society of Automation Standards Committee, ANSI/ISA-99.02.01-2009, "Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program," January 13, 2009.

National Institute of Standards and Technology Special Publication 800-48, "Wireless Network Security 802.1, Bluetooth and Handheld Devices," Revision 1, September 2008. http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

National Institute of Standards and Technology Special Publication 800-53, "Recommended Security Controls for Federal Information Systems," Revision 3 Final, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Institute of Standards and Technology Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," Final Public Draft, September 2008. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

National Institute of Standards and Technology Special Publication 800-127, "Guide to Securing WiMAX Wireless Communications," September 2010. http://csrc.nist.gov/publications/nistpubs/800-127/sp800-127.pdf

"Twenty Critical Controls for Effective Cyber Defense: Consensus Audit," Version 2.3, November 13, 2009. http://www.sans.org/critical-security-controls/print.php http://www.sans.org/whatworks/20-critical-controls-poster-122010.pdf

WIB, "Process Control Domain-Security Requirements for Vendors: Plant Security," second issue, M2784-X-10, Version 2.0, Evaluation International (EI), WIB and EXERA, October 2010. http://www.wib.nl/

Chemical:

Chemical Information Technology Council (ChemITC), Guidance for Cyber Security in Chemistry, Version 4.0, November 2009.

Department of Homeland Security – Office of Infrastructure Protection – Infrastructure Security Compliance Division – "Risk-Based Performance Standards Guidance (RBPS)– Chemical Facility Anti-Terrorism Standards," Version 2.4 May 2009. http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

Electric Power:

Institute of Electrical and Electronics Engineers 1402, "Guide for Electric Power Substation Physical and Electronic Security," January 30, 2000.

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 1, Smart Grid Cyber Security Strategy, Architeture, and High-Level Requirements," August 2010. http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 2, Privacy and the Smart Grid," August 2010. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

National Institute of Standards and Technology Interagency Report (NISTIR) 7628, "Guidelines for Smart Grid Cyber Security: Volume 3, Smart Grid Cyber Security: Supportive Analyses and References," August 2010. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-3 through CIP 009-3), Approved by Board of Trustees: December 16, 2009. http://www.nerc.com/page.php?cid=2%7C20

North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-4 through CIP 009-4), approved draft (Phase II), which involves the more complex FERC directives. These drafts have not yet been submitted to the NERC Board of Trustees for approval at the time of writing.

North American Electric Reliability Council, Security Guidelines for the Electricity Sector, Version 1.0, June 14, 2002.

Gas:

American Gas Association, "Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (AGA 12, Part 1)," March 14, 2006.

American Gas Association, "Cryptographic Protection of SCADA Communications Part 2: Retrofit link encryption for asynchronous serial communications (AGA 12, Part 2)," March 31, 2006.

Nuclear:

Department of Energy DOE O 205.1A "Department of Energy Cyber Security Management," December 4, 2006. http://cio.energy.gov/policy-guidance/doe_policies.htm

Department of Energy DOE M 205.1-4, "National Security System Manual," March 8, 2007. http://cio.energy.gov/policy-guidance/doe_policies.html

Department of Energy DOE M 205.1-5, "Cyber Security Process Requirements Manual."

Department of Energy DOE M 205.1-6, "Media Sanitization Manual," December 23, 2008.

Department of Energy DOE M 205.1-7, "Security Controls for Unclassified Information Systems Manual," January 5, 2009.

Department of Energy DOE M 205.1-8, "Cyber Security Incident Management Manual," January 8, 2009.

Nuclear Energy Institute "Cyber Security Plan for Nuclear Power Reactors," NEI 08-09, Revision 6, April 2010.

U.S. Nuclear Regulatory Commission – Regulatory Guide 5.71 "Cyber Security Programs for Nuclear Facilities," January 2010. http://nrc-stp.ornl.gov/slo/regguide571.pdf

Oil and Petroleum:

American Petroleum Institute, "API 1164: Pipeline SCADA Security, Second Edition," June 2009.

American Petroleum Institute, "Security Guidelines for the Petroleum Industry," April 2005.

Transportation:

American Public Transit Association "Securing Control and Communications Systems in Transit Environments – Part 1: Elements, Organization and Risk Assessment/Management," APTA RP-CCS-1-RT-001-10, July 2010.

Department of Transportation – Federal Transit Administration - 49 CFR, Part 659, Rail Fixed Guideway Systems; State Safety Oversight, April 2005 – This document authorizes 26 individual states authorization to implement and manage 43 separate rail transit agencies. http://transit-safety.fta.dot.gov/Publications/order/singledoc.asp?docid=603

Appendix A

Cross Reference of Standards

This cross reference mapping loosely correlates the requirements and guidance contained in the referenced source documents against the recommendations in the Catalog of Control Systems Security. This correlation depicts a general relationship between multiple documents in multiple industrial sectors. The cross reference cannot imply an exact matching between specific requirement details and multiple controls currently existing, but strives to implicitly address and associate specific controls across several standards and guidance documents.

The source documents in the cross reference are constantly evolving to address new and expanded understanding of security topics. Previous source documents have been deleted from this document as they are no longer relevant, or have been superseded by newer documents. This crosswalk attempts to use the most recent update of the source documents available at the time of publication, but availability, publishing and timing may result in older versions of source documents being referenced and used. Furthermore, it is not possible to determine the priority and baseline risk for each control family in every industrial facility and control system deployment.

Two reference sources were removed from the cross reference at this time. They are: (1) ChemITC—"Guidance for Addressing Cybersecurity in the Chemical Sector, Version 3.0; Chemical Sector Cyber Security Program May 2006"; This document has been superseded by "Guidance for Addressing Cyber Security in the Chemical Industry, Version 4, November 2009," and has not yet been reviewed; and (2) "NERC Security Guidelines—Security Guidelines for the Electricity Sector, Version 1.0 May 3, 2005," has been superseded by the NERC Critical Infrastructure Protection (CIP) reliability standards.

Two new additional reference sources were added at this time. They are (1) "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)," Version 2.3 November 13, 2009, and (2) U.S. Nuclear Regulatory Commission—Regulatory Guide 5.71—"Cyber Security Programs for Nuclear Facilities," January 2010. These two sources were added, as they are the latest cybersecurity standards released and provide a very good basis in industrial cybersecurity. The CAG, for instance, is broken down into four categories within each of the 20 critical controls. The first category is label "QW," which denotes a "quick win," action that will immediately improve the security posture, especially if addressed by the user. The second category is "Improved Visibility and Attribution," meant to increase monitoring, visibility and attribution, so organizations can better monitor network and computer systems. The third category is "Hardened Configuration and Improved Information Security Hygiene," and focuses on protecting against poor security practices by system administrators and end users. The final category is "Advanced" and identifies actions and items that further improve security beyond the other three categories. The CAG also lists functional/effectiveness testing to see how and if security functions are working. The NRC RG 5.71 takes elements from NIST SP 800-53 r3 and NIST SP 800-82 and focuses on how to use these elements in the operation of nuclear reactors. Most ICSs share similar layout, function and security. Three appendixes are in NRC 5.71. Appendix A is a generic Cyber Security Plan template for utilities to use. Appendix B contains Technical Security Controls, while Appendix C consists of Operational and Management Security Controls. The unique method on which roles, configuration, what to test, how to test, and periodic retesting provides an element lacking in current cybersecurity standards and guidelines.

The cross reference is accurate at the time of the most recent update. The reader is encouraged to confirm the currency, accuracy, and applicability of the source documents and obtain current copies of all