Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

How to Implement Security Controls for an Information Security Program at CBRN Facilities

With the support of

United Nations
Interregional Crime and Justice
Research Institute

Action Implemented by

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Funded by the European Union

CBRN Centres of Excellence
An initiative of the European Union

UNICRI Project 19

How to Implement Security Controls for an Information Security Program at CBRN Facilities

Prepared by the Pacific Northwest National Laboratory within the framework of the Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE) entitled:

“Development of procedures and guidelines to crate and improve security information management systems and data exchange mechanisms for CBRN materials under regulatory control.”

December 2015

unicri
United Nations
Interregional Crime and Justice
Research Institute

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

The document has been produced with the assistance of the EU. The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

The contents of this document do not necessarily reflect the views or policies of the United Nations, UNICRI or contributory organizations, or do they imply any endorsement. While reasonable efforts have been made to ensure that the contents of this document are factually correct and properly referenced, UNICRI does not accept responsibility for the accuracy or completeness of the contents, and shall not be liable for any loss or damage that may be occasioned directly or indirectly through the use of, or reliance on, the contents of this publication. The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI concerning the legal status of any country, territory or boundaries. This publication has not been formally edited by UNICRI.

Summary

Information assets, including data and information systems, need to be protected from security threats. To protect their information assets, chemical, biological, radiological, and nuclear (CBRN) facilities need to design, implement, and maintain an information security program.

The guidance provided in this document is based on international standards, best practices, and the experience of the information security, cyber security, and physical security experts on the document writing team. The document was developed within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative.

This document is the third in a series of three documents produced by Project 19. The first document in the series, *Information Security Best Practices for CBRN Facilities,*[1] provides recommendations on best practices for information security and high-value security controls. The second document in the series, *Information Security Management System Planning for CBRN Facilities*[2] focuses on information security planning. It describes a risk-based approach for planning information security programs based on the sensitivity of the data developed, processed, communicated, and stored on facility information systems.

This document is designed to assist CBRN facilities in developing a comprehensive set of security controls to support the implementation of a risk-based, cost-effective information security program. A security control is a "safeguard or countermeasure…designed to protect the confidentiality, integrity, and availability" of an information asset or system and "meet a set of defined security requirements." (NIST 2013). Security controls cover management, operational, and technical actions that are designed to deter, delay, detect, deny, or mitigate malicious attacks and other threats to information systems. The protection of information involves the application of a comprehensive set of security controls that addresses cyber security (i.e., computer security), physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, and environmental controls). The application of security controls is at the heart of an information security management system (ISMS). The selection and application of specific security controls is guided by a facility's information security plans and associated policies.

Not all facilities can afford to purchase, install, operate, and maintain expensive security controls and related systems; therefore, decisions on the application of security controls have to balance considerations of security risk and resource constraints. When resources are limited, investments in security controls should focus on implementing a set of controls that provide the greatest overall risk reduction given the

[1] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. Information Security Best Practices for CBRN Facilities. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

[2] UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. *Information Security Management System Planning for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute, Turin, Italy.

available resources. In this document, security controls are proposed for the following information security planning topic areas:

- Risk Assessment
- Risk Response
- Risk Monitoring
- Business Environment
- Asset Management
- Security Control Implementation
- Configuration Management
- Contingency Planning and Disaster Recovery
- Incident Response
- Monitoring and Auditing
- Awareness and Training.

For each topic area, security controls are presented along with the minimum risk level for the information system at which the listed security control should be applied. Also provided for each security control are a summary rationale and its publicly available source. The major sources used are the *Guide to Developing a Cyber Security and Risk Mitigation Plan*[1] and *Critical Security Controls for Effective Cyber Defense*, Version 5[2].

After reviewing the various security control options, a facility should select and implement an appropriate set of security controls based on risk levels and resource constraint. These security controls should then be tracked to ensure they are appropriately used and maintained, and that the associated responsibilities, assignments, deliverables, and deadlines are documented.

[1] NRECA - National Rural Electric Cooperative Association. 2014a. "Guide to Developing a Cyber Security and Risk Mitigation Plan". NRECA / Cooperative Research Network Smart Grid Demonstration Project. Arlington, Virginia. Available by using the download tool at https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx. Accessed November 23, 2015.

[2] Council on Cyber Security. 2015. "Critical Security Controls for Effective Cyber Defense, Version 5." Accessed November 23, 2015 at http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-critical-security-controls.pdf?epslanguage=en-gb.

Acknowledgments

This document was prepared by a team of cyber and information security researchers from the Pacific Northwest National Laboratory in the United States, the National Nuclear Laboratory in the United Kingdom, and the University of Glasgow in the United Kingdom. The U.S.-based members of the team are:

Joseph Lenaeus
Pacific Northwest National Laboratory

Lori Ross O'Neil
Pacific Northwest National Laboratory

Rosalyn Leitch
Pacific Northwest National Laboratory

Cliff Glantz
Pacific Northwest National Laboratory

Guy Landine
Pacific Northwest National Laboratory

Janet Bryant
Pacific Northwest National Laboratory

The European-based members of the team:

John Lewis
National Nuclear Laboratory

Gemma Mathers
National Nuclear Laboratory

Robert Rodger
National Nuclear Laboratory

Christopher Johnson
University of Glasgow

The document's technical editor was Cornelia Brim (Pacific Northwest National Laboratory). Administrative and management support was provided by Emily Davis, Josh Byrd, Monica Chavez, and Keith Freier (all of Pacific Northwest National Laboratory), and other members of the authors' organizations.

This document was produced within the scope of Project 19 of the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

Special thanks to Odhran McCarthy and the staff at the United Nations Interregional Crime and Justice Research Institute for their support, patience, and technical guidance during this project.

Acronyms and Abbreviations

AES	Advanced Encryption Standard
ASD	Australian Signals Directorate
CA	certificate authority
CBRN	chemical, biological, radiological, and nuclear
CoE	Centres of Excellence
CSC	Critical Security Control
DHCP	dynamic host configuration protocol
DMZ	demilitarized zone
DNS	domain name service
EPRI	Electric Power Research Institute
ESCSWG	Energy Sector Control System Working Group
FTP	file transfer protocol
ID	identification
IDS	intrusion detection system
IEEE	Institute for Electrical and Electronics Engineers
IP	Internet protocol
IPS	intrusion protection system
IPsec	Internet protocol security
ISMS	information security management system
IT	information technology
NIST	U.S. National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
PKI	public key infrastructure
SDLC	software development life cycle
SIEM	security information and event management
SPF	sender policy framework
SQL	Structured Query Language
TCP	transmission control protocol
TLS	transport layer security
UNICRI	United Nations Interregional Crime and Justice Research Institute
URL	uniform resource locator
USB	universal serial bus
UTC	Coordinate Universal Time
VLAN	virtual local area network
VPN	virtual private network

WPA2	Wi-Fi Protection Access 2
XML	extensible markup language

Contents

Tables

1.0 Introduction

This document is designed to assist facilities in developing a comprehensive set of security controls to support the implementation of a risk-based, cost-effective information security program. In particular, this guidance is intended for facilities that are tasked with creating, using, storing, or disposing of chemical, biological, radiological, and nuclear (CBRN) materials. This document may be used by information security managers, planners, designers, operators, and other workers at CBRN facilities and their contractors (including suppliers). It may be used by managers and information security personnel with parent organizations that have supervisory responsibilities for CBRN facilities. It may also be used by competent authorities that have regulatory responsibilities for CBRN facilities. While the guidance provided in this document is specifically provided for the context of CBRN facilities, it may also support information security at other types of facilities (i.e., those that do not involve CBRN materials, such as facilities that support critical infrastructure or provide business functions that involve sensitive information).

A security control is a "safeguard or countermeasure… designed to protect the confidentiality, integrity, and availability" of an information asset or system and "meet a set of defined security requirements." (NIST 2013). Security controls cover management, operational, and technical actions that are designed to deter, delay, detect, deny, or mitigate malicious attacks and other threats to information systems. The protection of information involves the application of a comprehensive set of security controls that address cyber security (i.e., computer security), physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, environmental controls). The application of security controls is at the heart of an information security management system (ISMS). The selection and application of specific security controls are directed by a facility's information security plans and policies.

The guidance provided in this document for information security controls is presented from a risk management perspective. Not all facilities can afford to purchase, install, operate, and maintain expensive security controls and related systems; therefore, decisions on the application of security controls have to balance considerations of security risk and resource constraints. When resources are limited, investments in security controls should focus on implementing a comprehensive set of controls that provide the greatest overall risk reduction given the available resources.

In this document, the reader will be introduced to risk-based security controls that are associated with each of the information security plans or planning components that are used to develop and implement an ISMS. These include three risk management components and eight other security components. The risk management components cover:

- Risk Assessment
- Risk Response
- Risk Monitoring.

The other security components cover:

- Business Environment
- Asset Management
- Security Control Implementation
- Configuration Management
- Contingency Planning and Disaster Recovery
- Incident Response
- Monitoring and Auditing
- Awareness and Training.

1.1 Document Context

This document is the third in a series of three information security guidance documents produced within the framework of Project 19 of the European Union CBRN Risk Mitigation Centres of Excellence Initiative. The initiative is implemented in cooperation with the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the European Commission Joint Research Center. The initiative is developed with the technical support of relevant international and regional organizations, the European Union Member States and other stakeholders, through coherent and effective cooperation at the national, regional, and international level.

The objective of Project 19 is to provide guidance on the security of information technology (IT) structures and data exchange mechanisms for CBRN facilities. This includes providing information on the management, operational, and technical security controls needed to address threats, characterize adversaries, identify vulnerabilities, and enhance defense and mitigation capabilities. The key objective of the project is to help CBRN security managers, IT/cyber security managers, and other decision makers typically involved in acquiring, auditing, regulating, and disposing of information to develop and implement appropriate and cost-effective information security programs.

The first of the three documents in the Project 19 Information Security series is *Information Security Best Practices for CBRN Facilities* (UNICRI 2015a) and is referred to as the “Best Practices” document. This document provides a high-level description of the best practices that support the development of an effective information security program. It provides a description of high-value security controls. The second document in the series, *Information Security Management System Planning for CBRN Facilities* (UNICRI 2015b), is referred to as the “ISMS Planning” document. It provides guidance for developing information security planning documents that establish information security roles, responsibilities, and policies.

In addition to the three documents, a two-day teach-the-teacher workshop on information security for CBRN facilities has been prepared. That workshop is designed to introduce the need for information security to CBRN facility decision makers and others with oversight responsibilities for CBRN materials and facilities.

1.2 Understanding Security Controls

It is often helpful to illustrate the concept of security controls for information systems by using a comparable physical security example. Think of a current-day information security program as being analogous to the security program of a castle in the Middle Ages. Like modern information security programs, castles relied on management, operational, and technical security controls to defend themselves from attackers.

Examples of management and operational security controls within the castle included: assigning roles and responsibilities for various security activities, hiring and training soldiers, providing assignments and schedules for members of the castle defense force, purchasing armaments, developing and implementing procedures for allowing visitors to enter the castle, conducting security inspections of castle defenses to identify potential vulnerabilities, characterizing the attack capabilities of potential adversaries, inspecting defenses for vulnerabilities, and maintaining communication with neighboring castles to provide each other with timely notification of attacks.

At the Middle Ages castle, technical security controls were designed and implemented. Examples include the design, construction, and operation of a water-filled moat; a drawbridge over the moat to restrict access to the castle gate and walls; high and thick castle walls; and a massive iron gate to block attackers from entering the interior of the castle. These and other technical security controls form the defensive architecture of the castle.

Many security controls for information systems serve analogous functions to those employed for castle defense. For example, management and operational security controls govern the assignment of information security roles and responsibilities, the hiring and training of staff to address information security issues, assigning staff to perform information security monitoring activities, conducting information security vulnerability assessments, procuring information system hardware and software, developing and implementing access control and authentication procedures, characterizing the attack capabilities of potential adversaries, identifying security vulnerabilities, and maintaining communication with applicable government, organization, and CBRN industry colleagues to provide timely notification of attacks.

Similarly, modern information security programs design and implement technical security controls. Examples include the design, implementation, and operation of multiple defensive layers within the facility's IT structure, firewalls to stop unauthorized access and communications, demilitarized zones (DMZs) or perimeter networks to securely exchange data with other systems, intrusion detection systems to detect unauthorized access, automated monitoring to detect attacks, and the elimination of backdoor entrances into the information system.

1.3 Source of Security Controls

The guidance provided in this document is informed by a number of generally accepted standards and guidance documents. The security controls we present were gleaned from several no-cost, publicly available, and widely accepted information security sources including:

- Council on Cyber Security*, Critical Security Controls for Effective Cyber Defense, Version 5* (Council on Cyber Security 2015)

- Australian Signals Directorate, *'Top 4' Strategies to Mitigate Targeted Cyber Intrusions Mandatory Requirements Explained* (ASD 2013)
- National Rural Electric Cooperative Association, *Guide to Developing a Cyber Security and Risk Mitigation Plan and Cyber Security Plan* (NRECA 2014a).

1.4 Using this Document to Select Security Controls

This document can be used concurrently with its companion the ISMS-Planning document (UNICRI 2015b) to identify general facility security strategies and then to choose specific security controls that meet the facility's needs and goals.

In Sections 2 and 3 of this document, potential security controls are presented to cover a range of information security program topics. Each topic area includes a checklist (in table form) summarizing the various security best practices and controls that a facility should consider for implementation, based on the risk level of the facility and the available resources. After reviewing the various security control options presented in the checklist, including consulting the references provided to gather more information, the facility should select and implement an appropriate set of security controls based on risk levels and resource constraints. These security controls should then be tracked to ensure they are appropriately used and maintained and that associated responsibilities, assignments, deliverables, and deadlines are documented.

Once the security controls are in place, they should undergo a thorough, periodic review (e.g., every 1-3 years) as part of the information security program review. As risks evolve and available resources for information security change, the checklists in this document should be reevaluated to determine if more rigorous security controls are required. In some cases, where risks or available resources decrease, a less rigorous set of controls might be appropriate to maintain an adequate level of information security.

1.5 Using the Security Control Checklists

Each subsection in Sections 2 and 3 includes a "checklist" table that provides guidance on the types of risk-based security controls to implement for the pertinent information security component. Table 1.1 provides a simple example to illustrate how to use these tables.

Table 1.1. A Sample Checklist Table

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Monitor and assess the effectiveness of controls.	Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate perceived risks.	NRECA Cyber Security Plan 8
Choose an item.	L	Establish internal and external information sources for threat intelligence and vulnerability data, monitoring them regularly and taking appropriate action for high-priority items.	Build operational awareness of threats and vulnerabilities, allowing the facility to address high-priority items.	NRECA Cyber Security Plan 32
Choose an item.	L	Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.	Maintains ongoing understanding of the effectiveness of the facility's security control versus threats facing the facility.	NRECA Cyber Security Plan 33
Choose an item.	L	Review and update the facility's threat model at regular intervals. Log any changes in a formal risk register.	Ensures that the facility's threat model remains relevant.	NRECA Cyber Security Plan 43

Table 1-1 consists of five columns:

- "✓" – This column is provided so that the facility can indicate that it has, has partially, or has not selected the listed security control.

- L/M/H – Denotes the minimum risk level for the information system at which the listed security control should be applied. Three risk levels are offered (i.e., L=Low, M=Medium, and H=High). The facility should customize its definition of the risk level. In Section 2.0 of the ISMS Planning document (UNICRI 2015b), four different classifications of information are discussed: unrestricted, restricted, confidential, and secret. Using this scheme, information systems involving unrestricted data might be designated as "Low" risk, restricted data might be "Medium" risk, and systems involving confidential or secret data or functions might be designated as "High" risk. Security controls associated with an "L" risk designation in the table level should be applied to all information systems (i.e., information systems assigned a low, medium, or high risk level). If the risk level is "M", the indicated security control should be applied to information systems designated as having a medium or high security risk. If the risk level is "H", the indicated security control should be applied to information systems designated as high risk. For all of recommended security controls, their actual implementation depends on both the applicability of the security control to the information system in question and the availability of resources to implement the security control.

- Activity/Security Control – This is a brief description of the security control or activity available for selection.

- Rationale – This is the explanation on what this security control is intended to achieve.

- Source – This is the reference for this security control. This publicly available reference should be consulted for additional information, or links to additional information, on this security control.

The security controls presented in this document are based on the NRECA's *Guide to Developing a Cyber Security and Risk Mitigation Plan* (NRECA 2014a) and *Critical Security Controls for Effective Cyber Defense, Version 5* (Council on Cyber Security 2015). The wording of these security controls, risk-level assignments, and the rationale provided to justify their use are taken verbatim, or with minor modifications to focus these security controls on information security and to clarify their presentation.

Security controls, and documents that present them, will evolve over time as new threats and mitigations are identified. It is recommended that the ISMS manager oversee a regular review of security control document to ensure the facility is basing their security controls on the latest set of tools and techniques.

It is important to consider timing when reviewing the recommended security controls presented in the following sections for potential implementation. Identify those controls that should be implemented immediately, those that should be implemented in the near future, and those that may need to be postponed until a later date because of resource limitations or other concerns. All recommended security controls will need to be approved by the facility's ISMS manager and other responsible decision makers. The responsibility for the implementation of individual security controls needs to be assigned within the facility. For those security controls that are selected but cannot be immediately implemented, a project plan should be developed to track their status pending future implementation.

2.0 Implementing a Risk-based Approach to the Protection of Critical Systems

When developing an information security program or an ISMS, the facility should identify their information systems and assets, determine the risks associated with these systems and assets, and evaluate methods for controlling or reducing these risks. This may include reducing the likelihood of a compromise of information security or reducing the potential consequences of such a compromise. Risk objectives should be established, documented, and approved by the facility's management.

2.1 Security Controls for Risk Assessment

In order to evaluate information security risks, and identify ways to manage and reduce these risks, a CBRN facility needs to characterize and understand the information security issues it may face.

A threat represents the motivation, capability, and opportunity of an adversary to attack or inflict harm. Motivation is the desired reason (or reasons) an individual or group has for mounting an attack. Motivation may involve political, cultural, financial, emotional, or other factors. The attacker's capability refers to the knowledge, skills, and tools necessary to conduct an attack. Opportunity represents the situational circumstances that would support the initiation of an attack. Identifying potential types of attackers (i.e., threat agents) is an initial step in performing an information security risk assessment.

Once potential threats have been identified, an information security program needs to evaluate the vulnerability of the facility's information assets to an attack. Vulnerability assessment starts with an identification of the facility's information assets and the pathways by which those assets can be compromised. Vulnerability is defined to be a weakness in the physical or electronic configuration of an asset that could allow an action that compromises the security of the asset.

Once identified, vulnerabilities can be evaluated to estimate their potential seriousness. This can be done in a graded manner. A simple approach is to evaluate the vulnerability in terms of high, medium, or low ranking. This is analogous to the information risk levels presented in this document for selecting security controls. For some facilities, a more rigorous approach might assess vulnerability in terms of the likelihood that the threat could be carried out and successfully exploit the vulnerability.

During the vulnerability assessment process, the facility should identify potential ways to mitigate the identified vulnerability and therefore reduce risks. This will be helpful in deciding how to implement appropriate security controls. The facility's security personnel should stay current on new threats and regularly assess systems for vulnerabilities that can be exploited by new threats.

In addition to identifying threats and vulnerabilities, the consequences of a successful exploitation of information security are evaluated. Consequence or impact evaluations should consider the potential loss of confidentiality (i.e., information is obtained by unauthorized individuals or organizations), loss of integrity of information (i.e., the manipulation or alteration of data), and the loss of availability of information (i.e., the inability for legitimate users to access data). Combining information on threats, vulnerabilities, and consequences provides an estimate of information security risk. The facility's risks should be documented and reviewed periodically. In particular, risks should be reassessed whenever a new and significant threat or vulnerability is identified.

Risks should be tracked by the facility in a risk inventory, sometimes called a risk registry. Table 2.1 presents security controls or activities that a facility should conduct to characterize risk.

Table 2.1. Risk Assessment

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Perform a vulnerability assessment.	Assessments of threats and weaknesses in existing security controls create the basis for estimating the potential or likelihood of successful attacks. They also help to prioritize remedial actions.	NRECA Cyber Security Plan 5
Choose an item.	L	Assess risks to system information and assets.	The risk assessment combines the potential of a successful attack with its assessed potential impact on the facility's mission and goals. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the facility.	NRECA Cyber Security Plan 6
Choose an item.	L	Track vulnerability and threat data via a formal risk register. The facility should track and manage its response to published vulnerabilities.	Activities related to vulnerability and threat management are formally documented and tracked across the facility.	NRECA Cyber Security Plan 45
Choose an item.	M	Build a threat model.	Characterizes the ways in which an adversary may try to compromise the system so that the system can be designed or reconfigured to resist such attacks.	NRECA Cyber Security Plan 50
Choose an item.	M	Perform architecture risk analysis.	Compares the system's architecture against a threat model to ensure that sufficient security controls are in place to prevent successful attacks.	NRECA Cyber Security Plan 51
Choose an item.	M	Perform risk-based security testing.	Runs through the top risks identified during the threat modeling and architecture risk analysis processes to ensure that the system has been designed and implemented in a way that mitigates these risks.	NRECA Cyber Security Plan 54

2.2 Security Controls for Mitigating and Responding to Risks

For an attack to succeed, it must exploit some inherent weakness or vulnerability contained within the target. If the vector of attack is poorly executed, or attempts to exploit a vulnerability that does not exist, the attack will likely be unsuccessful. This basic concept holds true regardless of whether the attack takes place within the physical or cyber domain.

Vulnerability mitigation seeks to address the identified weakness either through reconfiguration of the system or through the application of security controls (Table 2.2). In the case of digital systems, examples of system reconfiguration to mitigate vulnerabilities include, but are not limited to:

- Removal of unnecessary user accounts
- Removal of unneeded or default file shares
- Removal or disablement of vulnerable operating system services and ports
- Implementation of access controls on file systems, registries (if any exist), and binaries
- Implementation of encryption mechanisms.

Table 2.2. Risk Mitigation and Response Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Select security controls.	Selects appropriate and cost-effective security controls to strengthen defenses and lower security risk levels. In addition to assessed risks and costs, selection factors might include the facility's mission, environment, and culture.	NRECA Cyber Security Plan 7
Choose an item.	L	Document security requirements.	Explicitly documents security requirements of the information system so that its components can be designed, implemented, and tested to ensure that these requirements have been met.	NRECA Cyber Security Plan 49
Choose an item.	L	Assign responsibility for security risk management to a senior manager.	Assigning responsibility ensures that security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined executive with	NRECA Cyber Security Plan 9

✓	L/M/H	Activity / Security Control	Rationale	Source
			the requisite authority.	

2.3 Security Controls for Monitoring Risk

While security controls may be deployed with the intent of deterring, delaying, detecting, or denying an attack, it is extremely difficult to stop all attacks from a determined adversary without reinforcing actions. Therefore, it is imperative that a facility adequately monitor for anomalous behavior or activities that would suggest a potential breach in security is being attempted. Once an attack is detected, incident response activities can then be initiated.

Information security controls serve analogous functions. Instituting an information security program without a security monitoring program is like building a castle and failing to post guards. Without someone monitoring security at the castle, even a small attack force can leisurely fill in the moat and dig through the castle walls. The same is true for information systems; without monitoring firewalls or intrusion detection systems, facility security personnel cannot detect someone trying to break into the facility's digital networks. Because no defensive measure, or set of security controls, can resist all attacks for an indefinite period of time, actions must be taken to shore up defenses before they are under attack.

Therefore, security monitoring to protect information assets is an essential activity. Once started, monitoring may need to continue for some time to determine a baseline for normal system and user behavior. After learning the expected system behavior, anomalous behavior can be identified and investigated. This task is made much easier by having automated tools to assist with tracking, notifications, and trending. Table 2.3 provides a set of security actions needed to support monitoring.

Table 2.3. Security Monitoring

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Monitor and assess the effectiveness of security controls.	Effective testing and ongoing monitoring and evaluation can provide confidence that security controls adequately mitigate perceived risks.	NRECA Cyber Security Plan 8
Choose an item.	L	Establish internal and external information sources for threat intelligence and vulnerability data. Monitor sources and take appropriate action to address high-priority items.	Builds operational awareness of threats and vulnerabilities, allowing the facility to address high-priority items.	NRECA Cyber Security Plan 32
Choose an item.	L	Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.	Maintains ongoing understanding of the effectiveness of the facility's security control versus threats facing the facility.	NRECA Cyber Security Plan 33
Choose an	L	Review and update the facility's threat model at regular intervals, and log any changes in a formal	Ensures that the facility's threat model remains relevant.	NRECA Cyber Security Plan 43

✓	L/M/H	Activity / Security Control	Rationale	Source
item.		risk register.		

3.0 The Information Security Plan

The information security plan, or ISMS Security Plan, is the cornerstone for protecting the facility's assets and information. The following sections describe the various security controls that are associated with each component of a facility's ISMS Security Plan. A facility may choose to implement those security controls that are recommended for the risk level assigned to the information systems or supplement these with additional security controls to further enhance security. In the tables presented within each of the following subsections, first identify the risk level of the information system or assets being addressed, and then select the security controls that are applicable to that risk level. Remember that the security controls designated for low-risk systems must be applied to medium- and high-risk systems and security controls designated for medium-risk systems must be applied to high-risk systems.

3.1 Business Environment

Establishing the business environment under which your ISMS exists is the key to a successful program (Table 3.1). Having management and stakeholder buy-in is the surest path to a successful information security program. The stakeholders in question may include competent authorities (e.g., regulators), the parent organization, suppliers, contractors, and customers. As part of establishing the facility's information security program, it is important to identify and document:

- What is the mission and objectives of the ISMS?
- Who are the key stakeholders for the ISMS?
- What are the roles, responsibilities and authorities of the stakeholders and other key players?
- Are there any state, sector, legal or industry requirements that must be included as part of the ISMS?

Table 3.1. Business Environment Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Identify and classify critical information system assets.	It is important to understand the assets that may need to be protected, along with their classification (e.g., unrestricted information, or secret information). That way, an informed decision can be made as to the controls needed to protect these assets, commensurate with risk severity and impact on the business.	NRECA Cyber Security Plan 2

Table 3.1. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Provide active executive sponsorship.	Active and visible support from executive management at each stage of planning, deploying, and monitoring security efforts is crucial to success.	NRECA Cyber Security Plan 3
Choose an item.	L	Identify and analyze the electronic security perimeter(s).	To build a threat model, it is important to understand the entry points that an adversary may use to gain access to the facility's assets. The threat model then becomes an important component of the risk assessment.	NRECA Cyber Security Plan 4
Choose an item.	L	Assign responsibility for developing, implementing, and enforcing cyber security policy to a senior manager. Ensure that the senior manager has the requisite authority across departments to enforce the policy.	The development and implementation of effective security policies, plans, and procedures require the collaborative input and efforts of stakeholders in many departments of the facility. Assigning a senior manager to organize and drive the efforts, with the authority to make and enforce decisions at each stage, raises the chances of success.	NRECA Cyber Security Plan 13
Choose an item.	L	Identify security aspects to be governed by defined policies.	An effective security program requires policies and procedures that address a wide range of management, personnel, operational, and technical issues.	NRECA Cyber Security Plan 14
Choose an item.	L	Document a brief, clear, high-level policy statement for each issue identified.	The high-level policy statements express three things: • The commitment of the facility management's to the cyber security program • The high-level direction and requirements for plans and procedures • A framework to organize lower-level documents.	NRECA Cyber Security Plan 15

Table 3.1. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Reference lower-level policy documents.	Lower-level policies, plans, and procedures provide the details needed to put policy into practice.	NRECA Cyber Security Plan 16
Choose an item.	L	Define the implementation plan and enforcement mechanisms.	A careful rollout of the program, well-documented policies that are accessible to the personnel they affect, and clearly communicated consequences of violating policies will help ensure compliance.	NRECA Cyber Security Plan 17
Choose an item.	L	Define a policy management plan.	This will help maximize compliance by providing mechanisms to: • Request, approve, document, and monitor policy exceptions. • Request, approve, implement, and communicate changes to policies, plans, and procedures.	NRECA Cyber Security Plan 18
Choose an item.	L	Appoint a senior security manager with a clear mandate.	The responsibility for security must be assigned to a specific individual.	NRECA Cyber Security Plan 148
Choose an item.	M	Review the information security program regularly, and validate achieved milestones by an independent third party.	Ensure that external experts agree with the facility's assessment of its information security posture and program performance.	NRECA Cyber Security Plan 19

3.2 Asset Management

Asset management is intended to first identify all hardware, software, systems, and data that support a facility's information systems. Once that baseline is completed, regular audits and assessments should be conducted periodically (e.g., on an annual or biannual basis). This is to ensure that the system is operating as designed and approved.

There are many ways to perform an asset inventory and tracking, such as using automated tools or manual inspections. Most facilities will benefit from a combination of these two approaches. Once a baseline inventory is completed, the effort required to maintain and update the asset inventory is greatly reduced.

Table 3.2 provides the recommended security controls for asset management.

Table 3.2. Asset Management Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the facility's network.	An asset inventory is critical as the facility cannot protect unidentified assets.	Council on Cyber Security CSC 1-4 - Inventory of Authorized and Unauthorized Devices
Choose an item.	L	Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to a facility's public and private network(s).	A facility cannot protect systems it does not know it has. An automated tool can identify assets that might have been missed following a traditional inventory process.	Council on Cyber Security CSC 1-1 - Inventory of Authorized and Unauthorized Devices
Choose an item.	L	Deploy dynamic host configuration protocol (DHCP) server logging.	It is important to be able to detect unknown devices that may try to connect to a facility's information system. DHCP server logging can help accomplish this objective.	Council on Cyber Security CSC 1-2 - Inventory of Authorized and Unauthorized Devices
Choose an item.	L	Ensure that all equipment acquisitions update the inventory system, ideally automatically.	To keep the asset inventory up-to-date, new equipment should be added to the asset inventory as soon as it is installed.	Council on Cyber Security CSC 1-3 - Inventory of Authorized and Unauthorized Devices
Choose an item.	M	Integrate the software inventory systems with the hardware asset inventory.	Ensures that all devices and associated software are tracked from a single location.	Council on Cyber Security CSC 2-5 - Inventory of Authorized and Unauthorized Software

3.3 Common Security Controls

This subsection contains 10 categories of security controls that every facility should implement in their ISMS to provide a defense-in-depth approach to security:

- Access Control

- Baseline Configuration Security
- Communications Security
- Cryptography
- Information Sanitization and Destruction
- Human Resource Security
- Operational Security
- Physical and Environmental Security
- Security in Supplier and Third-Party Relations
- Security throughout the Asset Life Cycle.

3.3.1 Access Control

Access control is designed to ensure that someone without permission to access an information asset, or without a need to know that information, is restricted from access. Security controls for access control are provided in Table 3.3. Access can take many forms, such as digital or physical access to an information system or physical access to an information repository. Examples of digital access include accessing an information system using the facility's onsite network, remote access from an external site (e.g., a parent facility's computer network, a remote access location), and website access. In all cases, access to an information system must be granted, disabled, or revoked using an approved and documented process. Access credentials should never be shared, unless permission has been granted based on operational considerations and the security risks involved are explicitly accepted by the facility.

Whenever possible, the access approval process and the granting of access should be automated. Access should be monitored and logged at all times (preferably using automated tools), and log information should be stored to match the facility's data retention policy.

Table 3.3. Access Control Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Review all system accounts and disable any account that cannot be associated with a business process and owner.	Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers.	Council on Cyber Security CSC 16-1 - Account Monitoring and Control
Choose an item.	L	Ensure that all accounts have an expiration date associated with the account.	Forcing accounts to be reviewed and renewed ensures regular review of their continued need.	Council on Cyber Security CSC 16-2 - Account Monitoring and Control

Table 3.3. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.	Regular monitoring forces users to re-authenticate regularly.	Council on Cyber Security CSC 16-5 - Account Monitoring and Control
Choose an item.	L	Categorize identity management according to facility's risk criteria so that stricter access controls are required for more sensitive systems.	Systems that access or store sensitive data should be protected by multiple authentication factors. The facility's identity management system should be flexible enough to allow multi-factor authentication.	NRECA Cyber Security Plan 29
Choose an item.	L	Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.	This will help prevent installation of unauthorized software and other abuses of administrator privileges.	Council on Cyber Security CSC 3-3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Minimize the use of administrative privileges and only use privileged accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	Minimizing the use of elevated privileges reduces the chance that malicious activity can run with administrator or root privilege and cause serious damage.	Council on Cyber Security CSC 12-1 - Controlled Use of Administrative Privileges ASD Strategies to Mitigate Targeted Cyber Intrusions 4
Choose an item.	L	Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., non-shared) credentials.	Unauthorized users pose a substantial security risk for information systems. Ensuring all users granted access to the system are identified and authorized reduces these risks.	NRECA Cyber Security Plan 93
Choose an item.	M	Establish an identity management framework and supporting systems to include physical access and electronic access controls across major enterprise systems.	Rather than focusing primarily on separate access controls for individual systems, integrate the facility's approach to establishing and maintaining identities, striving for as much automated integration among systems as possible to reduce errors and delays.	NRECA Cyber Security Plan 26

Table 3.3. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
	M	Require that all non-administrator accounts have strong passwords that contain letters, numbers, and special characters; are changed at least every 90 days; have a minimal age of one day; and are not allowed to re-use the previous 15 passwords. These values can be adjusted based on the specific business needs of the facility.	Enforcing robust passwords reduces the chance that they can be easily guessed or cracked by unauthorized users.	Council on Cyber Security CSC 16-8 - Account Monitoring and Control
Choose an item.	M	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.	Account lockouts slow down password-guessing attacks.	Council on Cyber Security CSC 16-9 - Account Monitoring and Control
Choose an item.	M	Enforce “least privilege” access to cyber assets and periodically review access privileges.	Ensure that employees have only the privileges they need to perform their jobs.	NRECA Cyber Security Plan 27
Choose an item.	M	Deploy network level authentication via IEEE 802.1x[(a)] to limit and control which devices can be connected to the network.	Preventing the unauthenticated devices from being connected to information systems reduces risks.	Council on Cyber Security CSC 1-5 - Inventory of Authorized and Unauthorized Devices
Choose an item.	M	Deploy network access control to monitor authorized systems.	Network access controls reduce the risk of unauthorized access to information systems.	Council on Cyber Security CSC 1-6 - Inventory of Authorized and Unauthorized Devices
Choose an item.	M	Automatically generate reports of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.	Providing prompt notification to system administrators allows them to take immediate action to rectify potential issues that can lead to unauthorized system access.	Council on Cyber Security CSC 16-3 - Account Monitoring and Control
Choose an item.	H	Use client certificates to validate and authenticate authorized systems prior to connecting to the private network.	Using client certificates reduces the risk of unauthorized connections to information systems.	Council on Cyber Security CSC 1-7 - Inventory of Authorized and Unauthorized Devices

[(a)] The IEEE 802.1X standard (IEEE 2010) is designed to enhance the security of wireless networks. It provides an authentication framework, allowing a user to be authenticated by a central authority. Multiple algorithms for authentication are possible.

3.3.2 Baseline Configuration

Establishing a configuration to which all systems need to adhere is important for maintaining a safe and secure information infrastructure. This configuration is referred to as the baseline, meaning all systems shall at a minimum implement the security controls needed to maintain that baseline. Facilities shall establish and maintain baseline configurations systems (including hardware, software, firmware, and documentation) throughout the system's life cycles; and as well as establish and enforce security configuration settings for all systems.

The baseline must be assigned to, and owned by, an individual or group within the facility who has the authority granted by management to establish, review, update, and maintain the baseline. The baseline shall be reviewed and updated regularly, at least annually for most CBRN facilities or as new vulnerabilities and threats are identified. Ideally the baseline configuration will have input from many affected groups within the facility (e.g., IT, information security, operations, physical security, maintenance). Ensuring that all systems adhere to the facility's baseline configuration is important. Ideally this would be done via automated tools, as well as a manual evaluation to identify areas that are not in compliance. Monitoring and auditing will be covered in more detail in Section 3.7.

See Table 3.4 for the security controls associated with a baseline configuration.

Table 3.4. Baseline Configuration Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Develop a list of authorized software and versions that are required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses.	Developing and maintaining an inventory of authorized software is necessary. A facility cannot protect what the software it does not know it has.	Council on Cyber Security CSC 2-2 - Inventory of Authorized and Unauthorized Software
Choose an item.	L	Establish and ensure the use of standard secure configurations for operating systems. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. Hardening typically includes: • Removing unnecessary accounts (including service accounts). • Disabling or removing unnecessary services, configuring non-executable stacks and heaps. • Applying patches, ideally within two days of what?. Use the latest suitable operating system. • Closing open and unused network ports. • Implementing intrusion detection systems and/or intrusion prevention systems, and use of host-based firewalls.	Standard secure configurations for operating systems reduce security risks. Standardized images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.	Council on Cyber Security CSC 3-1 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers ASD Strategies to Mitigate Targeted Cyber Intrusions 3
Choose an item.	L	Configure laptops, workstations, and servers so that they will not auto-run content from removable media, such as universal serial bus (USB) tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares.	Removable media can be a malware vector.	Council on Cyber Security CSC 5-3 - Malware Defenses

Table 3.4. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Implement automated patching tools and processes for both applications and for operating system software. When outdated systems can no longer be patched, update to the latest version of the application software.	Updating vulnerable operating systems and software, and removing unused software, reduces security risks.	Council on Cyber Security CSC 3-2 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Build a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the facility's change management processes. Images should be created for workstations, servers, and other system types used by the facility.	Maintaining a library of secure images allows for timely restoration of compromised systems. This may lower risks by reducing the consequences of a successful compromise.	Council on Cyber Security CSC 3-4 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations. Alternatively, administrators can manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.	Anti-malware can reduce security risks by offering protection from known forms of malware. It is important to recognize that anti-malware cannot protect against those "zero day" attacks, for which malware signatures have not yet been added to the signature library maintained by the anti-malware service provider.	Council on Cyber Security CSC 5-2 - Malware Defenses
Choose an item.	L	Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.	Removable media can be a malware vector.	Council on Cyber Security CSC 5-4 - Malware Defenses
Choose an item.	L	Limit use of external devices to those that have a business need.	External devices are associated with higher security risks.	Council on Cyber Security CSC 5-7 - Malware Defenses
Choose an item.	L	Enable anti-exploitation features such as data execution prevention, address space layout randomization, and virtualization/ containerization.	These features can reduce information security risks by making it more difficult for attackers to achieve their objectives.	Council on Cyber Security CSC 5-6 - Malware Defenses

Table 3.4. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	For all acquired application software, check that the version being used is still supported by the vendor. Update to the most current version and install all relevant patches and vendor security recommendations.	Software is often updated to address security issues.	Council on Cyber Security CSC 6-1 - Application Software Security ASD Strategies to Mitigate Targeted Cyber Intrusions 2
Choose an item.	L	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.	Default passwords are published on the Internet and freely shared. Changing these immediately reduces the threat of compromise.	Council on Cyber Security CSC 12-4 - Controlled Use of Administrative Privileges
Choose an item.	L	Ensure all equipment connected to the network is uniquely identified and approved for use on the facility's network.	Control hardware that gets connected to the facility's information systems must be registered so that unauthorized devices can be readily detected.	NRECA Cyber Security Plan 95
Choose an item.	M	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe.	Automated tools can reduce information security risks by reducing the time between the availability and installation of security patches.	Council on Cyber Security CSC 4-5 - Continuous Vulnerability Assessment and Remediation
Choose an item.	M	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.	Segmenting or air-gapping critical systems from the rest of the network reduce the attack surface.	Council on Cyber Security CSC 2-7 - Inventory of Authorized and Unauthorized Software
Choose an item.	M	For applications that rely on a database, use standard hardening configuration templates.	All systems that are part of critical business processes should be tested.	Council on Cyber Security CSC 6-9 - Application Software Security
Choose an item.	M	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information.	To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure.	Council on Cyber Security CSC 8-1 - Data Recovery Capability

Table 3.4. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Install the latest stable version of any security-related updates.	Current versions address known vulnerabilities.	Council on Cyber Security CSC 10-5 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Choose an item.	M	Keep all services current and uninstall and remove any unnecessary components from the system.	Current versions address known vulnerabilities.	Council on Cyber Security CSC 11-4 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	M	Use access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading email, composing documents, or surfing the Internet. Web browsers and email clients especially must be configured to never run as administrator.	Basic office work should never be done with elevated privileges.	Council on Cyber Security CSC 12-7 - Controlled Use of Administrative Privileges
Choose an item.	M	If there is no business need for writing data to removable devices (i.e., USB tokens or hard drives), configure systems to prevent this. If such devices are required, enterprise software should be used that can configure systems to allow only specific removable devices (based on serial number or other unique identifier) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.	Once data are written to removable devices, they can be removed from the facility's control.	Council on Cyber Security CSC 17-8 - Data Protection
Choose an item.	M	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system.	Prevents execution of malicious or unapproved programs including dynamic link library files, scripts, and installers.	Council on Cyber Security CSC 2-1 - Inventory of Authorized and Unauthorized Software ASD Strategies to Mitigate Targeted Cyber Intrusions 1

Table 3.4 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	H	Configure client workstations with non-persistent, virtualized operating environments that can be quickly and easily restored to a trusted snapshot on a periodic basis.	Configuring systems to boot via the network using a standard configuration reduces the chances of system compromise. If compromised, the system can be returned to an approved state quickly.	Council on Cyber Security CSC 2-8 - Inventory of Authorized and Unauthorized Software
Choose an item.	H	Deploy software that only provides signed software identification (ID) tags.	A software identification tag is an extensible markup language (XML) file that is installed alongside software and uniquely identifies the software, providing data for software inventory and asset management.	Council on Cyber Security CSC 2-9 - Inventory of Authorized and Unauthorized Software
Choose an item.	H	For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (e.g., basic input/output system, extensible firmware interface), with password protections to lower the possibility that the user will override such configurations.	Only approved systems should have access to authorized wireless networks.	Council on Cyber Security CSC 7-5 - Wireless Access Control
Choose an item.	H	Disable peer-to-peer wireless network capabilities on wireless clients.	Peer-to-peer puts the facility's information and systems at risk.	Council on Cyber Security CSC 7-8 - Wireless Access Control
Choose an item.	H	Disable wireless peripheral access of devices (such as Bluetooth).	Peripheral access protocols can leak information about the facility or allow pairing with unapproved entities.	Council on Cyber Security CSC 7-9 - Wireless Access Control
Choose an item.	H	Configure all systems to use encrypted channels for the transmission of passwords over a network.	Encrypted channels provide protection from the insider threat.	Council on Cyber Security CSC 16-16 - Account Monitoring and Control

3.3.3 Communications Security

This section focuses on all digital communications within a facility that typically occur over a network. Protection of digital communications is important because anyone with malicious intent and access to the network can "sniff" or eavesdrop on facility communications. They can essentially infiltrate the facility's communication channels without actually being a part of them. These protections are also important in preventing the unintentional leak of the facility's sensitive information to groups that do not need this information, and more importantly can prevent information from leaking outside of the facility.

These communication security controls are typically implemented in the facility's firewalls, web proxy, and intrusion detection system/intrusion protection system (IDS/IPS). Rules and policies within these protection methods should always be treated as business sensitive. The rules and policies should be reviewed regularly, at least annually, to ensure that rules are still needed, and that new rules do not cancel out old rules.

Table 3.5 presents risk-based security controls for Communications.

Table 3.5. Communications Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Carry out all remote administration of servers, workstation, network devices, and similar equipment over secure channels.	Protocols such as telnet, virtual network computing, remote desk protocol, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as secure sockets layer or Internet Protocol Security (IPsec).	Council on Cyber Security CSC 3-7 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Only approved traffic should be allowed.	Council on Cyber Security CSC 11-2 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	L	Deny communications with (or limit data flow to) known malicious IP addresses (black lists) or limit access only to trusted sites (whitelists).	Lists of bogus IP addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.	Council on Cyber Security CSC 13-1 - Boundary Defense
Choose an item.	L	Configure operating systems so that passwords cannot be re-used within a time frame of six months.	Re-using passwords can lead to system compromise.	Council on Cyber Security CSC 12-9 - Controlled Use of Administrative Privileges
Choose an item.	L	Configure screen locks on systems to limit access to unattended workstations.	This prevents those with physical access to systems from using the account of someone already logged in as well as accessing systems they are not authorized to use.	Council on Cyber Security CSC 16-6 - Account Monitoring and Control

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Design the network using a minimum of a three-tier architecture (DMZ middleware, and private network). Any system accessible from the Internet should be on the DMZ, but DMZ systems should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier.	Designing a network infrastructure with segmenting or air-gapping critical systems reduces the attack surface.	Council on Cyber Security CSC 19-1 - Secure Network Engineering
Choose an item.	L	To support rapid response and shunning of detected attacks, engineer the network architecture and its corresponding systems for rapid deployment of new access control lists, rules, signatures, blocks, black holes, and other defensive measures.	Designing a network infrastructure to detect and reduce attacks can enable rapid response to malicious behavior.	Council on Cyber Security CSC 19-2 - Secure Network Engineering
Choose an item.	L	Deploy domain name service (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet.	DNS is a key infrastructure capability and often a target for attackers. Hardening this resource greatly reduces the facility's network attack surface.	Council on Cyber Security CSC 19-3 - Secure Network Engineering
Choose an item.	L	Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic moving from one network segment to another of a different security level should default to a "deny all" stance.	Provide security by default.	NRECA Cyber Security Plan 76

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Protect DNS traffic.	Ensures that data are routed to the right parties.	NRECA Cyber Security Plan 83
Choose an item.	L	Ensure that the source of network time is accurate and that accurate time is reflected on all network nodes for all actions taken and events logged.	Maintains accurate network time.	NRECA Cyber Security Plan 80
Choose an item.	L	Use intrusion detection systems (IDSs) to detect any anomalous behavior on the network. If anomalous behavior is encountered, isolate the potentially compromised nodes.	Detects intrusions.	NRECA Cyber Security Plan 90
Choose an item.	L	Limit remote access to networks to an absolute minimum. When required, use technologies like virtual private networks (VPNs) or IPsec. For example, a VPN creates a secure tunnel after properly authenticating the connecting party using its individual credentials.	Prevents unauthorized access.	NRECA Cyber Security Plan 94
Choose an item.	L	Ensure confidentiality of data traversing networks. If channel-level encryption is not possible, apply data-level encryption to protect the data traversing the network links.	Secures data in transit.	NRECA Cyber Security Plan 97
Choose an item.	L	Ensure confidentiality of data, where appropriate.	Secures communications.	NRECA Cyber Security Plan 138
Choose an item.	L	Ensure proper network segmentation.	Promotes compartmentalization, least privilege, isolation, and fault tolerance.	NRECA Cyber Security Plan 139
Choose an item.	L	Ensure data integrity.	Secures communications.	NRECA Cyber Security Plan 140
Choose an item.	L	Ensure origin integrity.	Secures communications.	NRECA Cyber Security Plan 141
Choose an item.	L	Protect from man-in-the-middle attacks.	Secures communications.	NRECA Cyber Security Plan 142
Choose an item.	L	Protect from replay attacks.	Secures communications.	NRECA Cyber Security Plan 143

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Protect web applications by deploying web application firewalls that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, Structured Query Language (SQL) injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	If properly configured, firewalls are an effective security control for reducing information security risks.	Council on Cyber Security CSC 6-2 - Application Software Security
	M	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border.	This traffic should be sent to a properly configured security information event management (SIEM) or log analytics system so that events can be correlated from all devices on the network.	Council on Cyber Security CSC 13-2 - Boundary Defense
Choose an item.	M	Implement the sender policy framework (SPF) by deploying related records in DNS and enabling receiver-side verification in mail servers.	Lowers the chance of spoofed email messages.	Council on Cyber Security CSC 13-3 - Boundary Defense
Choose an item.	M	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.	Looks for unusual attack mechanisms and detect compromise of these systems.	Council on Cyber Security CSC 13-4 - Boundary Defense

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Configure network boundary devices, including firewalls, network-based inbound and outbound proxies, and IPS to log all traffic (both allowed and blocked) arriving at the device.	Having logs makes it much easier to identify when anomalous system behavior began.	Council on Cyber Security CSC 14-6 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	M	Use network-based data loss prevention solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.	This can provide a timely warning of malicious activities, allowing protective measures to be implemented.	Council on Cyber Security CSC 17-9 - Data Protection
Choose an item.	M	Block access to known file transfer and email exfiltration websites.	This will help reduce the likelihood of data loss and unauthorized egress.	Council on Cyber Security CSC 17-13 - Data Protection
Choose an item.	M	Segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defenses.	Designing a network infrastructure with segmenting or air-gapping critical systems reduces the attack surface.	Council on Cyber Security CSC 19-4 - Secure Network Engineering
Choose an item.	M	Control the flow of electronic communications. Client systems should communicate with internal servers; these internal servers should not communicate directly with external systems but should use an intermediate system in the facility's DMZ/perimeter network. The flow of traffic should be enforced through boundary protection mechanisms.	Confines sensitive electronic communication to established trust zones.	NRECA Cyber Security Plan 77
Choose an item.	M	Ensure that all settings used on the network hardware have been set to their secure settings and that assigned staff fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.	Secures configuration.	NRECA Cyber Security Plan 78

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Disable all unneeded network services.	Reduces attack surface.	NRECA Cyber Security Plan 79
Choose an item.	M	Subject requests for allowing additional services through a firewall or other boundary protection mechanism for approval by the information security manager.	Centrally manages access according to business need.	NRECA Cyber Security Plan 81
Choose an item.	M	Use secure routing protocols or static routes.	Avoids the disclosure of information on internal routing.	NRECA Cyber Security Plan 84
Choose an item.	M	Deny use of source routing.	Prevents denial-of-service attacks.	NRECA Cyber Security Plan 85
Choose an item.	M	Use technologies like firewalls and virtual local area networks (VLANs) to properly segment the facility's network in order to increase compartmentalization (e.g., machines with access to business services like email should not be on the same network segment as control systems). Routinely review and test the firewall rules to confirm expected behavior.	Achieves network segmentation to achieve compartmentalization.	NRECA Cyber Security Plan 86
Choose an item.	M	Separate development, test, and production environments.	Avoids production data leaks into test environments.	NRECA Cyber Security Plan 87
	M	Ensure channel security of critical communication links with technologies like transport layer security (TLS). Where possible, implement public key infrastructure (PKI) to support two-way mutual certificate-based authentication between nodes on the network.	Secures data in transit.	NRECA Cyber Security Plan 88

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Ensure the availability of data traversing the networks. If a proper acknowledgment is not received from the destination node, ensure that provisions are in place to resend the packet. If that does not work, reroute the packet via a different network link. Implement proper physical security controls to make the network links harder to compromise.	Detects failures and promote fault tolerance.	NRECA Cyber Security Plan 89
Choose an item.	M	Ensure that proper certificate and key management practices are in place. Cryptography does not help if the encryption key is easy to compromise. Ensure that keys are changed periodically and that they can be changed right away in the event of compromise.	Ensures that cryptographic protection is not undermined through improper certificate or key management.	NRECA Cyber Security Plan 96
Choose an item.	M	Ensure integrity of data traversing the networks through use of digital fingerprints and signed hashes. If TLS is not used, ensure that other protections from man-in-the-middle attacks exist. Use time stamps to protect against replay attacks.	Preserves data integrity.	NRECA Cyber Security Plan 98
Choose an item.	M	Ensure that only standard, approved, and properly reviewed communication protocols are used on the network.	Using proven protocols that have been examined for security weaknesses can reduce information security risks.	NRECA Cyber Security Plan 99
Choose an item.	M	Ensure that sufficient redundancy exists in the network links so that rerouting traffic is possible if some links are compromised.	Ensures continuity of operations.	NRECA Cyber Security Plan 100
Choose an item.	M	Document the network access level that is needed for each individual or role at the facility and grant only the required level of access to these individuals or roles. All exceptions should be noted.	Maintains control over access to network resources and keep access privileges to a necessary minimum based on the individual's role.	NRECA Cyber Security Plan 103
Choose an	M	Use proven communications protocols with built-in security	Secures communications.	NRECA Cyber Security Plan 137

item.		capabilities.		

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Have a trusted third party perform network security penetration testing.	Receive greater assurance that communications are secure.	NRECA Cyber Security Plan 145
Choose an item.	M	Implement sufficient redundancy.	Fault tolerance.	NRECA Cyber Security Plan 146
Choose an item.	M	Use robust key management techniques.	Secure communications.	NRECA Cyber Security Plan 147
Choose an item.	H	Implement remote testing techniques for any information assets located outside the facility to ensure that their firmware has not been compromised.	Prevent unauthorized modification of firmware.	NRECA Cyber Security Plan 101
Choose an item.	H	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks.	Ensuring that only approved systems have access to authorized wireless networks can reduce security risks.	Council on Cyber Security CSC 7-4 - Wireless Access Control
Choose an item.	H	Create separate VLANs for "bring your own device" systems (e.g., privately owned cell phones, tablet computers) or other untrusted devices. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.	Permitting the use of untrusted devices increases information security risks. Creating a separate VLAN can reduce these risks.	Council on Cyber Security CSC 7-10 - Wireless Access Control
Choose an item.	H	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Network segmentation protects both the systems within and outside of that network.	Council on Cyber Security CSC 10-6 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	H	Network-based IPS devices should be deployed to complement IDS by blocking known bad signature or behavior of attacks.	A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.	Council on Cyber Security CSC 13-5 - Boundary Defense
Choose an item.	H	Design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet must pass through at least one proxy on a DMZ network. The proxy should support logging individual transmission control protocol (TCP) sessions; blocking specific uniform resource locators (URLs), domain names, and IP addresses to implement a black list; and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites.	Facilities should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Proxies can also be used to encrypt all traffic leaving a facility.	Council on Cyber Security CSC 13-6 - Boundary Defense
Choose an item.	H	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.	Two-factor authentication ensures a higher level of protection when remotely accessing resources.	Council on Cyber Security CSC 13-7 - Boundary Defense
Choose an item.	H	Devise internal network segmentation schemes to limit traffic to only those services needed for business use across the facility's internal network.	Limiting access by an insider, untrusted subcontractor/vendor, or malware spreading on an internal network reduces the insider threat to the facility.	Council on Cyber Security CSC 13-10 - Boundary Defense

Table 3.5. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	H	Allow only DMZ systems to communicate with private network systems via application proxies or application-aware firewalls over approved channels.	Minimizing the impact of an attacker pivoting between compromised systems reduces the likelihood of an attacker gaining a foothold.	Council on Cyber Security CSC 13-12 - Boundary Defense (note there is no CSC 13-11)
Choose an item.	H	Configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device.	This security control alerts personnel about potential attempts to exfiltrate data and identify the source and destination addresses associated with long sessions.	Council on Cyber Security CSC 13-13 - Boundary Defense
Choose an item.	H	Enable IP traffic collection and analysis to DMZ network flows to detect anomalous activity.	Having this network traffic will help detect anomalous activity on the facility's network.	Council on Cyber Security CSC 13-14 - Boundary Defense
Choose an item.	H	Restrict user-assigned devices to specific network segments.	Ensures least privilege through network segmentation.	NRECA Cyber Security Plan 75

3.3.4 Cryptography

Cryptography, or the encryption of data and communications, is an important tool for information security. All security controls take some commitment and effort to implement, and cryptography is no exception. The level of encryption or cryptography used should be commensurate with the level of risk and/or sensitivity of the information or information assets.

It is important to have both policy and procedures on the use of cryptographic security controls. It is also important to consider any regulations and/or national restrictions that might apply to the use of cryptographic techniques and to issues involving the trans-border flow of encrypted information.

Table 3.6 provides risk-based security controls for cryptography.

Table 3.6. Cryptography Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Ensure all communication of sensitive information over less-trusted networks is encrypted.	Compartmentalizing sensitive information protects it from the rest of the network.	Council on Cyber Security CSC 15-1 - Controlled Access Based on the Need to Know
Choose an item.	L	Use proven encryption techniques.	Secures communications.	NRECA Cyber Security Plan 144
Choose an item.	L	Protect data in transit.	Preserves the confidentiality and integrity of data in transit.	NRECA Cyber Security Plan 82
Choose an item.	M	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.	Protection of mobile devices is critical because of their transitory nature outside of the facility's physical protection.	Council on Cyber Security CSC 17-1 - Data Protection
Choose an item.	M	Manage network devices using two-factor authentication and encrypted sessions.	Encrypted sessions protect the facility and its data.	Council on Cyber Security CSC 10-4 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Choose an item.	M	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.	Encrypted wireless traffic protects the facility's data in transit.	Council on Cyber Security CSC 7-6 - Wireless Access Control
Choose an item.	M	Ensure passwords are hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800-132 (NIST 2010b) or similar guidance.	Steps taken to increase the security of passwords can reduce information security risks	Council on Cyber Security CSC 12-6 - Controlled Use of Administrative Privileges
Choose an item.	M	When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	Protection of certificates and private keys is critical to protect the facility and its data.	Council on Cyber Security CSC 12-13 - Controlled Use of Administrative Privileges

Table 3.6. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Verify that cryptographic devices and software are configured to use publicly vetted algorithms.	Publicly vetted algorithms are considered the most secure and robust.	Council on Cyber Security CSC 17-2 - Data Protection
Choose an item.	M	Allow only approved certificate authorities (CAs) to issue certificates within the enterprise; Review and verify each CA, certificate practices statement, and certificate policy.	Unapproved CAs will adversely affect both the certificate owner (the facility) and the third party relying on the certificate (users and customers).	Council on Cyber Security CSC 17-10 - Data Protection
Choose an item.	M	Where applicable, implement hardware security modules for protection of private keys (e.g., for sub CAs) or key encryption keys.	This additional layer of protection for keys is defense in depth.	Council on Cyber Security CSC 17-15 - Data Protection
Choose an item.	H	Ensure that wireless networks use authentication protocols such as extensible authentication protocol-transport layer security.	Authentication protocols provide credential protection and mutual authentication.	Council on Cyber Security CSC 7-7 - Wireless Access Control
Choose an item.	H	For authenticated access to web services within a facility, ensure that account usernames and passwords are passed over an encrypted channel and associated password hash files are stored securely if a centralized service is not employed.	This control minimizes opportunities for attackers to sniff or insert themselves into web traffic.	Council on Cyber Security CSC 16-15 - Account Monitoring and Control

3.3.5 Information Sanitization and Destruction

Protection of data in transit, such as when moving from one facility system to another, or when being transmitted to an external system, is critical for maintaining information security. Data at rest refers to data in databases, or data sitting on a device awaiting use. Protection of data at rest or during processing addresses a number of threats, including insider threats. Those without a business need to access the data can intentionally or unintentionally affect the confidentiality, integrity, or availability of the data.

When data are no longer needed, they must be made properly and securely irretrievable. This is often referred to as "sanitizing a system or media." Sanitization refers to a process that renders access to target data on the media impossible—or at least infeasible, given the level of effort that would be required to restore the data. If an information asset is going to be repurposed, a facility-approved media sanitizing procedure should be used, ideally one with three or more passes to remove all data from the media. There are several good and low- or no-cost solutions for sanitization (e.g., DBAN data wiping software; www.dban.org) may be a good solution. NIST Special Publication 800-88 Revisions 1 Appendix A (NIST 2014) provides a list of minimum sanitization methods. Appendix C of Special Publication 800-88 lists tools for sanitizing and Appendix E gives device specific wiping approaches that can be used for this effort.

The media that stored the data should be destroyed after wiping to ensure that information is not inadvertently leaked outside the facility. Media such as memory cards, hard drives, USB drives, etc. should be rendered unusable through physical destruction methods such as drilling all the way through the media itself in several places using a drill press or disassembling the media and crushing individual components with an industrial crusher or hammer. There are also commercial industrial grade chippers that chip or break hard drives into small unusable pieces. The broken components should be stored by the facility and then disposed of in a way that they do not end up in the hands of someone outside the facility. Parts should be disposed of in small increments rather than as one group of broken components that could be reassembled by someone with the persistence and skills to do so.

While the guidance presented here primarily addresses the digital storage of data, hard copies should also be stored and disposed of in a secure manner. When printed documents are not in use, they should be stored in locked containers or rooms with restricted access. When these printed copies are no longer needed, they should be shredded, preferably using a cross-cut shredder. The shredded documents should then be disposed of using a trusted method such as incineration or recycling by a security certified recycler. Table 3.7 presents security controls that applicable fore data security and destruction.

Table 3.7. Data Security and Destruction Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Put systems storing and/or processing any sensitive information on separated VLANs with firewall filtering.	Compartmentalizing sensitive information protects it from the rest of the network.	Council on Cyber Security CSC 15-1 - Controlled Access Based on the Need to Know
Choose an item.	L	Redeploy or dispose of protected assets in a secure manner. Establish procedures and practices for data and media sanitization/destruction.	Ensure that the redeployment or disposal of cyber assets does not inadvertently expose sensitive information to unauthorized entities.	NRECA Cyber Security Plan 39
Choose an item.	M	Segment the network based on the trust levels of the information stored on the servers.	Segmenting networks limits the ability of system users to access information that is beyond their security access level.	Council on Cyber Security CSC 15-4 - Controlled Access Based on the Need to Know

Table 3.7. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	H	Use host-based data loss prevention to enforce access control lists even when data are copied off a server.	To reduce information security risks, access control restrictions should be maintained when data are copied to different systems.	Council on Cyber Security CSC 15-5 - Controlled Access Based on the Need to Know
Choose an item.	H	Require multi-factor authentication for accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using Smart cards with certificates, one-time password tokens, or biometrics.	Sensitive data needs additional protections.	Council on Cyber Security CSC 16-14 - Account Monitoring and Control

3.3.6 Human Resource Security

A facility's workers are its greatest asset and represent the greatest threat to security. Unfortunately, people make mistakes, do not always follow procedures, and can act maliciously. For this reason it is important to conduct proper screening of potential staff members during the interview and hiring process and to properly set termination conditions and procedures to follow for personnel who are leaving employment at the facility.

Incorporating cyber security best practices into human resource processes is especially important. This includes conducting background checks to verify potential employees' past work experience, references, and education. For positions involving access to sensitive data and sensitive information systems, credit reports and social media postings may need to be examined. This also applies to those who will have access to sensitive areas, such as janitorial staff.

It is also important to take into account a staff member's access privileges when terminating a staff member or putting a staff member on disciplinary leave from their job. Computer accounts and physical access should be suspended immediately. This action may prevent malicious actions by a disgruntled employee. This action will also deny access to an inactive account, which could be a prime target for access by someone else with malicious intent. Unattended accounts are vectors into the facility as they allow someone to assume the identity of a trusted staff member and avoid raising concern about activities until a malicious action has occurred. Table 3.8 presents risk-based security control for human resources.

Table 3.8. Human Resource Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Adequately screen candidates for hire and repeat the screening process at regular intervals for sensitive positions.	Provides a level of confidence that new hires are trustworthy and ensure ongoing trust in the employee.	NRECA Cyber Security Plan 20
Choose an item.	L	Include cyber security-related items in the employee termination and transfer process and/or checklist.	Ensures that access privileges are revoked at termination or transfer and that all equipment and data are returned to the facility, as applicable.	NRECA Cyber Security Plan 24
Choose an item.	L	Document misuse and abuse cases.	A written description of past problems should be consulted when designing protections to prevent future problems.	
Choose an item.	M	Ensure that the employee evaluation process includes responsibilities related to cyber security, that these responsibilities are updated regularly, and they are managed to ensure they continue to address the facility's cyber security needs.	Ensures that job descriptions formally include cyber security responsibilities and that employee performance in this area is monitored and rewarded.	NRECA Cyber Security Plan 30
Choose an item.	M	Ensure that training and recruiting efforts are focused on cyber security.	Allows the facility to attract and retain top cyber security talent.	NRECA Cyber Security Plan 31
Choose an item.	M	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.	Accounts of contractors and employees who have been terminated can be misused to gain unauthorized system access. Disabling instead of deleting accounts allows preservation of audit trails.	Council on Cyber Security CSC 16-4 - Account Monitoring and Control

Table 3.8. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	H	Require managers to match active employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to active employees or contractors.	All accounts should have a reason to exist and be approved by management.	Council on Cyber Security CSC 16-10 - Account Monitoring and Control
Choose an item.	H	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.	Knowing typical activity helps identify anomalous and possibly malicious behavior of insiders.	Council on Cyber Security CSC 16-13 - Account Monitoring and Control

3.3.7 Operational Security

Staff members who manage information systems generally have the greatest access to the facility's sensitive information. These staff members should be of the highest integrity, but also be the most closely watched. Checks and balances should exist to monitor the actions of these staff using logging, and the logs should be reviewed regularly. No single person should be the only one who knows how a process or system works. At smaller facilities this can be difficult.

It is important that there are at least two staff members (ideally more) who know how to administer key information system operations. Very important operations should require a two-person rule, meaning it takes two people to carry out the task, and one person is not always working alone. It is also important to rotate tasks so that more than one person knows how to comfortably carry out key operations. Finally, it is important for operations staff to take vacation or time away from these tasks—not just because the tasks can be stressful—but because this allows another staff member to rotate in as the lead person to complete the tasks and review the processes with a fresh set of eyes.

Table 3.9 lists security controls for typical information system operations. These controls will protect the core operations at the facility from both staff and outsiders.

Table 3.9. Operations Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	Complex passwords are harder to crack.	Council on Cyber Security CSC 12-3 - Controlled Use of Administrative Privileges
Choose an item.	L	Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	Service accounts are often overlooked and may have default passwords, which makes them an easy conduit into the facility's infrastructure.	Council on Cyber Security CSC 12-5 - Controlled Use of Administrative Privileges
Choose an item.	L	Include at least two synchronized time sources (i.e., Network Time Protocol) from which all servers and network equipment retrieve time information on a regular basis and are set to Coordinate Universal Time (UTC).	The use of more than one time source increases the accuracy and consistency of timestamps and this can enhance the usefulness of log entries when investigating potential security issues.	Council on Cyber Security CSC 14-1 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	L	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and transaction. Systems should record logs in a standardized format.	Proper validation of log setting and standardized log formats can enhance the usefulness of log entries when investigating potential security issues.	Council on Cyber Security CSC 14-2 - Maintenance, Monitoring, and Analysis of Audit Logs

Table 3.9. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis.	The logs must be archived and digitally signed on a periodic basis. Log files must not fill up between log rotation intervals.	Council on Cyber Security CSC 14-3 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	L	Develop a log retention policy to make sure that the logs are kept for a sufficient period of time.	Facilities are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes a facility to detect an attack so they can accurately determine what occurred.	Council on Cyber Security CSC 14-4 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	L	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.	Knowing about anomalous behavior helps identify security events quickly.	Council on Cyber Security CSC 14-5 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	M	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.	Core services are often the target of attack and should be protected with additional diligence.	Council on Cyber Security CSC 11-6 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	M	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server.	Any unauthorized services or traffic should be blocked and an alert generated.	Council on Cyber Security CSC 11-7 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	M	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.	Logs track activity on the system and can be used for forensic purposes.	Council on Cyber Security CSC 12-10 - Controlled Use of Administrative Privileges

Table 3.9. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	Logs track activity on the system and can be used for forensic purposes.	Council on Cyber Security CSC 12-11 - Controlled Use of Administrative Privileges
Choose an item.	M	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, one-time password tokens, and biometrics.	Multifactor authentication is more difficult to guess or brute-force attack, keeping privileged access protected.	Council on Cyber Security CSC 12-12 - Controlled Use of Administrative Privileges
Choose an item.	M	Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged onto the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.	Separating administrative and user account access enhances security.	Council on Cyber Security CSC 12-14 - Controlled Use of Administrative Privileges
Choose an item.	M	For all servers, ensure that logs are written to write-only devices or to dedicated logging servers running on separate machines from the hosts generating the event logs.	Lowers the chance that an attacker can manipulate logs stored locally on compromised machines.	Council on Cyber Security CSC 14-7 - Maintenance, Monitoring, and Analysis of Audit Logs

Table 3.9. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Configure access for all accounts through a centralized point of authentication, for example Active Directory or Lightweight Directory Access Protocol. Configure network and security devices for centralized authentication as well.	Central, consistent services ensure account access enforcement.	Council on Cyber Security CSC 16-12 - Account Monitoring and Control
Choose an item.	H	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls.	Mitigates the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.	Council on Cyber Security CSC 8-4 - Data Recovery Capability
Choose an item.	H	Ensure that the log collection system does not lose events during peak activity, and that the system detects and alerts if event loss occurs (such as when volume exceeds the capacity of a log collection system).	Ensures that the log collection system can accommodate intermittent or restricted-bandwidth connectivity through the use of handshaking/flow control.	Council on Cyber Security CSC 14-10 - Maintenance, Monitoring, and Analysis of Audit Logs

3.3.8 Physical and Environmental Security

Physical and environmental protections are key ways to protect a facility’s information infrastructure from physical attack and maintain environmental conditions that support information system operation. Today, many physical and environmental controls, such as door access, security alarms, lighting systems, fire suppression systems, heating and cooling, etc. are controlled by computers. This trend will continue to increase with time. While this reliance on digital controls enhances efficiency, a compromise of these physical and environmental systems can place information systems at risk. Table 3.10 lists security controls involving physical security and environmental systems.

Table 3.10. Physical and Environmental Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Ensure that backups are properly protected via physical security or encryption when they are stored, and when they are moved across the network.	The protection of backups ensures they are secure and ready to use whenever needed.	Council on Cyber Security CSC 8-3 - Data Recovery Capability
Choose an item.	L	Document, implement, and maintain a physical security plan.	Physical security is considered in a structured manner that can be tracked.	NRECA Cyber Security Plan 57
Choose an item.	L	All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server.	Ensures the ability to detect unauthorized access attempts and enables the facility to take appropriate action if unauthorized access occurs.	NRECA Cyber Security Plan 59
Choose an item.	L	Retain physical access logs for at least 90 days.	Ensures the ability to perform historical analysis of physical access.	NRECA Cyber Security Plan 60
Choose an item.	L	Test each physical security system at least once every three years to ensure that it operates correctly.	Ensures that proper physical security posture is maintained.	NRECA Cyber Security Plan 61
Choose an item.	L	Maintain testing and maintenance records at least until the next testing cycle.	Preserves the ability to understand what was tested and improve testing procedures.	NRECA Cyber Security Plan 62
Choose an item.	L	Retain outage records at least one calendar year.	Preserves the ability to investigate causes of outages and tie them to unauthorized physical access.	NRECA Cyber Security Plan 63
Choose an item.	L	Implement physical security controls and detection mechanisms where tampering could occur.	Ensures that information systems and their data are not physically compromised.	NRECA Cyber Security Plan 126
Choose an item.	M	Document and implement the technical and procedural controls for monitoring physical access at all access points at all times.	The ability to detect unauthorized physical access attempts could enable information security team members to take protective actions before negative consequences are experienced.	NRECA Cyber Security Plan 58

3.3.9 Security in Supplier and Third-party Relations

Suppliers and contractors may develop important and trusted relationships with the facility. While they support operations at the facility, supply personnel to work on facility instruments and systems, or provide essential parts and supplies, their motivations, goals, and objectives will differ from those of the facility.

Facility staff members have the responsibility to protect their facility's mission, resources, and processes. To meet the facility's security goals, information security must be considered when negotiating new work orders, writing requests for proposals, and establishing new contracts with vendors. This may mean requiring vendors to meet information security requirements that are the same or similar to those of the facility. Security needs to be a key consideration and feature of their products and services.

An example would be the requirement that the supplier of digital information assets offers firmware, software, and operating system patches that are tested and installed in a timely manner. There are many cases where information assets were purchased but a plan was not implemented to keep patches and firmware current in order to protect from malicious software. The reasoning at the time was that the instrument was only accessible by physical access. Unfortunately, no one can foresee the future. Over time users needed greater access to their information systems and they were placed on the facility's network, opening the information assets to all the malicious software that passes through a network. The result was that information assets were unprotected and rendered unusable by the malware. In some cases, systems worth many millions of dollars were damaged beyond repair by malicious software.

A number of resources for information on security-based procurement language are available. One example is a document issued by the Energy Control Systems Working Group in 2014 (ESCSWG 2014). This document provides easy-to-use cyber security-based procurement language for the energy delivery systems. Another example was issued by the Electric Power Research Institute in 2012 (EPRI 2012), which provides a cyber security-based procurement methodology for electric power delivery systems. Table 3.11 lists supplier and third-party relationships security controls.

Table 3.11. Supplier and Third-party Relationships Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Negotiate contracts to buy systems configured securely out of the box using standardized images.	Standardized images should be devised to avoid extraneous software that would increase their attack surface and susceptibility to vulnerabilities.	Council on Cyber Security CSC 3-6 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Prior to using, review cloud provider security practices for data protection, and if needed, negotiate additional security to protect the facility's data.	Poor security practices by a third party can endanger information security at the facility.	Council on Cyber Security CSC 17-4 - Data Protection
Choose an item.	L	Ensure that service-level agreements and other contractual tools are properly leveraged so that vendors and partners live up to their obligations. For instance, if a breach occurs at a partner organization, there needs to be a provision to have the facility notified of the full extent of the breach as soon as the information is available.	A contractual obligation will help the facility transfer some of the security risks.	NRECA Cyber Security Plan 68
Choose an item.	L	Request evidence from software vendors that their software development life cycles build security into activities.	Ensures that the product supplied to the facility by the vendor or partner has been designed and built with security in mind.	NRECA Cyber Security Plan 69
Choose an item.	L	For acquired application software, examine the product security process of the vendor (history of vulnerabilities, customer notification, patching/remediation) as part of the overall enterprise risk management process.	The acquisition of software from a vendor with deficiencies in their security program can increase information security risks at the facility systems.	Council on Cyber Security CSC 6-8- Application Software Security
Choose an item.	M	Verify the business, financial, and security reputation of vendor/partner organization.	Concerns that others have about your potential business partners can be indicative of potential security issues that might emerge if you pursue that relationship without taking adequate precautions.	NRECA Cyber Security Plan 64

Table 3.11. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Ask questions during the request-for-proposal process to understand the security posture and practices of the partner organization, and whether its offerings meet security requirements. Compare the security policies and procedures of a third party against the facility's own security policy to ensure compliance.	Ensures that the security practices of the vendor/partner comply with those of the own facility. Ensures that the purchased product or service meets the facility's security requirements. Failure to do so could negatively affect the facility's information security risk	NRECA Cyber Security Plan 65
Choose an item.	M	Identify and prioritize external dependencies, both upstream (The facility depends on whom?) and downstream (Who depends on the facility?). The facility should pay special attention to critical dependencies. An example of a critical dependency is relying on a single external party for a key function/service with no secondary party readily available as backup.	Having an understanding of the dependency chain is critical in managing risk introduced by third-party dependencies, in addition to highlighting areas where additional contingency planning may be required in case a third party becomes unavailable.	NRECA Cyber Security Plan 66
Choose an item.	M	Review the hiring practices and personnel background checks of vendors and partners to ensure that they comply with the facility's policies.	Vendor/partner security issues translate into security issues in their products and services.	NRECA Cyber Security Plan 67
Choose an item.	M	Conduct periodic audits and monitoring of the third-party organization to ensure adherence to its security policies and procedures.	Failure to perform periodic audits and monitoring could have a negative affect the facility's information security risk	NRECA Cyber Security Plan 70
Choose an item.	M	For software purchases, request a trusted independent third-party review, to include a report outlining the discovered security weaknesses in the product.	An independent review will help ensure that the product supplied by the vendor/partner is secure.	NRECA Cyber Security Plan 71

Table 3.11. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Ask the vendors and partners about the process they use to ensure the security of the components and services that they receive from their own suppliers in order to ascertain appropriate due diligence.	Ensure that none of the third-party components that the vendor/partner used in its product introduces security vulnerabilities that could negatively affect the facility's information security risk.	NRECA Cyber Security Plan 72
Choose an item.	M	Actively manage security risks related to third parties, including formal tracking of these risks, addressing such risks in contracts and agreements, and facilitating the two-way exchange of cyber security and threat information with trusted third parties.	This practice builds a foundation of mutual trust and information sharing during the third-party relationship.	NRECA Cyber Security Plan 73
Choose an item.	M	Establish an information-sharing program for third-party organizations, including vendors, suppliers, and connected utilities. Identify external sources of cyber security information and expertise that can be consulted when required. Set up and maintain secure communication channels for the exchange of sensitive data, along with any required legal protections (such as non-disclosure agreements).	To help maintain appropriate information security, establish a trusted network of contacts and facilitate the free flow of both sensitive and non-sensitive information between the facility and third parties. This can reduce the facility's information security risk.	NRECA Cyber Security Plan 74
Choose an item.	M	Apply a qualified third-party security penetration testing to test all hardware and software components prior to live deployment.	Ensures that procured products undergo adequate security testing.	NRECA Cyber Security Plan 129
Choose an item.	H	Ask software vendors, including vendors of hardware that contains embedded software for evidence (e.g., third-party assessment) that their software is free of vulnerabilities.	Ensures that acquired software is not compromised.	NRECA Cyber Security Plan 123

3.3.10 Security throughout the Asset Life Cycle

It is important for the facility to adopt a life cycle view on information security. This involves providing governance over the design, acquisition, installation, operation, maintenance, evolution, and disposal of its components. As part of the life cycle nature of information security, a process of continuous improvement should be included. Results from risk assessment and risk management activities, as well as performance evaluations, should be used to support continuous improvement activities. However, continuous improvements should not wait for periodic reassessments and evaluations. Over the course of routine activities, changes in threats, vulnerabilities, and security technologies will be identified and security enhancements should be made as warranted to address changes in the information security landscape.

To ensure that modifications that have the potential to affect information security are appropriately analyzed, evaluated, and implemented in a controlled manner, a comprehensive and structured approach is required to address information security throughout the life cycle of the system. IEEE Standard 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes" (IEEE 1995) is a useful resource for addressing the software component of life cycle issues.

Table 3.12 presents risk-based system development life cycle security controls.

Table 3.12. System Development Life Cycle Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Robust software helps prevent buffer overflows and other threat vectors.	Council on Cyber Security CSC 6-3 - Application Software Security
Choose an item.	L	Define roles and responsibilities for the management of encryption keys throughout the information system life cycle	The definition of these roles and responsibilities helps maintain data protection throughout the CA life cycle.	Council on Cyber Security CSC 17-14 - Data Protection
Choose an item.	L	Ensure that all software (developed internally or procured from a third party) is developed using security-aware software development life cycle (SDLC).	Ensures that the product supplied to the facility by the vendor/partner has been designed and built with security in mind.	NRECA Cyber Security Plan 125
Choose an item.	M	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment.	Testing detects vulnerabilities before web applications become operational. Detecting and eliminating vulnerabilities reduces security risks.	Council on Cyber Security CSC 6-4 - Application Software Security

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Do not display system error messages to end-users (output sanitization).	Error messages can reveal system weaknesses.	Council on Cyber Security CSC 6-5 - Application Software Security

Table 3.12. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Maintain separate environments for production and nonproduction systems.	Developers should not typically have unmonitored access to production environments.	Council on Cyber Security CSC 6-6 - Application Software Security
Choose an item.	M	Test in-house-developed web and other application software for coding errors and potential vulnerabilities prior to deployment using automated static code analysis software, as well as manual testing and inspection.	Input validation and output encoding routines of application software should be reviewed and tested to ensure information security is not jeopardized by undetected vulnerabilities.	Council on Cyber Security CSC 6-7 - Application Software Security
Choose an item.	M	For in-house developed applications, ensure that development artifacts (e.g., sample data and scripts; unused libraries, debug code) are not included in the deployed software, or accessible in the production environment.	Unused artifacts (e.g., libraries, components, debug code) represent potential security vulnerabilities if deployed in software or accessible in the production environment.	Council on Cyber Security CSC 6-11 - Application Software Security
Choose an item.	M	Define secure implementation guidelines.	Ensures that developers use defensive programming techniques when implementing the system to avoid introducing security weaknesses.	NRECA Cyber Security Plan 52
Choose an item.	M	Perform secure code reviews.	Ensures that software complies with security implementation guidelines, that security controls are properly implemented, and that the implementation itself does not introduce any new security risks.	NRECA Cyber Security Plan 53
Choose an item.	M	Have penetration testing conducted.	Penetration testing by a qualified third party can increase confidence that the software built by the facility or parent organization is secure.	NRECA Cyber Security Plan 55

Table 3.12. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Create a secure deployment and operations guide.	Provides the teams deploying and operating the software in production with instructions to meet security requirements.	NRECA Cyber Security Plan 56
Choose an item.	M	Implement security activities into the facility's SDLC.	Increases the likelihood that the facility develops software that does not have security weaknesses.	NRECA Cyber Security Plan 119
Choose an item.	H	Request an independent-party review of software security to gauge the security posture of acquired.	Minimizes the likelihood that acquired third-party software will have security vulnerabilities.	NRECA Cyber Security Plan 120

3.4 Configuration Management

Configuration management is used to establish, implement, and actively manage (e.g., track, report on, and correct) the security configuration of systems. A rigorous configuration management and change control process reduces security risks for information systems.

To support security within the life cycle of information systems, the versions of hardware and software that are in use should be kept as current as feasible. Hardware and software configurations should be reviewed and approved by the information or cyber security team within the facility. Reviews are often conducted annually, if not more frequently, to ensure configurations are adequate to meet identified threats.

Table 3.13 provides risk-based security controls for configuration management.

Table 3.13. Configuration Management Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Implement a strict change-control process to control any addition or changes to the software on an information asset. This includes checking for unrecognized or altered versions of software by comparing file hash values components.	Attackers often use altered versions of known software to perpetrate attacks, and file hash comparisons will reveal the compromised software. Adhering to a change control process for authorized software reduces the attack surface of systems.	Council on Cyber Security CSC 2-4 - Inventory of Authorized and Unauthorized Software

Table 3.13. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management.	Ensures that only authorized changes to the images are possible.	Council on Cyber Security CSC 3-5 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.	All alterations to such files should be automatically reported to security personnel. The reporting system should have the ability to account for routine and expected changes and highlight unusual or unexpected alterations.	Council on Cyber Security CSC 3-8 (1)- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Establish and maintain secure configuration management processes.	Ensures that information assets, including data, are not compromised.	NRECA Cyber Security Plan 124
Choose an item.	L	Define and enforce secure change control and configuration management processes.	Ensures that system changes do not break security controls established to protect information assets.	NRECA Cyber Security Plan 40
Choose an item.	M	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals or on an event-driven basis.	These tools help ensure that information assets, including data, are not compromised.	Council on Cyber Security CSC 3-10 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	M	Measure the delay in patching new vulnerabilities and ensure that the delay is equal to or less than the benchmarks set forth by the facility. Alternative security controls should be considered if patches are not available in a timely manner.	Prompt patching decreases the likelihood that information assets, including data, will be compromised.	Council on Cyber Security CSC 4-8 - Continuous Vulnerability Assessment and Remediation

Table 3.13. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Evaluate critical patches in a test environment before pushing them into production on enterprise systems. If such patches break critical business applications on test machines, the facility must devise other mitigating controls that block exploitation on systems where the patch cannot be deployed because of its impact on business functionality.	The evaluation of critical patches in a test environment reduces the likelihood of an unexpected and adverse outcome resulting from the installation of the patches.	Council on Cyber Security CSC 4-9 - Continuous Vulnerability Assessment and Remediation
Choose an item.	M	Establish a process to evaluate the risk of vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops).	A risk-based approach can provide an optimal reduction in risk at an affordable cost. In doing this, first apply patches for the riskiest vulnerabilities first and then implement a phased rollout to minimize the impact on facility resources.	Council on Cyber Security CSC 4-10 - Continuous Vulnerability Assessment and Remediation
Choose an item.	M	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be automatically reported to security personnel.	The use of automated tools can reduce the likelihood that information assets, including data, are vulnerable to compromise.	Council on Cyber Security CSC 10-3 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Choose an item.	H	Document and record in a configuration management system all new configuration rules, beyond a baseline-hardened configuration, that allow traffic to flow through network security devices, such as firewalls and network-based IPS. Document the specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.	The use of a structured and well-documented configuration management system can reduce information security risks.	Council on Cyber Security CSC 10-2 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Table 3.13. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
	H	All devices remotely logging into the information system should be managed by the facility, with remote control of their configuration, installed software, and patch levels. For third-party (e.g., subcontractors or vendors) devices, publish minimum security standards for access to the information system and perform a security scan before allowing access.	Remote systems should be held to the same high standard as local ones.	Council on Cyber Security CSC 13-8 - Boundary Defense
Choose an item.	H	Ensure that each wireless device connected to the information system matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Deny access to those wireless devices that do not have an appropriate configuration and profile.	Confirming the appropriate configuration of wireless devices can reduce the potential for compromise.	Council on Cyber Security CSC 7-1 - Wireless Access Control
Choose an item.	H	Test data on backup media on a regular basis by performing a data restoration process.	Ensure that the backup system is working properly and backups are available if needed.	Council on Cyber Security CSC 8-2 - Data Recovery Capability
Choose an item.	H	Compare firewall, router, and switch configuration against the standard secure configurations defined for information assets. Document and approve in a change control system any deviations from the standard configuration or updates to the standard configuration.	The use of non-standard configurations could introduce vulnerabilities that are associated with increased information security risks.	Council on Cyber Security CSC 10-1 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

3.5 Contingency Planning and Disaster Recovery

Contingency and disaster recovery concentrates on returning affected information systems, network or processes to a fully operational status. Having a contingency or disaster recovery plan in place ensures that if a serious event such as a natural disaster or the loss of critical infrastructure should occur, the facility is prepared to deal with the event and has a plan in place to efficiently return information systems to near-normal operations.

NIST has a special publication 800-34, *Contingency Planning Guide for Federal Information Systems* (NIST 2010a) that may be useful for facilities.

Table 3.14 provides security controls for Contingency Planning and Disaster Recovery. Note that only two controls are specified and both are applicable for all risk levels.

Table 3.14. Contingency Planning and Disaster Recovery Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Create and document contingency plans and procedures, based on business and security impacts. Consider information system recovery time objectives. Reviewed, exercise, and update the plans regularly.	Ensures that the facility is prepared to act quickly and correctly to recover critical information assets and continue operations after a major disruption.	NRECA Cyber Security Plan 41
Choose an item.	L	Develop and test continuity and disaster recovery plans.	Ensures that critical information system operations can be restored within an acceptable timeframe.	NRECA Cyber Security Plan 159

3.6 Incident Response

An incident response and recovery process is an important element in an information security program. It is important to identify the problem, implement corrective actions, and return the facility's information systems to normal operations in a timely manner. It is also important to safeguard the forensic data necessary to counter future cyberattacks.

Incident response for an information security event should be integrated with the incident response programs for cyber and physical security; they must also meet both national and international reporting requirements. For many types of information security compromises, both cyber and physical incident responses will be needed. Facilities are encouraged to reach out to appropriate local, regional, national and international organizations to report attacks affecting information security. These organizations are designed to gather and share information on these types of attacks that will allow other facilities to recognize future attacks and take steps to stop them.

Table 3.15 provides a set of risk-based security controls for incident response.

Table 3.15. Incident Response Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	For investigative support, ensure that the reporting system is able to show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch)	Integrity checks should identify suspicious system alterations (e.g., owner and permissions changes, the use of alternate data streams to hide malicious activities, detecting the introduction of extra files that may indicate malicious payloads left by attackers).	Council on Cyber Security CSC 3-8(2) - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	L	Ensure that written incident response procedures include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.	Protects the facility's information and reputation by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, and management oversight) prior to an event.	Council on Cyber Security CSC 18-1 - Incident Response and Management
Choose an item.	L	Assign roles and responsibilities for handling information security incidents to specific individuals.	Establishes roles and responsibilities for incident response prior to an event.	Council on Cyber Security CSC 18-2 - Incident Response and Management
Choose an item.	L	Define management personnel who will support the incident handling process by acting in key decision-making roles.	Establishes management's roles and responsibilities for incident response prior to an event.	Council on Cyber Security CSC 18-3 - Incident Response and Management
Choose an item.	L	Devise facility-wide standards for the time required for reporting anomalous events to the incident response team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include appropriate external-to-the-facility notifications.	Timely reporting an information security event is essential for timely actions.	Council on Cyber Security CSC 18-4 - Incident Response and Management
Choose an item.	L	Assemble and maintain information on third-party contact information to be used to report a security incident.	Establishes points of contact for incident response prior to an event.	Council on Cyber Security CSC 18-5 - Incident Response and Management
Choose an	L	Publish information for all personnel, including employees	Staff members are aware of reporting procedures for	Council on Cyber Security CSC 18-6 - Incident

✓	L/M/H	Activity / Security Control	Rationale	Source
item.		and contractors, regarding the reporting of information security anomalies and incidents.	information security incidents prior to an actual event.	Response and Management

Table 3.15 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Create and document incident-handling policies, plans, and procedures. This includes regular reviews, exercises, and reporting/correlation of events.	Ensures that the facility is prepared to act quickly and correctly to avert or contain damage after an information security incident. Incident-handling procedures also ensure that staff members follow proper procedures and preserve potential evidence.	NRECA Cyber Security Plan 34
Choose an item.	L	Establish and document formal criteria for information security event declaration and escalation, including centralized logging and tracking of event escalations.	Ensures that employees know what constitutes an event, how they should respond, and to whom they should report events.	NRECA Cyber Security Plan 38
Choose an item.	L	Train employees in incident-handling and contingency plans.	Ensures that personnel have a firm grasp of the response plans and can execute them under stress.	NRECA Cyber Security Plan 42
Choose an item.	L	Ensure information security incidents are handled in coordination with external stakeholders when appropriate, such as law enforcement and government agencies.	Ensures proper handling of serious incidents and preserves evidence.	NRECA Cyber Security Plan 25
Choose an item.	M	Use escalations of information security events to support near real-time situational awareness and provide insight over time.	Further enhances the situational awareness of the security posture.	NRECA Cyber Security Plan 47
Choose an item.	M	Conduct periodic incident response drills to ensure incident response team members understand current threats and risks, as well as their responsibilities.	Tests incident response approach capabilities prior to an event.	Council on Cyber Security CSC 18-7 - Incident Response and Management
Choose an item.	H	Implement an incident response process to have the IT organization supply the security team and security vendors with samples of malware running on corporate systems that do not appear to be recognized by the enterprise's anti-malware software. This can result in a more timely and effective response to malware affecting the facility's information systems.	Reducing the time required to enhance protections against new types of malware reduces information security risks.	Council on Cyber Security CSC 5-10 - Malware Defenses

3.7 Monitoring and Auditing

Information security must be treated as a continuous effort to defend and protect a facility's information assets. Security controls are deployed with the intent of deterring, delaying, detecting, or denying an attack. Monitoring and auditing security controls address the detection element of security. Security personnel must continuously acquire, assess, and take action on new information in order to identify and mitigate vulnerabilities and minimize the window of opportunity for attackers. Automated tools for monitoring and auditing can be implemented at an affordable cost and can substantially increase the facility's ability to assess the security status of its information systems. These software tools can provide a security trend analysis and to proactively protect against emerging threats.

A robust information security program will include capabilities for the collection and analysis of indication and warning data to detect and respond to intrusions. These data can come from many different devices and applications in a networked environment. Common examples include event and logging information originating from routers, firewalls, proxies, operating system security event logs, and application logs.

Table 3.16 provides a set of risk-based controls for monitoring and auditing security.

Table 3.16. Monitoring and Auditing Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Perform regular scanning for unauthorized software and generate alerts when it is discovered on a system.	Allowing only authorized software limits the attack surface of a facility.	Council on Cyber Security CSC 2-3 - Inventory of Authorized and Unauthorized Software
Choose an item.	L	Closely monitor and/or block dangerous file types (e.g., .exe, .zip, .msi).	Preventing known dangerous file types reduces the attack surface.	Council on Cyber Security CSC 2-6 - Inventory of Authorized and Unauthorized Software
Choose an item.	L	Run automated vulnerability scanning tools against all systems on an information security system. Perform these scans on a weekly or more frequent basis. Deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator.	Vulnerability scanners help identify both code-based vulnerabilities (such as those described by common vulnerabilities and exposures entries) and configuration-based vulnerabilities.	Council on Cyber Security CSC 4-1 - Continuous Vulnerability Assessment and Remediation

Table 3.16 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.	Reducing the time required to enhance protections against new types of malware would reduce information security risks.	Council on Cyber Security CSC 5-1 - Malware Defenses
Choose an item.	L	Correlate event logs with information from vulnerability scans.	Personnel should be able to correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. Doing so enhances information security.	Council on Cyber Security CSC 4-2 - Continuous Vulnerability Assessment and Remediation
Choose an item.	L	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.	Ensures that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.	Council on Cyber Security CSC 4-3 - Continuous Vulnerability Assessment and Remediation
Choose an item.	L	Subscribe to vulnerability intelligence services in order to stay aware of new issues. Use information gained to enhance vulnerability scanning.	Ensures that vulnerability scanning tools are regularly updated with all relevant important security vulnerabilities.	Council on Cyber Security CSC 4-4 - Continuous Vulnerability Assessment and Remediation
Choose an item.	L	Scan and block all email attachments that contain malicious code or file types that are unnecessary for the business.	Reduces threats from malware. Scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.	Council on Cyber Security CSC 5-5 - Malware Defenses
Choose an item.	L	Ensure that only ports, protocols, and services with validated business needs are running on each system.	Contributes to a defense-in-depth security architecture.	Council on Cyber Security CSC 11-1 - Limitation and Control of Network Ports, Protocols, and Services

Table 3.16 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline.	If a change that is not listed on the facility's approved baseline is not discovered, the information security risk will increase.	Council on Cyber Security CSC 11-3 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	L	Control, monitor, and log all access to protected assets. The facility should aggregate its logging data in a central system or repository to allow for detection, correlation, and reporting of security events.	Prevents and detects unauthorized access to assets. Centralized monitoring and analysis capabilities enhance the effectiveness of this security control.	NRECA Cyber Security Plan 35
Choose an item.	L	Actively manage vulnerabilities through vulnerability discovery and intelligence, prioritization, documentation, and disposition (mitigation or removal).	Achieves detection of vulnerabilities and facilitates their closure.	NRECA Cyber Security Plan 37
Choose an item.	L	Monitor to ensure the latest security patches are applied to all software running on the network hosts.	Monitoring the status of security patches reduces the likelihood that some key security patches have not been installed.	NRECA Cyber Security Plan 104
Choose an item.	L	Monitor to ensure that the latest antivirus/antimalware software runs regularly.	Detect known viruses and/or malware.	NRECA Cyber Security Plan 105
Choose an item.	L	Monitor to ensure that passwords are of sufficient complexity and are changed periodically.	Prevents unauthorized access.	NRECA Cyber Security Plan 108
Choose an item.	L	Monitor to ensure that a reliable source of network time is maintained.	Accurate time keeping is an essential element of logging.	NRECA Cyber Security Plan 121
Choose an item.	L	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to.	This information is used to build a baseline training and awareness roadmap for all employees.	Council on Cyber Security CSC 9-1 - Security Skills Assessment and Appropriate Training to Fill Gaps
Choose an item.	L	Monitor to ensure that all security settings on the hosts are configured with security in mind.	Prevents unauthorized access.	NRECA Cyber Security Plan 112
Choose an item.	L	Monitor to ensure that shared passwords are not used to access hosts or applications running on	Allows for accountability; prevents unauthorized access.	NRECA Cyber Security Plan 113

		these hosts.		

Table 3.16 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Monitor to ensure that authentication is required prior to gaining access to any services or applications running on the network hosts, and that it cannot be bypassed.	Prevents unauthorized access.	NRECA Cyber Security Plan 114
Choose an item.	L	Monitor to ensure that users have only the minimum privileges needed for their job functions. If an elevation of privilege is needed, it should be for the minimum amount of time needed. Enforce the principle of least privilege; prevent unauthorized access; and make it easy to change passwords, revoke access, and enforce password complexity.	Prevents unauthorized access.	NRECA Cyber Security Plan 115
Choose an item.	L	Monitor to ensure that all software updates are properly signed and coming from a trusted source.	Ensures that updates are coming from authorized sources rather than attackers.	NRECA Cyber Security Plan 116
Choose an item.	L	Routinely review the network logs for anomalous/malicious behavior via automated and manual techniques.	The review of network logs can promptly detect intrusion attempts and reduce security risks.	NRECA Cyber Security Plan 92
Choose an item.	L	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.	Sensitive data needs additional monitoring to ensure unauthorized access is not occurring.	Council on Cyber Security CSC 15-3 - Controlled Access Based on the Need to Know (note no 15-2)
Choose an item.	M	Deploy a SIEM or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis.	Automated tools can be tuned to detect unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.	Council on Cyber Security CSC 14-8 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	M	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that all scanning activity and associated access via the privileged account is limited to the time frames of legitimate scans.	Unauthorized scanning activity should be identified and reported quickly.	Council on Cyber Security CSC 4-6 - Continuous Vulnerability Assessment and Remediation

Table 3.16 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Use wireless intrusion detection systems to identify rogue wireless devices and detect attack attempts and successful compromises.	Prompt detection of security issues allows for timely protective actions.	Council on Cyber Security CSC 7-3 - Wireless Access Control
Choose an item.	M	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk.	Acceptance of risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address these vulnerabilities or if conditions have changed, thereby increasing the risk.	Council on Cyber Security CSC 4-7 - Continuous Vulnerability Assessment and Remediation
Choose an item.	M	Implement an automated configuration monitoring system for all secure configuration elements that can be measured through remote testing. This should include tools compliant with Security Content Automation Protocol that alert when unauthorized changes occur.	This includes detecting new listening ports, new administrative users, changes to group and local policy objects, (where applicable), and new services running on a system. Prompt detection of security issues allows for timely protective actions.	Council on Cyber Security CSC 3-9 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Choose an item.	M	Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection.	This control provides a defense-in-depth approach to anomaly detection.	Council on Cyber Security CSC 5-8 - Malware Defenses
Choose an item.	M	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.	This control exhibits a defense-in-depth approach for malware detection and removal.	Council on Cyber Security CSC 5-9 - Malware Defenses
Choose an item.	M	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Reconcile identified devices against a list of authorized wireless access points.	Timely detection of unauthorized (i.e., rogue) access points supports their deactivation before information security can be jeopardized.	Council on Cyber Security CSC 7-2 - Wireless Access Control

Table 3.16 (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
	M	Move any external server that is not required for business purposes to an internal VLAN and give it a private address.	Enhances security of servers that may be otherwise visible from the Internet or by an untrusted network.	Council on Cyber Security CSC 11-5 - Limitation and Control of Network Ports, Protocols, and Services
Choose an item.	M	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.	Privileged access should be given sparingly and only to those with approved business need.	Council on Cyber Security CSC 12-2 - Controlled Use of Administrative Privileges
Choose an item.	M	Monitor for service creation events and enable process tracking logs. For example, on Windows systems, many attackers use PsExec functionality to spread from system to system. Creation of a service is an unusual event and should be monitored closely.	Process tracking is valuable for incident handling.	Council on Cyber Security CSC 14-9 - Maintenance, Monitoring, and Analysis of Audit Logs
Choose an item.	M	Monitor account usage to identify dormant accounts. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations).	Dormant accounts can be used to gain unauthorized access to resources.	Council on Cyber Security CSC 16-7 - Account Monitoring and Control
Choose an item.	M	Monitor attempts to access deactivated accounts through audit logging.	Inactive accounts can be used to gain unauthorized access to resources.	Council on Cyber Security CSC 16-11 - Account Monitoring and Control
Choose an item.	M	Perform assessments of data to identify sensitive information that requires the application of encryption and integrity controls	Knowing facility data types better enables the implementation of appropriate security controls. A facility cannot protect data that it does not know it has.	Council on Cyber Security CSC 17-3 - Data Protection
Choose an item.	M	Deploy an automated tool on network perimeters that monitors for certain sensitive information, keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries. Block such transfers while alerting	Enables identification of data are egressing from the facility or the information system and if they are sensitive or should not be publically shared.	Council on Cyber Security CSC 17-5 - Data Protection

		information security personnel.		

Table 3-16. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Conduct periodic scans of servers using automated tools to determine whether sensitive data are present on the system in clear text.	Such tools search for patterns that indicate the presence of sensitive information and can help identify if a business or technical process is leaving behind or leaking sensitive information. This can help ensure sensitive data are appropriately encrypted at rest.	Council on Cyber Security CSC 17-6 - Data Protection
Choose an item.	M	Move data between networks using secure, authenticated, and encrypted mechanisms.	Checks to ensure data are appropriately encrypted in transit.	Council on Cyber Security CSC 17-7 - Data Protection
Choose an item.	M	Perform an annual review of algorithms and key lengths in use for protection of sensitive data.	Review of algorithms and key lengths ensures that protection mechanism is functioning as expected.	Council on Cyber Security CSC 17-11 - Data Protection
Choose an item.	M	Monitor all traffic leaving the facility and detect any unauthorized use of encryption.	Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that facilities be able to detect rogue connections, terminate the connection, and remediate the infected system.	Council on Cyber Security CSC 17-12 - Data Protection
Choose an item.	M	Control and monitor any user or system accounts used to perform penetration testing to make sure they are only being used for legitimate purposes. Remove or restore them to normal function after testing is over.	Removing these accounts when not being used for approved penetration testing protects the facility's resources from unauthorized access.	Council on Cyber Security CSC 20-2 - Penetration Tests and Red Team Exercises
Choose an item.	M	Perform periodic exercises to test facility readiness to identify and stop attacks or to respond quickly and effectively.	Testing ensures that incident response approach works as planned.	Council on Cyber Security CSC 20-3 - Penetration Tests and Red Team Exercises

Table 3-16. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Test for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.	It is important to think like an attacker and to look for the often forgotten or overlooked information	Council on Cyber Security CSC 20-4 - Penetration Tests and Red Team Exercises
Choose an item.	M	Plan clear goals for penetration tests with blended attacks in mind. Identify the target asset. Use manual or automated testing that captures pivoted and multi-vector attacks to offer a more realistic assessment of security posture and risk to critical assets.	Many advanced-persistent-threat attacks deploy multiple vectors, such as social engineering combined with web or network exploitation.	Council on Cyber Security CSC 20-5 - Penetration Tests and Red Team Exercises
Choose an item.	M	Use vulnerability scanning and penetration testing tools in concert.	The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	Council on Cyber Security CSC 20-6 - Penetration Tests and Red Team Exercises
Choose an item.	M	Devise a scoring method for determining the results of exercises.	Compares results over time and shows progress in security exercises.	Council on Cyber Security CSC 20-7 - Penetration Tests and Red Team Exercises
Choose an item.	M	Create a test bed that mimics a production environment for specific penetration tests. Simulate attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	It is important to think like an attacker and to look for the often forgotten or overlooked information	Council on Cyber Security CSC 20-8 - Penetration Tests and Red Team Exercises
Choose an item.	M	Use logging and monitoring functions to establish a near real-time awareness of the facility's operations, including communications across the facility.	Gain additional insight into the general real-time operational picture and enable faster responses to changing conditions.	NRECA Cyber Security Plan 36

Table 3-16. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Have vulnerability assessments performed by independent third parties at regular intervals, covering all of the facility's key systems, based on its threat model.	Have independent experts review critical systems for known vulnerabilities to reduce likelihood of internal or external compromise.	NRECA Cyber Security Plan 44
Choose an item.	M	Use logging and monitoring functions to specifically understand the facility's cyber security posture and operations in near real time, including information from external sources.	Enhances the situational awareness specific to cyber security, enabling effective security countermeasures if required.	NRECA Cyber Security Plan 46
Choose an item.	M	Ensure that all unneeded services and interfaces on hosts (e.g., USB ports) are turned off.	Minimizes the attack surface.	NRECA Cyber Security Plan 106
Choose an item.	M	Ensure that the hosts only run services and applications that are absolutely necessary.	Minimizes the attack surface.	NRECA Cyber Security Plan 107
Choose an item.	M	Ensure that system logs are checked regularly and any abnormalities investigated.	Detects intrusions/attack attempts (both external and internal).	NRECA Cyber Security Plan 109
Choose an item.	M	Ensure that all access attempts and any elevation of privilege situations are properly logged and reviewed.	Detects intrusions/attack attempts (both external and internal).	NRECA Cyber Security Plan 111
Choose an item.	M	Changes to digital device settings should be reported and logged in a central location. These logs should be reviewed frequently.	Maintains confidence in data coming from digital devices by ensuring that they have not been subjected to tampering.	NRECA Cyber Security Plan 117
Choose an item.	M	If possible, verify integrity of firmware running on information assets. Consult with the equipment vendor for assistance.	Maintains confidence in data coming from digital devices by ensuring that they have not been subjected to tampering.	NRECA Cyber Security Plan 118

Table 3-16. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Monitor to ensure that all software development personnel receive training in writing secure code for their specific development environment.	Role-based training is important to ensure a defense-in-depth approach to security.	Council on Cyber Security CSC 6-10 - Application Software Security
Choose an item.	H	Run software like Tripwire to monitor for file system changes. Make sure that these changes are monitored.	Detects system infections with malware.	NRECA Cyber Security Plan 110
Choose an item.	H	Enable domain name system query logging to detect hostname lookup for known malicious command and control domains.	This control exhibits a defense-in-depth approach.	Council on Cyber Security CSC 5-11 - Malware Defenses
Choose an item.	H	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to networks including those using wireless, dial-up modems, or other mechanisms.	It is important to scan all resources, even those used infrequently.	Council on Cyber Security CSC 13-9 - Boundary Defense
Choose an item.	H	Audit all access to password files in the system. Verify that all password files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges.	Password protection reduces chances of unauthorized access.	Council on Cyber Security CSC 16-17 - Account Monitoring and Control
Choose an item.	H	Conduct external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. This work is done by information and cyber security experts. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around a facility) as well as from within its boundaries (i.e., on the internal network) to simulate	Penetration tests and appropriate responses to their findings can reduce the likelihood of unauthorized access.	Council on Cyber Security CSC 20-1 - Penetration Tests and Red Team Exercises

		both outsider and insider attacks.		

3.8 Awareness and Training

The purpose of security awareness and training is to provide personnel supporting the CBRN facility with the skills needed to minimize information security risks. This begins by assessing the current level of information security knowledge. This is used to identify knowledge gaps between what personnel know and put into practice, and what the facility is targeting for information security practices. Knowledge of gaps is used to enhance the design of information security training. Many facilities find it appropriate and efficient to incorporate information security with cyber security and physical security training because so many elements are common to all three security topics.

Information security training is needed for all functional roles in the facility—for general personnel, information system and sensitive information users and program managers, and information security specialists. The amount of training required varies for the different functional roles. Training also should be provided to vendors, contractors, corporate staff, and regulators who have a legitimate need to access the facility's information systems or sensitive information.

NIST SP 800-50 *Building an Information Technology Security Awareness and Training Program* (NIST 2003) presents a conceptual framework for providing IT security training for a distributed computing environment.

Table 3-17 provides risk-based security controls for information security awareness and training.

Table 3.17. Awareness and Training Security Controls

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Establish a security-awareness program with detailed objectives and review its content regularly.	Ensures that all personnel have an understanding of sensitive information, common security risks, and basic steps to prevent security breaches. Ensures that personnel develop habits that would make them less susceptible to social engineering attacks.	NRECA Cyber Security Plan 21
Choose an item.	L	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to.	This information is used to build a baseline training and awareness roadmap for all employees.	Council on Cyber Security CSC 9-1 - Security Skills Assessment and Appropriate Training to Fill Gaps
Choose an item.	L	Deliver training to fill identified skills gaps.	Applicable, focused training is more memorable and valuable to staff.	Council on Cyber Security CSC 9-2 - Security Skills Assessment and Appropriate Training to Fill Gaps

Table 3.17. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	L	Provide information to all personnel, including employees and contractors, regarding reporting information security anomalies and incidents.	It is important to make staff aware of reporting procedures for incident response prior to an event.	Council on Cyber Security CSC 18-6 - Incident Response and Management
Choose an item.	L	Conduct personnel security awareness training.	Helps improve the people aspect of security.	NRECA Cyber Security Plan 149
Choose an item.	M	Provide enhanced training employees who have access to sensitive information security assets.	Ensures that employees who have electronic or physical access to sensitive information assets know how to maintain information security and how to report and respond to security incidents.	NRECA Cyber Security Plan 22
Choose an item.	M	Assign information security-related responsibilities, particularly training responsibilities, to specific people or positions within the facility, and to external service providers as appropriate. Document these responsibilities in writing.	Ensures that information security training tasks are clearly assigned and that employees and contractors understand the expectations of their roles.	NRECA Cyber Security Plan 23
Choose an item.	M	Ensure that all software development personnel receive training in writing secure code for their specific development environment.	Role-based training is a key to ensuring a defense-in-depth approach to security.	Council on Cyber Security CSC 6-10 - Application Software Security
Choose an item.	M	Implement an online security awareness program that: • focuses on the common intrusion methods that can be blocked by individual action • is delivered in short modules convenient for employees • is updated frequently (at least annually) to cover the latest attack techniques • is mandated for completion by all employees • is reliably monitored for employee completion.	Online training gives staff flexibility to complete the training at their own pace.	Council on Cyber Security CSC 9-3 - Security Skills Assessment and Appropriate Training to Fill Gaps

Table 3.17. (contd.)

✓	L/M/H	Activity / Security Control	Rationale	Source
Choose an item.	M	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious email or provide sensitive information on the telephone without following appropriately authenticating a caller.	Targeted training should be provided to those who fall victim to the exercise.	Council on Cyber Security CSC 9-4 - Security Skills Assessment and Appropriate Training to Fill Gaps
Choose an item.	M	Train system administrators to establish different passwords for their administrative and non-administrative accounts. Each person requiring administrative access should be given his or her own separate account. Users should be trained to only use the Windows administrator or UNIX root accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	Training to develop and implement appropriate password administration policies and practices can lower information security risks.	Council on Cyber Security CSC 12-8 - Controlled Use of Administrative Privileges
Choose an item.	H	Establish an information security sharing program and designate personnel to be responsible for the key roles. Include training on what types of information need to be shared, with whom, and at which frequency. Encourage frank discussions about information security within the facility and foster a cooperative approach, rather than have each group rely on its own resources.	Ensures that throughout the facility there is awareness of the security-related activities of other departments or functions.	NRECA Cyber Security Plan 28
Choose an item.	H	Use hands-on, real-world examples to measure information security performance. If the facility does not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs to measure the mastery of skills.	Security skills assessments for each of the mission-critical roles identify skills gaps.	Council on Cyber Security CSC 9-5 - Security Skills Assessment and Appropriate Training to Fill Gaps

4.0 Sources of Information / References

ASD – Australian Signals Directorate. 2013. *'Top 4' Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirements Explained.* Accessed September 11, 2014 at http://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf.

Council on Cyber Security. 2015. *Critical Security Controls for Effective Cyber Defense, Version 5.* Accessed November 23, 2015 at http://www.cpni.gov.uk/documents/publications/2014/2014-04-11-critical-security-controls.pdf?epslanguage=en-gb.

EPRI – Electric Power Research Institute. 2012. *Cyber Security Procurement Methodology for Power Delivery Systems*. EPRI 1026562, Electric Power Research Institute, Palo Alto, California. Available at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026562.

ESCSWG – Energy Sector Control Systems Working Group. 2014. *Cybersecurity Procurement Language for Energy Delivery Systems*. Energy Sector Control Systems Working Group, Washington, D.C. Available at http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

IEEE – Institute for Electrical and Electronics Engineers. 2010. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. 802.1X-2010, Institute for Electrical and Electronics Engineers, New York.

IEEE – Institute for Electrical and Electronics Engineers. 1995. *IEEE Standard for Developing Software Life Cycle Processes*. IEEE Standard 1074-1995, Institute for Electrical and Electronics Engineers, New York.

NIST - National Institute of Standards and Technology. 2003. *Building an Information Technology Security Awareness and Training Program,* NIST SP 800-50. Available at http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

NIST - National Institute of Standards and Technology. 2010a. *Contingency Planning Guide for Federal Information Systems*. NIST Special Publication 800-34 Rev.1, Available at http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

NIST - National Institute of Standards and Technology. 2010b. *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications.* NIST Special Publication 800-132. Available at http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf.

NIST - National Institute of Standards and Technology. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST Special Publication 800-53, Revision 4. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

NIST - National Institute of Standards and Technology. 2014. *Guidelines for Media Sanitization*. NIST Special Publication 800-88, Revision 1. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

NRECA - National Rural Electric Cooperative Association. 2014a. *Guide to Developing a Cyber Security and Risk Mitigation Plan*. NRECA / Cooperative Research Network Smart Grid Demonstration Project. Arlington, Virginia. Available by using the download tool at https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx. Accessed November 23, 2015.

NRECA - National Rural Electric Cooperative Association. 2014b. "Cyber Security Plan Template." NRECA / Cooperative Research Network Smart Grid Demonstration Project. Arlington, Virginia. Available by using the download tool at https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx. Accessed November 23, 2015.

UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015a. *Information Security Best Practices for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25112.pdf

UNICRI - United Nations Interregional Criminal Justice Research Institute. 2015b. *Information Security Management System Planning for CBRN Facilities*. United Nations Interregional Criminal Justice Research Institute. Turin, Italy. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24874.pdf

Contact:
UNICRI
Viale Maestri del Lavoro, 10,
10127, Turin, Italy
Tel: (+39) 011 6537 111
Fax: (+39) 011 63133 68
information@unicri.it
www.unicri.it

Clifford Glantz
Pacific Northwest National Laboratory
P.O. Box 999, MSIN K9-30, Richland, WA 99352
Tel: 001-509-375-2166
cliff.glantz@pnnl.gov
www.pnnl.gov