NRECA / Cooperative Research Network

Smart Grid Demonstration Project

Guide to Developing a Cyber Security and Risk Mitigation Plan

DOE Award No: DE-OE0000222

National Rural Electric Cooperative Association, Copyright 2011

NRECA / Cooperative Research Network

Smart Grid Demonstration Project

Guide to Developing a Cyber Security and Risk Mitigation Plan

Prepared by

Evgeny Lebanidze
Cigital
21351 Ridgetop Circle
Suite 400
Dulles, VA 20166-6503

evgeny@cigital.com
703-585-5047

for

The National Rural Electric Cooperative Association's
Cooperative Research Network
4301 Wilson Boulevard
Arlington, VA 22203

The National Rural Electric Cooperative Association

The National Rural Electric Cooperative Association (NRECA), founded in 1942, is the national service organization supporting more than 900 electric cooperatives and public power districts in 47 states. Electric cooperatives own and operate more than 42 percent of the distribution lines in the nation and provide power to 40 million people (12 percent of the population).

The Cooperative Research Network (CRN) is the technology research arm of NRECA.

©Guide to Developing a Cyber Security and Risk Mitigation Plan

Copyright © 2011 by National Rural Electric Cooperative Association.

Legal Notice

This work contains findings that are general in nature. Readers are reminded to perform due diligence in applying these findings to their specific needs as it is not possible for NRECA to have sufficient understanding of any specific situation to ensure applicability of the findings in all cases.

Neither the authors nor NRECA assumes liability for how readers may use, interpret, or apply the information, analysis, templates, and guidance herein or with respect to the use of, or damages resulting from the use of, any information, apparatus, method, or process contained herein. In addition, the authors and NRECA make no warranty or representation that the use of these contents does not infringe on privately held rights.

This work product constitutes the intellectual property of NRECA and its suppliers, as the case may be, and contains confidential information. As such, this work product must be handled in accordance with the CRN Policy Statement on Confidential Information.

Contact:

Craig Miller
CRN Project Manager
Craig.miller@nreca.coop
703-626-9683

Evgeny Lebanidze
Security Team Lead
evgeny@cigital.com
703-585-5047

Compliance vs. Plans

This document is intended to help cooperatives develop a cyber-security plan for general business purposes, not to address any specific current or potential regulations. Its foundation is the National Institute of Standards and Technology Interagency Report 7628 (NIST-IR 7628), which is a survey of standards and related security considerations for the smart grid. NIST-IR 7628 does not establish regulations, but is a forward-looking document outlining a strategy for improving smart grid interoperability and security.

Independent of this document, co-ops should understand what regulations, if any, pertain to them. A plan as addressed here is not required and development of a plan is not a substitute for, nor guarantee of compliance with any standards. Conversely, real security requires more than simply compliance with rules – the organization must embrace security as a basic requirement of business operations and develop a broad understanding of security.

This guide helps cooperatives think about security in a systematic way, consistent with the current Federal thinking. The basic concept is not “do this and you are secure” but a commitment to a process of continuous improvement.

Table of Contents

List of Figures

List of Tables

Preface

Purpose

The purpose of this document is to provide an electric cooperative organization with guidance that will help it improve its security posture, as well as help make sure that security is not undermined as new smart grid components and technologies are acquired, integrated, deployed in the field, and maintained.

Scope

This document focuses on cyber security controls that an organization should have in place to meet the security challenges introduced by the smart grid.

Target Audience

The target audience of this document is the electric cooperative's information technology (IT) organization and leadership team.

Contacts

The following are the primary individuals to contact with questions regarding this guide.

Contact	Title	Contact	E-mail Address
Craig Miller	NRECA CRN Project Manager	703-626-9683	craig.miller@nreca.coop
Sammy Migues	Principal	703-404-5830	smigues@cigital.com
Evgeny Lebanidze	Managing Consultant	703-585-5047	evgeny@cigital.com

Executive Summary

This document provides practical security best practices and controls designed to help an electrical cooperative improve the security posture of its smart grid. There is a large volume of guidance from organizations such as the National Institute of Standards (NIST), North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), and others that the reader is encouraged to review (referenced later in this document). The goal of this document is not to supplant or replace the other extensive work on this topic, but rather to boil security guidance down to a more digestible set that electric cooperatives can more naturally internalize and start adopting today. Condensing best practices into such a set required the authors of this document to make trade-offs and use their experience to focus on the most important "do first" types of activities. While not comprehensive by design, the guidance in this document represents actionable best practices and controls that organizations can begin to adopt to mitigate some of today's top security risks.

Every organization's environment is different. While most best practices and guidelines described in this document are applicable to all environments, your organization may discover that some are less relevant to your particular installation. Further, the specific implementation details will differ according to the technology choices that your organization has already made, your technology road map, available resources, and other factors. To maintain its focus on a condensed set of best practices, this guide does not delve into lower-level implementation details (although some examples are provided for reference).

It is also important to note that adding or modifying existing security controls should be done with care and sufficient planning. Your environment will require testing to ensure that changes to controls do not break important functionality or introduce new risks. The guidance in this document should be used as a description of what needs to be done, but your organization should introduce changes to your environment in a careful and thoughtful manner. Security improvement does not happen overnight; it is a gradual process.

This document describes security risks and recommends security controls in each of the following categories:

- People and policy security risks
- Operational security risks
- Insecure software development life cycle (SDLC) risks
- Physical security risks
- Third-party relationship risks
- Network security risks
- Platform security risks
- Application security risks

Introduction

Smart grid technologies introduce significant new risks into electrical cooperative environments. Smart grids, by design, make extensive use of remote network connectivity, advanced communication protocols, sophisticated hardware that is difficult to configure, and complex software. This added complexity and connectivity introduce additional security risk. There are some significant steps being taken in the context of the current smart grid demonstrations project to help electric cooperatives mitigate some of these risks. One example is the introduction of security extensions into MultiSpeak® communications protocols to help preserve the confidentiality and integrity of communications between smart grid nodes.

An important aspect of the smart grid is to make decisions and take actions based on real-time data coming from field devices. While benefits are numerous, so are the security implications. These technological changes make it increasingly important that electric cooperatives ensure the bar is set high enough to preserve the confidentiality, integrity, and availability of cyber assets. The most pressing security concern is to ensure that attempts to tamper with field device data, software, or hardware do not disrupt the overall operations of the grid on a large scale and do not result in incorrect actions being taken at the SCADA level.

A corresponding increase in the maturity of a cooperative's security practices will be required. Security risks can be categorized in many ways, but we will put them into three categories: people, process, and technology. Raising the security posture of a cooperative requires raising the bar in all of these categories. Adversaries will go after the weakest link, so it is important to approach any security program comprehensively using risk management practices as a guide. It is also important to comply with principles such as defense in depth, compartmentalization, least privilege, and fault isolation. Failure will happen, so it is important to plan for it, isolate it, contain its damage, and recover from it gracefully.

An organization's security policy and controls must be adaptable to emerging threats in a constantly evolving world. Only recently, Stuxnet malware targeting specific programmable logic controllers (PLCs) was made public. The malware remained dormant and hid its tracks while propagating, but once infecting a machine used to program PLCs, injected some of its own code into the PLC ladder logic that interrupted the normal operation of physical hardware (uranium enrichment centrifuges, in this case). The vulnerabilities allowing Stuxnet to succeed included insecure software (technology), improper IT security management (process), and insufficient security training of personnel (people)—the usual people, process, and technology triad that underlies the security (or insecurity) of any system.

There is little doubt that Stuxnet will be used as blueprint for similar malware to target other types of industrial control installations. Instituting practices such as proper network segmentation, regular security patching, up-to-date antivirus software that runs regularly, security-aware software development and acquisition processes, proper vendor risk management, remote attestation of firmware running on field equipment, and personnel security training will go a long way toward mitigating that particular risk. But this is just one example of many.

The ongoing assessment of security threats, balanced against the existence and adequacy of security controls at your organization, is needed to ensure that security controls and countermeasures in place are commensurate with potential risks. The effort is never ending. The goal of this guide is to provide concise, understandable guidance that will help a cooperative maintain an adequate security posture as it acquires, integrates, deploys, and maintains smart grid technologies.

To assist each cooperative in managing risk associated with smart grid technologies, this document includes the following:

- Checklists of security items in the beginning of each section that summarize the key security best practices and controls. Additional detail is provided in the text description following the checklist.
- Color maps that visually indicate the degree to which various security risks are applicable to various smart grid activity types:
  - Advanced metering infrastructure (AMI)
  - Meter data management (MDM)
  - Communication systems (COMM)
  - Supervisory control and data acquisition (SCADA)
  - In-home device / Web portal (IHD/ Web portal)
  - Demand response over advanced metering infrastructure (DR over AMI)
  - Interactive thermal storage
  - Smart feeder switching
  - Advanced volt/VAR control
  - Conservation voltage reduction (CVR)

  Note: Your organization may not be currently adopting all of these smart grid technologies. Please disregard security concerns specific to the technologies that are not being used.

  For each risk, potential security impact and mitigation strategies are summarized. This is to help your organization focus on implementing security best practices and controls that directly mitigate the risks most applicable to the demonstration activities being deployed at your organization.
- A summary of specific security concerns and controls that are unique to or important for each demonstration activity type.

- Logical organization of security risks grouped by people / policy, process, and technology, with further breakdown of risks and associated security controls in each of these groupings.
- Hyperlinked references to external standards and detailed guidance for each key topic.

Quick Start Guide

The guide is structured to make it easy for organizations to decide on and make improvements to the security posture of their installations starting on day one. How you might want to use this guide will depend on where you are focusing your security initiatives, what you already have in place, the top security risks that you have identified within your organization, the smart grid activity types that you are implementing, and other factors.

Passively reading this cyber security guide cover to cover is not likely the best approach. Instead, we recommend the following:

- Review the table of contents of this document to get a sense of how it is organized and what topics may be most applicable to your current needs.
- Think about the people, process, and technology security dimensions in your organization and determine where you may need the most help in the short term. You may want to get started in the appropriate section.
- In each section, look at the activities in the checklist presented in the beginning of the section for a list of *to do*s. If you want to get more information about each *to do* and why it is important, browse through the supporting text in the body of that section.
- If you want to implement only the security controls from each section that are most relevant to a particular smart grid activity type, browse through the color map to understand what risks are most relevant to that activity type, and focus on security best practices and controls that address these risks.
- Browse through the sections of this document that are specific to smart grid activity / technology if you want to understand the unique security requirements that it introduces into your environment and how to cope with these.
- For each section of the document that you review, document the gaps between the described security controls / best practices and what your organization is already doing in that regard. Then create a remediation road map for how you are going to close the gaps (for gaps that you believe are worth closing). To decide which gaps to prioritize, you may want to review what security risks each of the proposed security best practices / controls is intended to address. If that risk is applicable to your environment and reaches a sufficient severity threshold, then closing the associated control gap makes sense.

Additional Cyber Security Standards and Guidance

This document is intended to be supplemented with standards and guidance provided by other organizations that have done extensive work on smart grid security. The reader is encouraged to review the following sources of information:

- NERC CIP Standards 002–009:[1] NERC critical infrastructure protection (CIP) standards for entities responsible for the availability and reliability of the bulk electric system.
- NIST IR 7628:[2] Smart grid cyber security strategy and requirements.
- NIST SP800-53, *Recommended Security Controls for Federal Information Systems and Organizations:* Catalog of security controls in 18 categories, along with profiles for low-, moderate-, and high-impact systems.
- NIST SP800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*
- NIST SP800-39, *DRAFT Integrated Enterprise-Wide Risk Management*: Organization, mission, and information system view.
- AMI System Security Requirements: Security requirements for advanced metering infrastructure.
- ISO (International Organization for Standardization) 27001, *Information Security Management Systems:* Guidance on establishing governance and control over security activities (this document must be purchased).
- IEEE (Institute of Electrical and Electronics Engineers) 1686-2007, *Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities* (this document must be purchased).

NIST continues its efforts to create and harmonize interoperability and cyber security guidelines. Your organization should continue to stay abreast of those changes.

[1] In *Reliability Standards for the Bulk Electric Systems of North America.*

[2] Three volumes plus an introduction are available at http://csrc.nist.gov/publications/PubsSPs.html.

Building a Risk Management Program

No usable system is 100 percent secure or impenetrable. The goal of a risk management program is to identify the risks, understand their likelihood and impact on the business, and then put in place security controls that mitigate the risks to a level acceptable to the organization. In addition to assessment and mitigation, a robust risk management program includes ongoing evaluation and assessment of cyber security risks and controls throughout the life cycle of smart grid component software.

The following checklist summarizes security best practices and controls that you should consider implementing. This section includes details about the practices.

✓	Activity / Security Control	Rationale
	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.
	Assign responsibility for security risk management to a senior manager.	Have security risk mitigation, resource-allocation decisions, and policy enforcement roll up to a clearly defined executive with the requisite authority.
	Define the system.	Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security.
	Identify and classify critical cyber assets.	It is important to understand the assets that may need to be protected, along with their classification (e.g., confidential information, private information, etc.). That way an informed decision can be made as to the controls needed to protect these assets, commensurate with risk severity and impact to the business.
	Identify and analyze the electronic security perimeter(s) (ESPs).	To build a threat model, it is important to understand the entry points that an adversary may use to go after the assets of an organization. The threat model then becomes an important component of the risk assessment.
	Perform a vulnerability assessment.	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.
	Assess risks to system information and assets.	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization'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 organization.

✓	Activity / Security Control	Rationale
	Select security controls.	Appropriate management, operational, and technical controls cost-effectively strengthen defenses and lower risk levels. In addition to assessed risks, selection factors might include the organization's mission, environment, culture, and budget.
	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.

Appointing Leadership

It is the executive management's responsibility to establish risk management fundamentals within the organization. This includes a business framework for setting security objectives and aligning strategic risk management with business needs as well as external statutory and regulatory compliance drivers. Without active sponsorship by executive management and a specific role dedicated to ensuring the fulfillment of security goals, instituting security controls is next to impossible.

A senior manager must have clear responsibility and authority to drive planning, enforce compliance with defined policies, and approve all exceptions to the security policy.

Establishing a Risk Management Framework

It is important for an organization to define a risk management framework that will be used to:

- Define the system.
- Identify cyber assets and their classification.
- Identify the electronic security perimeter (ESP) protecting these assets.
- Conduct vulnerability assessment:
  - Identify threats.
  - Identify vulnerabilities.
- Identify security risks along with their impact and likelihood.
- Assess the effectiveness of existing security controls in mitigating the risks.
- Recommend new security controls or changes to existing security controls to mitigate the severity of the risks to a level acceptable to the organization.
- Continuously monitor the effectiveness of security controls.
- Periodically repeat this process to account for system changes and changes in the threat landscape.

These steps are described in more detail below.

Defining the System

Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cyber security. Not all systems require the same level of protection.

The following are a few major elements of a system definition:

- The logical and physical boundaries of the system within its environment:
  - Which components and resources belong to the system?
  - Which are external to the system?
- The system's mission and primary functions.
- The system's architecture (physical, logical, and security) and data flows.
- Details for interfaces and protocols.
- Types of information the system stores, uses, or transmits, and the sensitivity of each.
- Existing management, technical, operational, and physical security controls.

Additional Guidance

- Elements of a System Definition in Appendix E: Procedures list additional elements of a system definition, along with useful sources of input.
- Section 3.1, System Characterization, of NIST SP800-30, *Risk Management Guide for Information Technology Systems*, describes the inputs and outputs of the system definition activity (which it calls system characterization).
- Chapter 10.1, Risk Assessment, in NIST SP800-100, *Information Security Handbook: A Guide for Managers*, gives a summary of system characterization.

Cyber Asset Identification and Classification

Systems have access to and operate using assets that adversaries may want to compromise. Using a risk-based methodology to identify critical cyber assets is a crucial step in managing security risk. The NERC glossary[3] gives the following definitions:

- *Critical assets*: Facilities, systems, and equipment that if destroyed, degraded, or otherwise rendered unavailable would affect the reliability or operability of the bulk electric system.
- *Cyber assets*: Programmable electronic devices and communications networks including hardware, software, and data.
- *Critical cyber assets*: Cyber assets essential to the reliable operation of critical assets.

Note: Risk assessments generally consider both the impact of an adverse event and the likelihood that the event will occur. However, the identification of critical assets considers only the impact of the event; it assumes that the loss will in fact occur.

[3] NERC, *Glossary of Terms Used in Reliability Standards*.

Identifying Critical Cyber Assets

NERC provides detailed guidelines for identifying *critical assets*—assets whose loss could cause failure or unacceptable degradation of the bulk power system—and related *critical cyber assets*. (See guidance documents below.) The following steps summarize the process:

1. Identify critical assets.
   a. Identify the asset types to be evaluated:
      - Facilities such as generation resources, transmission substations, control centers.
      - Special systems such as SCADA systems, real-time decision-support systems.

   b. Enumerate the assets within each type. This is the list of critical assets.

   c. List the essential functions of each critical asset.
2. Identify cyber assets associated with a critical asset. Grouping cyber assets by application can simplify the process.
3. Narrow the list of identified cyber assets from step 2 to those supporting the *essential functions* of critical assets.
4. Further narrow the list from step 3 to cyber assets that meet one of the following conditions defined in the NERC CIP-002-3 standard:[4]
   a. Cyber assets that use a routable protocol to communicate outside the ESP.

   b. Cyber assets that use a routable protocol within a control center.

   c. Cyber assets that are dial-up accessible.

A designated senior manager or delegate must annually review and approve the lists of critical assets and critical cyber assets.

Additional Guidance

- NERC Security Guideline for the Electricity Sector: *Identifying Critical Assets*.
- NERC Security Guideline for the Electricity Sector: *Identifying Critical Cyber Assets*.
- NIST SP800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
- ISO 27000 series[5] of information security and management international standards.

Classifying Cyber Assets

Classifying cyber assets as public, restricted, confidential, or private will help dictate the rigor with which they need to be protected by security controls. If your organization has developed an internal asset classification system, it can be used instead of the one suggested below. Consider classifying your cyber assets in the following categories:

Public

[4] NERC CIP-002-3, *Critical Cyber Asset Identification*.

[5] See the IT Security Techniques standards at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

This information is in the public domain and does not require any special protection. For instance, the address and phone number of the headquarters of your electrical cooperative is likely to be public information.

Restricted

This information is generally restricted to all or only some employees in your organization, and its release has the potential of having negative consequences on your organization's business mission or security posture. Examples of this information may include:

- Operational procedures
- Network topology or similar diagrams
- Equipment layouts of critical cyber assets
- Floor plans of computing centers that contain critical cyber assets

Confidential

Disclosure of this information carries a strong possibility of undermining your organization's business mission or security posture. Examples of this information may include:

- Security configuration information
- Authentication and authorization information
- Private encryption keys
- Disaster recovery plans
- Incident response plans

Personally Identifying Information (PII)

PII is a subset of confidential information that uniquely identifies the private information of a person. This information may include a combination of the person's name and social security number, person's name and credit card number, and so on. PII can identify or locate a living person. Such data has the potential to harm the person if it is lost or inappropriately disclosed. It is essential to safeguard PII against loss, unauthorized destruction, or unauthorized access.

To ensure the comprehensive identification of all data requiring privacy protections, apply a test such as the one used in concert with the European Union Data Protection Act.[6] This test can be applied to data that is stored, processed, or transmitted. It poses a short series of questions about the characteristics of the data to facilitate its categorization, such as the following:

- Can a living person(s) be individually identified with the data?
- Does the data relate specifically to the identifiable person in some way?
- Does loss or misuse of the data have the potential to affect an individual?

See **Identifying and Protecting Private Data** in Appendix E: Procedures for additional guidance about identifying and protecting private data.

Additional Guidance

- NIST SP800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*.

Identifying the Electronic Security Perimeter (ESP) Protecting Cyber Assets

All critical cyber assets should reside behind logical security protections. Each collection of logical security protections is an *electronic security perimeter (ESP)*. NERC defines the ESP as "the logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled."[7]

This logical border is the collection of proxies, gateways, routers, firewalls, encrypted tunnels, etc., that monitor and control communications at the external boundary of the system to prevent and detect malicious and other unauthorized communication. At a minimum, identify and document the following:

- The critical cyber assets requiring an ESP.
- The *access points* to each perimeter, for example:
  - Firewalls
  - Routers
  - Modems
  - Virtual private network (VPN) endpoints
  - Proxy servers
  - Web servers

The analysis of ESPs, and whether critical cyber assets reside fully within a secure perimeter, requires care. Identifying all access points and the controls on them can be tricky, and it is possible to overlook an avenue of access that could be exploited.

[6] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf.

[7] http://www.nerc.com/files/Glossary_of_Terms_2011Mar15.pdf

Notes:

- Many critical cyber assets should include their own security controls rather than merely residing within an ESP.
- Noncritical cyber assets inside a defined perimeter must be afforded the same protections as critical cyber assets.

Additional Guidance

For certain wireless assets, see NIST SP800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*.

Conducting a Vulnerability Assessment

Perform a cyber vulnerability assessment of the access points to each ESP at least once a year. The vulnerability assessment should examine ways in which the security perimeter can be breached and existing security controls bypassed to compromise confidentiality, integrity, or availability of critical cyber assets.

A cyber *threat* is any entity or circumstance that has the potential to harm an information system and, through that system, the organization's mission and goals. A cyber *vulnerability* is a gap or weakness in a system's security controls that a threat can exploit.

Vulnerability assessments broaden and deepen awareness of threats, attacks, vulnerabilities, and the effectiveness of existing controls. They also establish baselines that future assessments can use to determine whether planned improvements have occurred.

See *Steps in Vulnerability Assessments* in Appendix E: Procedures for guidance about conducting a vulnerability assessment.

Additional Guidance

- NIST SP800-30, *Risk Management Guide for Information Technology Systems*.
- DOE Vulnerability Assessment Methodology—Electric Power Infrastructure.
- ISACA IS Auditing Procedure, Security Assessment—Penetration Testing and Vulnerability Analysis.

Assessing and Mitigating Risks

Vulnerability assessments will identify certain risks. An important part of the risk management process is to determine the severity of each risk as a function of its impact and likelihood. It is also important to understand the extent to which existing security controls completely or partially mitigate each risk. It is then possible to enumerate the gaps in protection and make an informed risk-based decision on next steps.

Although a risk management strategy strives for risk prevention where practical, it also must balance the costs and benefits of security controls. The goal is cost-effective controls that ensure acceptable risk levels for participating cooperatives and the smart grid as a whole.

We can think of security risks as belonging to one of three main categories:

- People and policy
- Process
- Technology

A cyber security program must be comprehensive—it is only as strong as its weakest link. Failure to develop appropriate controls in any category provides openings for attackers. This guide includes sections that describe common risks and mitigations in each category.

Assessing Impact and Risk Levels

A careful risk assessment considers both the likelihood of a successful attack and its impact on the organization's mission and goals. When assessing the level of security protection required for smart grid assets, NIST guidance is to consider only the *potential impact* of exposed, compromised, or lost data or operations. Furthermore, the most valuable part of a system—the "high-water mark"—determines the impact level of the system itself.

For example, consider a system that is not critical to smart grid operations: The potential impact of a loss of integrity or availability for each asset is low. Therefore, the system's assessed impact levels for these two security goals are both low. In addition, most of the data stored, used, or transmitted by the system is not sensitive; these cyber assets have a low potential impact from a loss of confidentiality.

However, if a single system data set contains PII, that asset has a high level of potential impact from a loss of confidentiality. Therefore, the confidentiality impact level is high for the *entire system.* In turn, the overall impact level of the system—considering all three security goals—is high. The entire system requires a high level of security protection.

The *risk level,* or its severity, is a combination of assessed likelihood and assessed impact. Although the likelihood of loss does not affect the level of protection the system requires, it usually plays a role in prioritizing security efforts. Among systems with high impact ratings, those with significant threats and vulnerabilities might currently carry the highest risk to the organization and receive high priority for remediation.

Finally, the nature of an impact affects the level of risk the organization is willing to assume. Not all high impact ratings are equal. Impacts could be ranked as follows:

- *Safety:* Causing risk to life and limb.
- *Outage:* Leading to improper operation of a power system device, possibly resulting in a consumer outage.
- *Privacy:* Disclosing private data, such as social security or credit card numbers.
- *Monetary:* Leading to increased tangible costs to the utility.

Once your organization identifies and prioritizes risks and the gaps that exist in current security controls, it is possible to build a prioritized remediation plan that focuses on improving existing security controls or adding security controls to mitigate high-priority risks first, then medium priority, and then low priority (as appropriate).

Mitigating Risks with Security Controls

Understanding an event's impact allows the organization to make informed decisions about mitigating the risk by some combination of the following:

- Reducing the likelihood of its occurrence
- Detecting an occurrence
- Improving the ability to recover from an occurrence
- Transferring the risk to another entity (e.g., buying insurance)

It is important to apply risk mitigation strategies at each stage in the life cycles of system components and protocols. Questions such as the following can help guide strategy choices:

- Is the risk a compliance issue, a privacy issue, a technical issue, or some other issue?
- Does the mitigation deal primarily with people, process, or technology?
- Is the assessed risk acceptable to the organization?
- Is the cost of fully remediating the risk reasonable?

NIST SP800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, includes an extensive catalog of management, operational, and technical security controls. Table 1. Families of Security Controlslists the controls and maps them to risk categories.

Table 1. Families of Security Controls

Control Family	NIST Class	Risk Category
Access control	Technical	Process
Awareness and training	Operational	People/Policy
Audit and accountability	Technical	Technology
Security assessment and authorization	Management	Process
Configuration management	Operational	Process
Contingency planning	Operational	Process
Identification and authentication	Technical	Technology
Incident response	Operational	Process
Maintenance	Operational	Process
Media protection	Operational	Process
Physical and environmental protection	Operational	Process
Planning	Management	Process
Personnel security	Operational	People/Policy

Control Family	NIST Class	Risk Category
Risk assessment	Management	Process
System and services acquisition	Management	Process
System and communications protection	Technical	Technology
System and information integrity	Operational	Process
Program management	Management	Process

The selection of controls depends on (a) the system's impact level and (b) the vulnerabilities found in existing protections. SP800-53 includes security profiles for each impact level.[8] NIST gives guidance for tailoring controls and profiles to site-specific requirements.[9] Also, this guide recommends controls to mitigate identified risks. Together, these approaches will identify cost-effective controls for the required level of protection.

The following steps summarize a process for assessing and mitigating risks:[10]

1. *System characterization:* Identify the system's boundaries, resources, and information.
2. *Threat identification:* List all entities (natural, human, or environmental) that could harm the system's capability to fulfill its critical functions. List their potential attack methods and assess their capacity and motivation (for humans) to mount an attack.
3. *Vulnerability identification:* List and assess all gaps or weaknesses in the system's management, operational, and technical security controls that a threat could accidentally or intentionally exploit to harm the system.
4. *Risk assessment:* Estimate the risks to the system posed by specific threats and vulnerabilities. This process consists of four tightly linked activities:
   a. Analyze the capability of existing security controls to prevent an occurrence of the adverse event, detect an occurrence, and contain the impact of an occurrence.
   b. Estimate the likelihood (high, medium, low)[11] of an occurrence given the nature of the vulnerability, the capability of existing threats, and the strength of current controls.
   c. Analyze the potential damage an occurrence would do to the system, its data, and the organization's business goals. Rate the potential impact as high, medium, or low.
   d. Derive the risk rating from the combination of likelihood and impact.
5. *Control recommendations:* Identify and select additional security controls to eliminate the risks or lower them to an acceptable risk level.

[8] NIST SP800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

[9] NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

[10] Chapter 10 in NIST SP800-100, *Information Security Handbook: A Guide for Managers*.

[11] As an alternative, use a five-level scale for likelihood and potential impact.

A good approach is to apply the methodology described above from two directions:

- A *bottom-up analysis* focuses on well-understood security problems and how they are addressed. Such problems include authenticating and authorizing users, authenticating devices and control data, protecting private data, and protecting cryptographic material.
- A *top-down analysis* starts with threats and attacks, examines relevant requirements and attack surfaces, determines risks that must be mitigated, and recommends security controls.

Additional Guidance

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, summarizes security controls in 17 categories and the profiles for 3 levels of security.
- NIST SP800-30, *Risk Management Guide for Information Technology Systems* (includes a detailed elaboration of the process summarized above).
- NIST SP800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
- NIST SP800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.
- NIST SP800-100, *Information Security Handbook: A Guide for Managers* (includes a streamlined version of the process steps in SP800-30).

Evaluating and Monitoring Control Effectiveness

Analysis can show the absence or presence of controls, but testing is usually required to demonstrate the effectiveness of each control in mitigating a particular risk. The organization must develop, implement, and maintain cyber security test procedures and tools. Multiple types of testing may be required:

- Testing of personnel awareness and capability requires tailored skills reviews.
- Testing of security features and software logic requires manual penetration testing.
- Testing of software security requires static analysis tools.
- Testing of Web applications requires dynamic testing tools.
- Testing of protocols requires interoperability harnesses and fuzzing tools.
- Testing of hosts and networks requires network penetration testing tools.

Notes:

- Ensure that skilled individuals perform security testing and analysis with tools.
- The level of detail in test plans depends on the type of testing. It can range from simple plans for basic testing to detailed plans for complex interoperability and security testing.
- Testing must reflect production environments, and the results must be documented.

Additional Guidance

- NIST SP800-42, *Guideline on Network Security Testing*.
- NIST SP800-115, *Technical Guide to Information Security Testing and Assessment* .

Addressing People and Policy Risks

Training people to adopt security conscious behaviors and establishing policies for maintaining a secure environment go a long way toward improving an organization's overall security posture. The next two sections cover the people and policy dimensions of cyber security.

Cyber Security Policy

The corporate security policy expresses the management's commitment to securing critical assets and provides the framework for developing, implementing, and enforcing security controls. The policy document(s) must be available to all personnel who are required to comply with its requirements. Review and update the policy periodically.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	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 organization. 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.
	Define security-related roles and responsibilities.	Employees at virtually every organizational level have responsibility for some part of developing or applying security policies and procedures. Defined roles and responsibilities will clarify decision-making authority and responsibility at each level, along with expected behavior in policy implementation. Creating a multidisciplinary oversight committee ensures that all stakeholders are represented.
	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.
	Document a brief, clear, high-level policy statement for each issue identified.	The high-level policy statements express three things: • The organization management's commitment to the cyber security program. • The high-level direction and requirements for plans and procedures addressing each area. • A framework to organize lower-level documents.
	Reference lower-level policy documents.	Lower-level policies, plans, and procedures provide the details needed to put policy into practice.

✓	Activity / Security Control	Rationale
	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.
	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.

Security Policy Elements

The security policy should address the following, where applicable:

- Policy management
  - Purpose, scope, and applicability
  - Roles and responsibilities
  - Implementation and enforcement procedures
  - Exceptions
  - Policy reviews, approvals, and change management
- Personnel and training
  - Personnel risk assessment
  - Security awareness program
  - Cyber security training
- Critical asset management
  - Methodology for identifying critical cyber assets
  - Inventory and classification of cyber assets
  - Information protection and data privacy
  - Cyber vulnerability assessment
  - Access control, monitoring, and logging
  - Disposal or redeployment of assets
  - Maintenance and change control of the asset inventory and classifications

- Electronic security perimeter (ESP)
  - Critical assets within the perimeter
  - Cyber vulnerability assessment
  - Access control, monitoring, and logging
  - Configuration, maintenance, and testing
  - Documentation maintenance to support compliance
- Physical security
  - Critical assets within the perimeter
  - Access control, monitoring, and logging
- Incident reporting and response
- Disaster recovery and business continuity plans

Most of these topics are expanded in other sections of this guide. Note that the master security policy document may address some topics briefly and reference lower-level security policy documents, such as the following:

- *Human Resources Security Policy and Procedures*
- *Guidelines for Handling Sensitive Information Assets*
- *Physical Security Policy and Procedures*
- *Disaster Recovery and Business Continuity Plans and Procedures*
- *Asset Disposal Procedures*
- *Encryption Standard and Usage Guidelines*
- *Third-Party Software and Service Provider Standards*
- *Configuration Standards*
- *Data Backup Standard*

Security-Related Roles and Responsibilities

Everyone in the organization has a role in maintaining security. Define and document the roles and responsibilities of at least the following:

- The governing body for the security policy, e.g., an oversight board comprising representatives of stakeholder groups (engineering, legal, IT, etc.).
- A designated information security manager who maintains the policy and provides guidance for implementation and enforcement.
- Department managers who “own” the critical cyber assets and are responsible for implementing the security policies and procedures to protect those assets.
- Personnel with authorized access to critical assets who must review, provide feedback on, and comply with security policies.

Policy Implementation and Enforcement

Implementation and enforcement of security policies and procedures require defined processes to disseminate them effectively, ensure that they are understood and are available at all times, and enforce compliance (e.g., through audits and disciplinary actions for noncompliance).

Over time, organization or environmental changes will require changes to the security policy. Defined and documented processes for requesting, evaluating, and approving changes will ensure that the policy remains current and relevant.

Policy Exceptions

Policy exceptions occur for a variety of reasons. Simple examples include an overriding business need, a delay in vendor deliverables, new regulatory or statutory requirements, and temporary configuration issues. The exception process must ensure these circumstances are addressed in a manner that makes all stakeholders aware of the event, the risks, and the timeline for eliminating the exception.

Additional Guidance

- ISO 27001, *Information Security Management Systems—Requirements*.
- Chapter 5 in NIST SP800-12, *An Introduction to Computer Security: The NIST Handbook*.

Personnel and Training

Insufficiently trained personnel are often the weakest security link in the organization's security perimeter and are the target of social engineering attacks. It is therefore crucial to provide adequate security awareness training to all new hires, as well as refresher training to current employees on a yearly basis.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Adequately vet candidates for hire.	Provide a level of confidence that new hires are trustworthy.
	Establish a security-awareness program.	Ensure that all personnel have an understanding of sensitive information, common security risks, and basic steps to prevent security breaches. Further, ensure that personnel develop habits that would make them less susceptible to social engineering attacks.
	Train employees who have access to protected assets.	Ensure that employees who have electronic or physical access to critical assets know how to handle the assets securely and how to report and respond to cyber security incidents.

✓	Activity / Security Control	Rationale
	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.

Security Awareness and Training

The organization must establish, document, implement, and maintain a security awareness program for all personnel. The awareness program describes common security risks and how to avoid them. Awareness reinforcement should occur at least quarterly.

For personnel having authorized cyber access or authorized unescorted physical access to critical cyber assets, the organization should establish a training program that includes at least the following:

- The policies, access controls, and procedures developed for critical cyber assets.
- The proper use of critical cyber assets.
- The proper handling of critical cyber asset information.
- Action plans and procedures to recover or reestablish critical cyber assets, and the required access to these assets, following a cyber security incident.

Additional Guidance

- NIST SP800-16 Rev. 1, *Information Security Training Requirements: A Role- and Performance-Based Model.*
- SP800-50, *Building an Information Technology Security Awareness and Training Program*.

Due Diligence in Hiring

Diligence in the hiring and personnel review process is crucial. It is important to define and document a risk assessment program for personnel with authorized cyber access or authorized unescorted physical access to critical cyber assets. The program must comply with applicable laws and existing collective bargaining agreements. The risk assessment must include, at a minimum, identity verification and a seven-year criminal check. This information must be updated at least once every seven years (or for cause).

In addition, ensure that third-party vendors enforce similar checks for their personnel.

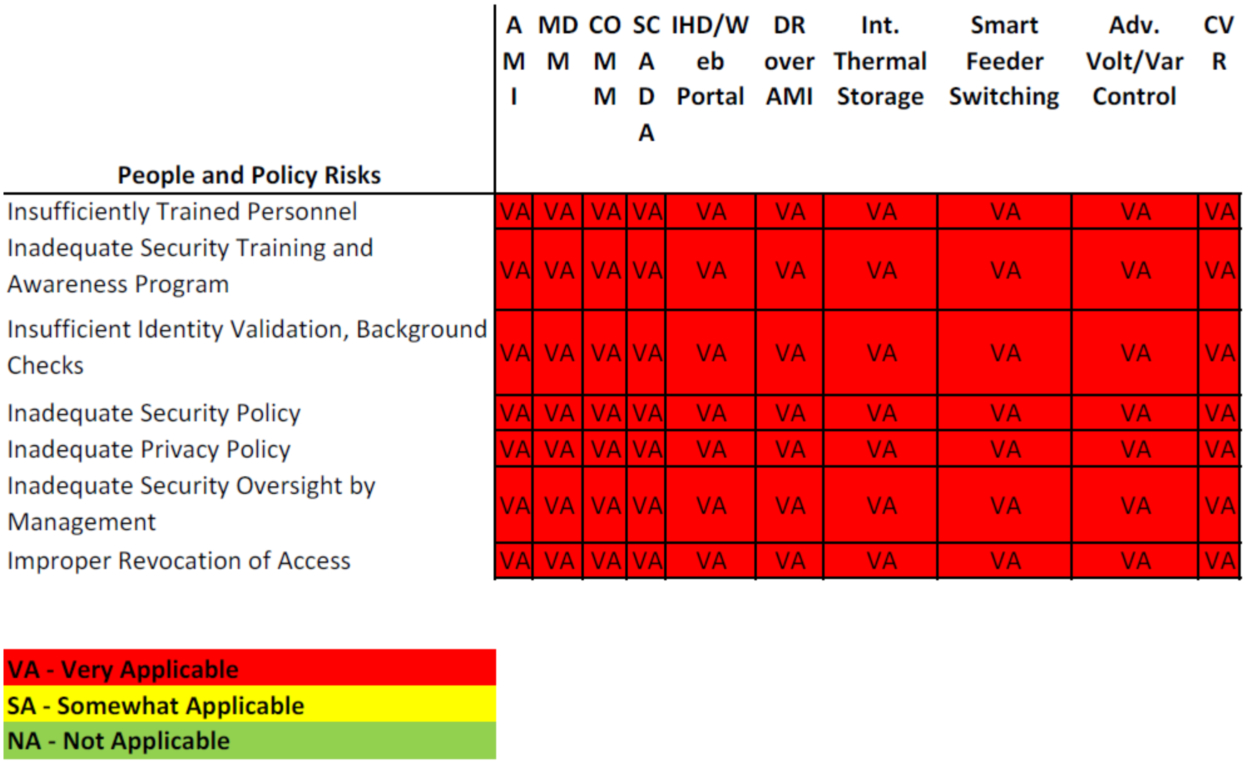
Access Privileges

Grant each employee the *lowest* levels of access to cyber assets and other privileges needed to do his or her job efficiently.

Maintain a list of all personnel who have authorized cyber access or authorized unescorted physical access to critical cyber assets. This list must include each person's specific electronic and physical access rights to such assets. Review the list quarterly and update it within seven days of any change in a list member's access rights.

Accesses must end (to avoid redundancy) *before* an employee is terminated for cause, and within seven days for personnel who no longer require such access.

Table 2. Summary of People and Policy Risks[12]



People and Policy Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Adv. Volt/Var Control	CVR
Insufficiently Trained Personnel	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Inadequate Security Training and Awareness Program	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Insufficient Identity Validation, Background Checks	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Inadequate Security Policy	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Inadequate Privacy Policy	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Inadequate Security Oversight by Management	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Improper Revocation of Access	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA

🟥 VA - Very Applicable

🟨 SA - Somewhat Applicable

🟩 NA - Not Applicable

[12] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Table 3. Impacts and Mitigations for People and Policy Risks[13]

People and Policy Risks	Potential Impact	Mitigations
Inadequate security training and awareness.	Insufficiently trained personnel may inadvertently provide the visibility, knowledge, and opportunity to execute a successful attack. An inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited. They may, for example: • Insert malicious USB sticks found in the parking lot into machines with access to control systems, providing attackers control over the control systems. • Hold the door for potential attackers carrying a big box entering a "secured premise," allowing them unauthorized access and physical proximity to critical / control systems. • Surf porn sites, which often compromise workstations with bots or worms. • Fail to respond to someone capturing wireless network traffic on the front lawn or parked in the guest parking lot. • Be careless with ID badges and credentials that can be leveraged to gain access to critical machines.	Ensure that the security training and awareness program is adequate to address the risks resulting from insecure behavior of employees. Ensure that all employees undergo security training when hired and at least once a year thereafter. The degree and nature of security training for personnel may vary based on their job function.
Insufficient identity validation, background checks	The human factor must always be considered the weakest element within any security posture; identity validation and background checks are measures that are imperative in managing this risk. As the amount and sensitivity of the information one is given responsibility for increases, consideration should be given to requiring separation of duties to ensure that no one individual is given the "keys to the kingdom."	Institute appropriate procedures to conduct background checks of all new hires. Further, prior to being granted access to sensitive information and resources, proper authentication and authorization mechanisms are required. The latter first verifies the identity of the party requesting access and then confirms that this party is authorized to access resources to which access is being requested.

[13] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

People and Policy Risks	Potential Impact	Mitigations
Inadequate security policy.	Vulnerabilities are often introduced due to inadequate or lacking policies. Policies need to drive operating requirements and procedures.	Ensure that security policies adequately cover all aspects of maintaining a secure environment.
Inadequate privacy policy.	Insufficient privacy policies can lead to unwanted exposure of employee or customer / client personal information, leading to both business risk and security risk.	Ensure that the privacy policies adequately cover all aspects of safeguarding access to private information.
Inadequate security oversight by management.	A lack of clear senior management ownership of a security program makes it almost impossible to enforce the provisions of the program in the event of a policy being compromised or abused.	Ensure that a senior manager is assigned responsibility for the overall security program at your organization. Empower this individual to make decisions to refine and enforce the security policies.
Improper revocation of access.	Failure to ensure that employee access is revoked when no longer needed may result in unauthorized access.	Ensure that employees have access to resources and systems only as needed to perform their job function and only for the duration that this need exists. Revoke all access for terminated employees before notifying them of termination.

Addressing Process Risks

Process gaps leave the door open to an adversary. For instance, failure to conduct a vulnerability assessment of a system when introducing new functionality may allow a security weakness to go undetected. To provide another example, lack of periodic review of system logs may let a breach go undetected. Instituting and following proper security processes is vital to the security of an organization.

Operational Risks

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions following the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Perform periodic risk assessment and mitigation, including threat analysis and vulnerability assessments.	Maintain a fresh picture of the effectiveness of the organization's security control versus threats facing the organization.
	Control, monitor, and log all access to protected assets.	Prevent unauthorized access to assets; detect unauthorized access to assets; enforce accountability.
	Redeploy or dispose of protected assets securely.	Ensure that the redeployment or disposal of cyber assets does not inadvertently expose sensitive information to unauthorized entities.
	Define and enforce secure change control and configuration management processes.	Ensure that system changes do not "break" security controls established to protect cyber assets.
	Create and document incident-handling policies, plans, and procedures.	Ensure that the organization is prepared to act quickly and correctly to avert or contain damage after a cyber security incident.
	Create and document contingency plans and procedures.	Ensure that the organization is prepared to act quickly and correctly to recover critical assets and continue operations after a major disruption.
	Train employees in incident-handling and contingency plans.	Ensure that personnel responsible for responding to cyber incidents or major disruptions have a firm grasp of the response plans and can execute them under stress.

Perform Periodic Risk Assessment and Mitigation

Your organization should define a risk management framework and periodically conduct risk assessments on your systems, along with mitigation, as appropriate. This process is defined in more detail earlier in this document in Building a Risk Management Program.

Enforce Access Control, Monitoring, and Logging

Access to critical cyber assets must be restricted to authorized users (human users or information system devices that represent human users) and the transactions those users are authorized to perform with the protected assets:

- Host all critical cyber security assets within a secure environment with appropriate perimeter protection.
- Deploy strong authentication controls to verify the identities of authorized users.

All cyber assets, where technically feasible, should include automated tools or organizational process controls to monitor cyber security-related system events. Document each of these automated mechanisms or processes. The monitoring function should log each detected cyber security incident and issue an alert. All such events should be reviewed and the log should be maintained for at least 90 days.

Perform Disposal or Redeployment of Assets

To ensure sensitive information is not released accidentally, the organization must document and implement formal methods, processes, and procedures for disposal or redeployment of cyber assets that are within an ESP. These include, at a minimum, destroying or erasing the data storage media and maintaining records of asset disposition.

Additional Guidance

- NIST SP800-88, *Guidelines for Media Sanitization*.

Enforce Change Control and Configuration Management

Managing change is essential to maintaining a robust ongoing security posture. Executive managers must establish and promulgate a change management process that is consistent with policy and compliance requirements. At a minimum, this process must address adding, modifying, replacing, or removing critical cyber asset hardware, software, or related documentation. The process must also address vendor-related changes to critical cyber assets.

Ensure that all documents produced as part of ESP documentation, assessment, and remediation are kept up to date with current physical and logical configurations. Update documents within 90 days of physical or logical changes.

Conduct Vulnerability Assessments

Perform a cyber vulnerability assessment of the access points to each ESP at least once a year. Include the following as a minimum:

- A description of the vulnerability assessment process
- A discovery of all access points to the ESP
- A review of ports and services configurations to verify that only the ports and services required for operation of the cyber assets within the perimeter are enabled
- A review of network and asset accounts, focusing on controls for default accounts
- Documented findings, a remediation plan, and the plan's execution status

See *Steps in Vulnerability Assessments* in Appendix E: Procedures for guidance about conducting a vulnerability assessment.

Additional Guidance

- NIST SP800-30, *Risk Management Guide for IT Systems*.
- DOE *Vulnerability Assessment Methodology—Electric Power Infrastructure*.[14]
- ISACA IS *Auditing Procedure, Security Assessment—Penetration Testing and Vulnerability Analysis.*[15]

Control, Monitor, and Log All Access to Assets

Document and implement mechanisms to control access at all electronic access points to the ESPs. These include technical and procedural controls (e.g., logs, user account review, account management, restricting use of shared accounts, password use) that enforce the authentication and accountability of all user activity.

Use an access control model whose default setting is to *deny* access, thereby requiring explicit permission changes to enable access. Similarly, for all access points, enable only the ports and services required for approved operations and monitoring. Remote interactive access to a point within the perimeter typically must be accompanied by strong procedural or technical controls to enforce authentication.

Electronic or manual processes for monitoring and logging usage of electronic perimeter access points must be documented and operational at all times. Where technically feasible, these processes must detect unauthorized access attempts and alert specified personnel.

If no alerting capability exists, review the access logs at least every 90 days. Electronic access logs typically are kept for at least 90 days.

Ensure that only the most limited access privileges are granted to fulfill the business need.

[14] DOE *Vulnerability Assessment Methodology—Electric Power Infrastructure* (http://www.esisac.com/publicdocs/assessment_methods/VA.pdf).

[15] ISACA IS *Auditing Procedure, Security Assessment—Penetration Testing and Vulnerability Analysis.*

Configuration and Maintenance

The organization must ensure that new cyber assets and significant changes to existing cyber assets do not adversely impact existing cyber security controls or the overall security posture of the system. Document and implement processes that help ensure ongoing system security, such as the following:

- Ensuring that all ports and services not required for normal and emergency operations are disabled.
- Tracking, evaluating, testing, and installing applicable cyber security patches for all cyber assets within the ESPs.
- Testing after the installation of security patches, cumulative service packs, and version upgrades (which are all considered significant changes).
- Using antivirus and malicious software prevention tools, where technically feasible.
- Defining and enforcing restrictions on who can perform maintenance and repair, emergency procedures, and remote configuration and maintenance.

Additional Guidance

- NIST SP800-83, *Guide to Malware Incident Prevention and Handling*.

Incident Handling

An *incident* is a breach of security or reliability protections that can potentially do harm—for example, the loss of confidentiality, integrity, or availability of data or operations. In addition to preventive measures to protect systems from the effects of security incidents, the reliability of the smart grid depends on the ability of participant organizations to quickly detect, report, and respond to incidents. Problems detected and correctly handled in time can prevent them from expanding or spreading to other entities.

A robust incident-handling capability requires planning, documented procedures, and ongoing training and rehearsal for all personnel who might be required to report, analyze, or respond to incidents. This capability begins with a clear policy statement of incident-handling requirements.

Additional Guidance

- *Incident Response Planning Items* in Appendix E: Procedures*.*
- NIST SP800-34, *Contingency Planning Guide for IT Systems*.
- NIST SP800-61, *Computer Security Incident Handling Guide*.
- NIST SP800-86, *Guide to Integrating Forensic Techniques into Incident Response*.

Contingency Planning

A *contingency* is any unplanned outage or failure of a system component. In addition to an incident-handling plan, organizations need policy, plans, and procedures for disaster recovery, continuity of operations, and possibly other contingency plans. Policy and plans must include preparation and training for responding to an emergency along with detailed procedures for executing defined strategies.

A *disaster recovery plan* applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. It includes the preparation (e.g., off-site storage of system backups), emergency facilities, and procedures for restoring critical cyber assets and infrastructure at an alternate site after an emergency.

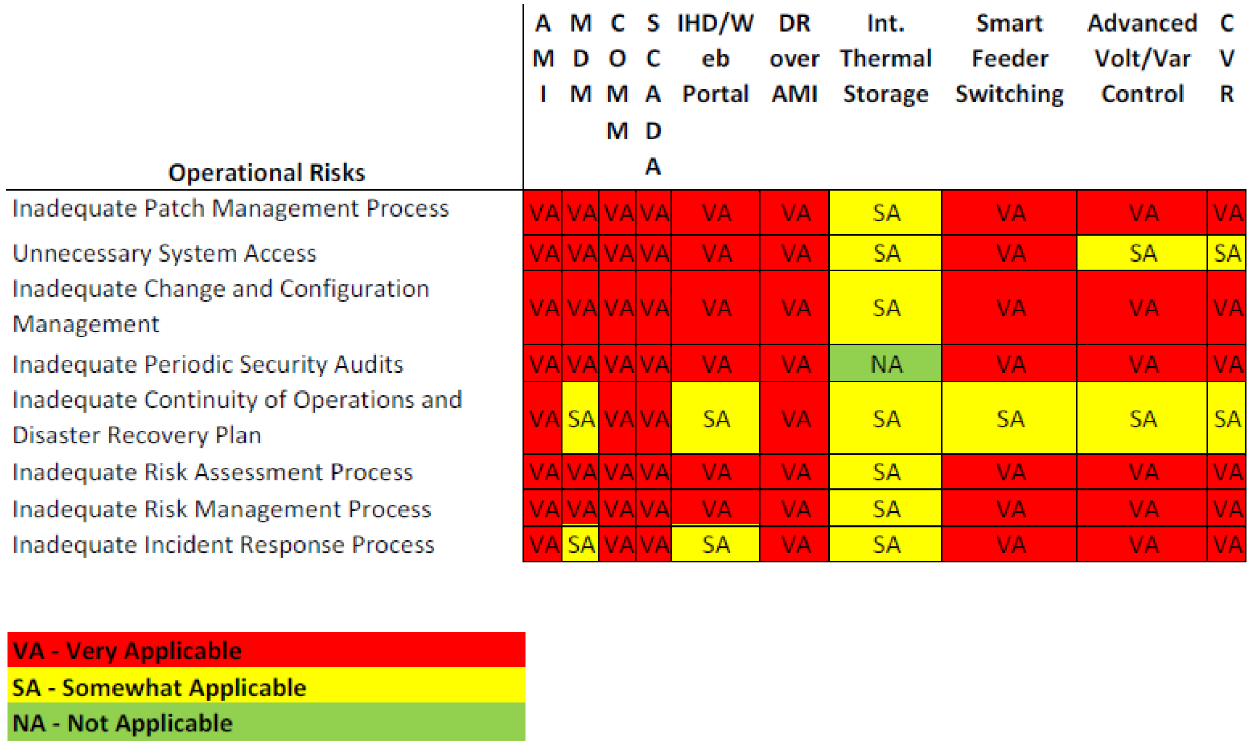
A *business continuity plan* focuses on sustaining an organization's mission/business functions during and after a disruption. A business continuity plan may be written for mission/business functions within a single business unit or may address the entire organization's processes.

Continuity and recovery plans define interim measures that increase the speed with which organizations resume service after disruptions. These plans must be tailored to each system. Creating specific measures requires a detailed understanding of specific scenarios.

Additional Guidance

- NIST SP800-34, *Contingency Planning Guide for IT Systems*.
- *Disaster Response Planning Items* in Appendix E: Procedures.

Table 4. Summary of Operational Risks[16]



Operational Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Inadequate Patch Management Process	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Unnecessary System Access	VA	VA	VA	VA	VA	VA	SA	VA	SA	SA
Inadequate Change and Configuration Management	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Inadequate Periodic Security Audits	VA	VA	VA	VA	VA	VA	NA	VA	VA	VA
Inadequate Continuity of Operations and Disaster Recovery Plan	VA	SA	VA	VA	SA	VA	SA	SA	SA	SA
Inadequate Risk Assessment Process	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Inadequate Risk Management Process	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Inadequate Incident Response Process	VA	SA	VA	VA	SA	VA	SA	VA	VA	VA

VA - Very Applicable

SA - Somewhat Applicable

NA - Not Applicable

[16] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Table 5. Impacts and Mitigations for Operational Risks[17]

Operational Risks	Potential Impact	Mitigation
Inadequate patch management process.	Missing patches on firmware and software have the potential to present serious risk to the affected system.	Automate the mechanism of monitoring and receiving alerts when new security patches become available. Make sure that security patches are applied at least weekly or more often as appropriate.
Unnecessary system access.	System access that is not managed can result in personnel obtaining, changing, or deleting information they are no longer authorized to access. Related problems include: • Administrators with false assumptions of what actions any one user may be capable. • One user (or many individual users) with sufficient access to cause complete failure or large portions of the electric grid. • Inability to prove responsibility for a given action or hold a party accountable. • Accidental disruption of service by untrained individuals. • Raised value for credentials of seemingly insignificant personnel.	Periodically review the access lists for each critical resource or system to ensure that the right set of individuals has authorized access. Establish standards procedures and channels for granting and revoking employee access to resources or systems.
Inadequate change and configuration management.	Improperly configured software/systems/devices added to existing software/systems/devices can lead to insecure configurations and an increased risk of vulnerability.	Ensure that all hardware and software are configured securely. When unclear, seek further clarification from vendors as to secure settings and do not assume that shipped default settings are secure. Establish change management and approval processes for making changes to the configuration to ensure that the security posture is not jeopardized.

[17] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Operational Risks	Potential Impact	Mitigation
Inadequate periodic security audits.	The audit process is the only true measure by which it is possible to continuously evaluate the status of the implemented security program in terms of conformance to policy, to determine whether there is a need to enhance policies and procedures, and to evaluate the robustness of the implemented security technologies. Failure to perform periodic security audits may lead to unidentified security risks or process gaps.	Ensure periodic security audits that focus on assessing security controls at the various levels, such as people and policy, operational, network, platform, application, process, physical security, and third-party relationships.
Inadequate continuity of operations and disaster recovery plan.	An inadequate continuity of operations or disaster recovery plan could result in longer-than-necessary recovery from a possible plant or operational outage.	It is essential to ensure within the various plant/system disaster recovery plans that are in place that an associated cyber contingency plan and cyber security incident response plan is developed. Each plant/system disaster recovery plan should highlight the need to determine if the disaster was created by or related to a cyber security incident. If such is the case, then part of the recovery process must be to ensure cyber incident recovery and contingency activities are implemented. This means taking added steps like validating backups, ensuring devices being recovered are clean before installing the backups, incident reporting, etc.
Inadequate risk assessment process.	Lack or misapplication of adequate risk assessment processes can lead to poor decisions based on inadequate understanding of actual risk.	A documented risk assessment process that includes consideration of business objectives, the impact to the organization if vulnerabilities are exploited, and the determination by senior management of risk acceptance is necessary to ensure proper evaluation of risk.

Operational Risks	Potential Impact	Mitigation
Inadequate risk management process.	Lack of an adequate risk management process may result in the organization focusing its resources on mitigating risks of little impact or likelihood, while leaving more important risks unaddressed.	Ensure that the organization's risk management process uses the results of the risk assessment process to initiate the timely and appropriate mitigation of risks in a fashion commensurate with their likelihood and impact. A systematic approach should be developed; an executive dashboard needs to show all risks where mitigations are past due.
Inadequate incident response process.	Without a sufficient incident response process, time-critical response actions may not be completed in a timely manner, leading to the increased duration of risk exposure.	An incident response process is required to ensure proper notification, response, and recovery in the event of an incident.

Insecure Software Development Life Cycle (SDLC) Risks

Secure software is a product of a secure software development process. If your organization develops software internally, you should make sure that it does so by leveraging security activities during the various phases of software development.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Document misuse / abuse cases.	Think of ways in which system functionality can be abused so that protections can be built in to prevent that abuse.
	Document security requirements.	Explicitly call out security requirements of the system so that software can be designed, implemented, and tested to ensure that these requirements have been met.
	Build a threat model.	Enumerate the ways in which an adversary may try to compromise the system so that the system can be designed from the get-go to resist such attacks.
	Perform architecture risk analysis.	Compare the system's architecture against a threat model to ensure that sufficient security controls are in place to prevent successful attacks.

✓	Activity / Security Control	Rationale
	Define secure implementation guidelines.	Ensure that developers use defensive programming techniques when implementing the system to avoid introducing security weaknesses.
	Perform secure code reviews.	Ensure 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.
	Perform risk-based security testing.	Run through the top risks identified during the threat modeling and architecture risk analysis process to ensure that the system has been designed and implemented in a way that mitigates these risks.
	Have penetration testing conducted.	Gain assurance from a qualified third party that the software built by your organization is secure.
	Create a secure deployment and operations guide.	Provide the teams deploying and operating the software in production with whatever knowledge they need to ensure that software security requirements are met.

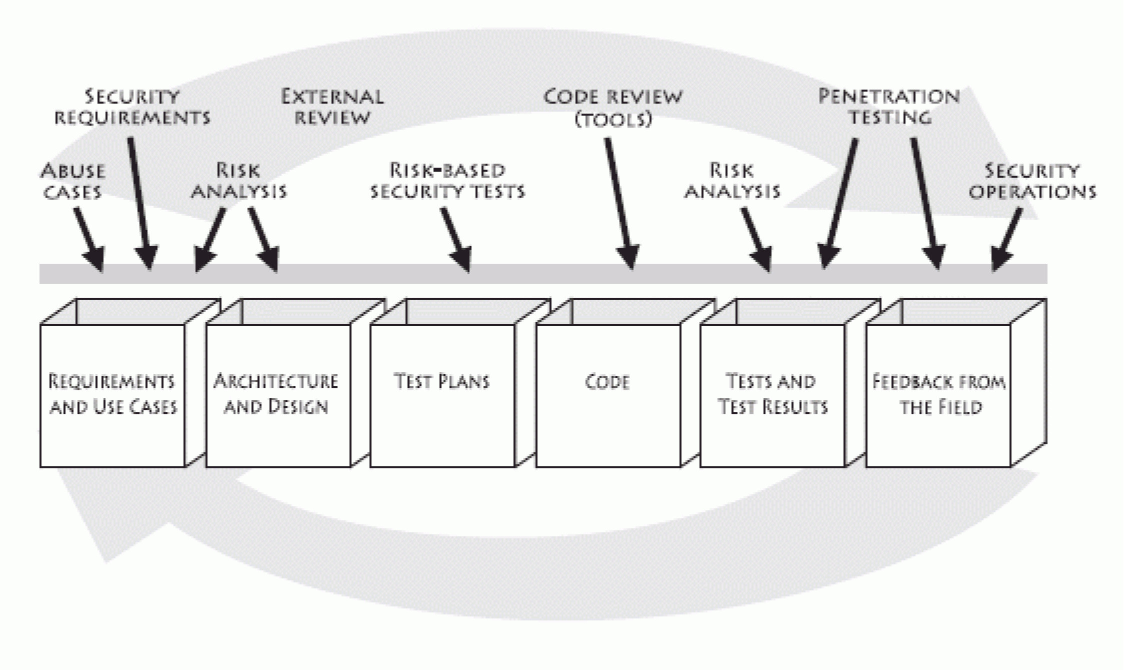


Figure 1. Seven Touch Points for Software Security[18]

- **Document misuse / abuse cases**

  Aside from documenting normal use cases, it is also important to consider ways in which the system's functionality can be misused / abused and to document these explicitly. This will help system designers and implementers to build prevention / detection mechanisms for attempts to misuse or abuse the system.

- **Document security requirements**

  It is important to explicitly document the security requirements that the system must meet. There are often implicit expectations for security, but when these are made explicit it allows the designers / implementers of the system to build in appropriate controls and testers of the system to create and execute tests to make sure that the security requirements have been met.

[18] From Gary McGraw, Software Security: Building Security In

- **Build a threat model**

  Threat modeling considers a system from the point of view of an adversary; there are various types of attacks to which a skilled attacker may subject a system. During the threat modeling phase, the goals of an attacker are considered in terms of which system assets may be compromised. To this end, the system's assets and attack surface (e.g., system entry points) are enumerated. Attack patterns that may enable an attacker to compromise the confidentiality, integrity, or availability of various system assets are then systematically documented. In this light, the effectiveness of the controls used to protect these assets is considered and possible weaknesses noted.

- **Perform architecture risk analysis**

  Architecture risk analysis considers the threat model of the system and asks the following questions:

  - Are the security controls being designed sufficient to protect the system from the attack patterns identified in the threat model and misuse / abuse cases?
  - Does anything in the system's design open up new attack vectors to an adversary?
  - Does the architecture / design of the system meet the documented security requirements?

  Architectural security flaws are then documented, along with the appropriate course of remediation.

- **Define secure implementation guidelines**

  It is important for your organization to define secure development guidelines to which your developers and architects should adhere. Also ensure that your staff is sufficiently trained in defensive programming and secure architecture techniques. Here are some industry sources of secure development guidelines, standards, and best practices:

  - Secure coding standards from CERT: https://www.securecoding.cert.org/confluence/display/seccode/CERT+Secure+Coding+Standards.
  - Guidance: www.owasp.org.
  - Common weakness enumeration: http://cwe.mitre.org.

- **Perform secure code reviews**

  An implementation security review is conducted to ensure that the mandated security controls have been properly implemented and that the implementation of the system does not in itself introduce any additional security weaknesses. This review leverages a combination of human expertise and applicable tools to yield optimal results.

- **Perform risk-based security testing**

  The role of risk-based security testing is to attempt the misuse / abuse cases defined earlier in the life cycle and also to attempt the various attack scenarios in the system's threat model. This will ensure that the design and implementation level controls that have been put in place to mitigate these abuse scenarios work as they should (e.g., they cannot be circumvented). Risk-based security tests should be defined early in the product life cycle and executed when testing of the integrated product commences.

- **Have penetration testing conducted**

  Penetration testing serves as the final verification to ensure that the system's security controls perform their functions properly. During this phase, all assumptions about the system are put aside in an attempt to undermine the security mechanisms built into the system. During this phase a combination of automated and manual techniques are used to emulate a real attacker trying to break into the system.

  All weaknesses identified as part of the security assessment are ranked using a risk-driven approach, considering the likelihood that they can lead to an exploit and the impact that a successful exploit would have. Pragmatic remediation guidance is given to the product team for each of the identified weaknesses.

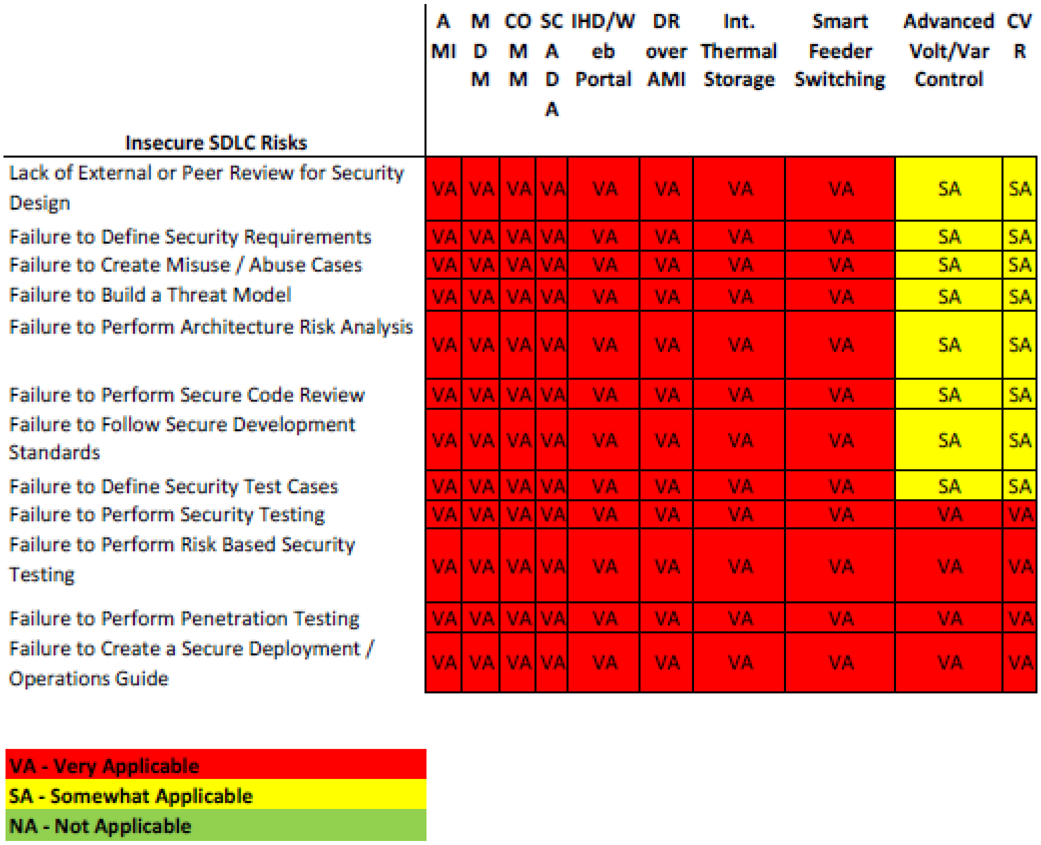
  It is always advisable that an external third party conduct a security test of the completed system within its production environment prior to the system going live. It is important to use a third party to ensure that no bias or assumptions internalized by system builders affect the security testing.

- **Create a secure deployment and operations guide**

  It is important to have a document that conveys any applicable product security configurations, assumptions, expectations, and operating instructions to the people who will be deploying and operating the software product. The secure deployment and operations guide can be a chapter within a broader deployment and operations guide or a stand-alone document.

  The tables following summarize insecure SDLC risks, impacts, and mitigations.

Table 6. Summary of Insecure SDLC Risks[19]



Insecure SDLC Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Lack of External or Peer Review for Security Design	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Define Security Requirements	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Create Misuse / Abuse Cases	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Build a Threat Model	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Perform Architecture Risk Analysis	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Perform Secure Code Review	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Follow Secure Development Standards	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Define Security Test Cases	VA	VA	VA	VA	VA	VA	VA	VA	SA	SA
Failure to Perform Security Testing	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Failure to Perform Risk Based Security Testing	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Failure to Perform Penetration Testing	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Failure to Create a Secure Deployment / Operations Guide	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA

🟥 VA - Very Applicable
🟨 SA - Somewhat Applicable
🟩 NA - Not Applicable

Table 7. Impacts and Mitigations for Insecure SDLC Risks[20]

Risks	Potential Impact	Mitigation
All insecure SDLC risks.	Failure to secure the SDLC during software development will leave the software susceptible to many application layer risks.	Ensure that your company secures the SDLC for any software developed internally and requests evidence from third-party software vendors that their organizations do likewise for any acquired software.

[19] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

[20] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Physical Security Risks

Physical security measures aimed at protecting critical infrastructure of the smart grid are of paramount importance and form a key element of the overall security strategy. While other controls need to exist for defense in depth in case the adversary is successful in gaining physical access, physical security concerns should not be underestimated.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Document, implement, and maintain a physical security plan.	Ensure that physical security is considered in a structured manner that can be tracked.
	The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
	All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server.	Ability to detect unauthorized access attempts. Take appropriate action if unauthorized access occurred.
	Physical access logs should be retained for at least 90 days.	Ability to perform historical analysis of physical access.
	Each physical security system must be tested at least once every three years to ensure it operates correctly.	Ensure that proper physical security posture is maintained.
	Testing and maintenance records must be maintained at least until the next testing cycle.	Ability to understand what was tested and improve testing procedures.
	Outage records must be retained for at least one calendar year.	Ability to investigate causes of outages and tie them to unauthorized physical access.

Particularly for field equipment, if an adversary gains access to a functioning piece of hardware, it might attempt to:

- Observe the communications of the field device with the rest of the smart grid to glean their syntax and semantic meaning in order to launch broader attacks.
- Impersonate that piece of equipment (or another similar piece of equipment) before the rest of the smart grid in order to feed malicious / inaccurate data to other components of the system.
- Extract any encryption keys / passwords used for communication. If these are stored on the device, it is essentially impossible to stop a dedicated attacker from extracting them.
- Use the access privileges / trusted relationship granted by the controlled device to gain access or launch attacks on other components of the smart grid.
- Modify the data sent from that piece of equipment to the other components on the smart grid.
- Observe any confidential / private data sent from the device.
- Launch denial-of-service attacks or distributed denial of service attacks if control was gained of many devices that can all be called into service at one time to perform some action.

The goal of physical security is to make it as hard as possible for the adversary to gain physical access to critical infrastructure. There should at a minimum be an alert to indicate if unauthorized physical access has been gained, which would notify system administrators to take appropriate action.

Plan and Protection

Senior managers must document, implement, and maintain a physical security plan. This plan must address, at a minimum:

- The protection of all cyber assets within an identified physical security perimeter or by way of alternate measures if a completely enclosed border is not feasible.
- The identification of all physical access points past the physical security perimeter and measures to control entry at those access points.
- Processes, tools, and procedures to monitor physical access to the perimeter(s).
- Appropriate use of physical access controls.
- Review of access authorization requests and revocation of access authorization.
- A visitor control program for personnel without authorized unescorted access to a physical security perimeter.
- Physical protection from unauthorized access and a location within an identified physical security perimeter for cyber assets that authorize or log access or monitor access to a physical or electronic security perimeter.
- Documentation and implementation of operational and procedural control to manage physical access at all access points at all times.

Monitoring, Logging, and Retention

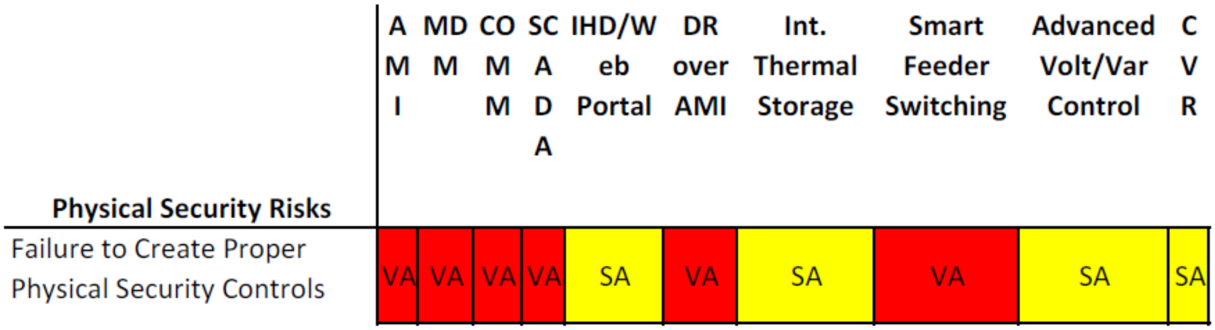
The organization must document and implement the technical and procedural controls for monitoring physical access at all access points at all times. Unauthorized access attempts must be reviewed immediately and handled in accordance with procedures. Logging will be sufficient to uniquely identify individuals and the time of access. Physical access logs should be retained for at least 90 calendar days.

Maintenance and Testing

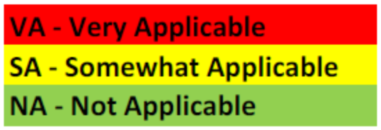
Each physical security system must be tested at least once every three years to ensure it operates correctly. Testing and maintenance records must be maintained at least until the next testing cycle. Outage records must be retained for at least one calendar year.

The tables below summarize physical security risks, impacts, and mitigations.

Table 8. Summary of Physical Security Risks[21]



Physical Security Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Failure to Create Proper Physical Security Controls	VA	VA	VA	VA	SA	VA	SA	VA	SA	SA



🟥	VA - Very Applicable
🟨	SA - Somewhat Applicable
🟩	NA - Not Applicable

Table 9. Impacts and Mitigations for Physical Security Risks[22]

Risks	Potential Impact	Mitigation
All physical security risks.	Failure to maintain proper physical security controls may adversely affect the confidentiality, integrity, and availability of the grid resources.	Physical security is an important layer of the overall security strategy and should be applied as appropriate. Physical security for SCADA is easier to implement than for field equipment.

Third-Party Relationship Risks

The security posture and practices of vendors and partners may introduce risks into an electric cooperative organization. If a cooperative acquires software from a vendor that did not pay attention to security during its development, that introduces a risk. If a cooperative utilizes a service from a provider who does not take proper precautions to safeguard the data that the cooperative places in its possession, that introduces a risk. These risks must be managed.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

[21] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

[22] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

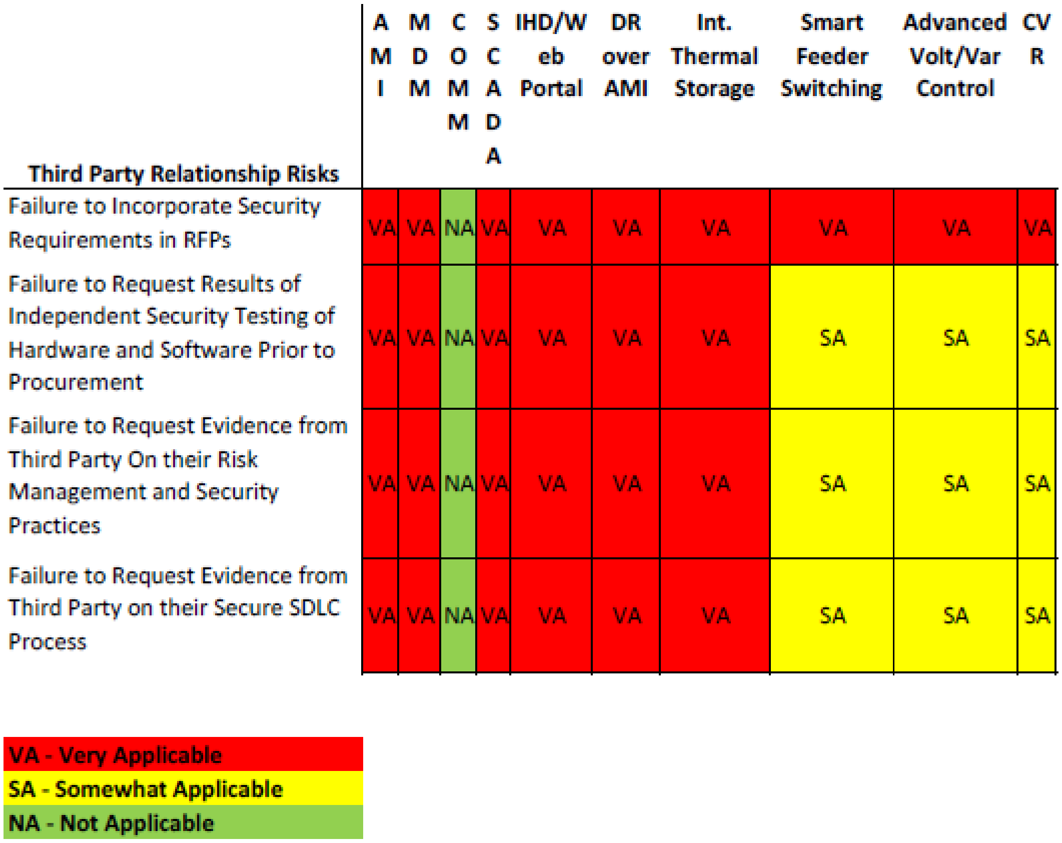
✓	Activity / Security Control	Rationale
	Perform due diligence on each vendor and partner organization to understand its business, financial, and security track record.	Verify the business, financial, and security reputation of your vendor / partner organization.
	Ask the right questions during the request for proposal (RFP) process to understand the security posture and practices of the partner organization, and whether their offerings meet security requirements. Compare the security policies and procedures of a third party against your organization's own security policy to ensure compliance.	Ensure that the security practices of the vendor / partner organization comply with those of your own organization. Ensure that the purchased product / service meets your organization's security requirements.
	Review the hiring practices and personnel background checks of your vendors and partners to ensure that they comply with your organization's policies.	Make sure that your vendor / partner organization's background checks during the hiring process are consistent with your own. Security issues at vendors translate into security issues in their products.
	Conduct periodic audits and monitoring of the third-party organization to ensure adherence to its security policies and procedures.	Make sure that your vendor / partner complies with its own security policies and procedures.
	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 your vendor / partner is secure.
	Ensure that service level agreements (SLAs) 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 your organization notified of the full extent of the breach as soon as the information is available.	A contractual obligation will help your organization transfer some of the security risks.
	Request evidence from software vendors that their software development lifecycle makes use of building security in activities.	Ensure that the product supplied to your organization by your vendor / partner has been designed and built with security in mind.
	Ask your organization's 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 your vendor / partner used in its product introduce security weaknesses.

A cooperative organization should take the following steps to reduce third-party relationship risks:

- Perform due diligence on each vendor and partner organization in order to understand its business, financial, and security track record.
- Ask the right questions during the RFP process to understand the security posture and practices at the partner organization, and whether their offerings meet the security requirements of your cooperative. Compare the security policies and procedures of a third party against your organization's own security policy to ensure compliance.
- Review the hiring practices and personnel background checks of your vendors and partners to ensure that they comply with your organization's policies.
- Conduct periodic audits and monitoring of the third-party organization to ensure adherence to their security policies and procedures.
- For software purchases, request a trusted independent third-party review, to include a report outlining the discovered security weaknesses in the product.
- Ensure that service level agreements (SLAs) 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 your organization notified of the full extent of the breach as soon as the information is available.
- Request evidence from software vendors that their software development lifecycle makes use of building security in activities.
- Ask your organizations' vendors and partners about the process that they use to ensure the security of the components and services that they receive from their own suppliers to ascertain appropriate due diligence.

The tables following summarize third-party relationship risks, impacts, and mitigations.

Table 10. Summary of Third-Party Relationship Risks[23]



Third Party Relationship Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Failure to Incorporate Security Requirements in RFPs	VA	VA	NA	VA	VA	VA	VA	VA	VA	VA
Failure to Request Results of Independent Security Testing of Hardware and Software Prior to Procurement	VA	VA	NA	VA	VA	VA	VA	SA	SA	SA
Failure to Request Evidence from Third Party On their Risk Management and Security Practices	VA	VA	NA	VA	VA	VA	VA	SA	SA	SA
Failure to Request Evidence from Third Party on their Secure SDLC Process	VA	VA	NA	VA	VA	VA	VA	SA	SA	SA

VA - Very Applicable

SA - Somewhat Applicable

NA - Not Applicable

[23] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Table 11. Impacts and Mitigations for Third-Party Relationship Risks[24]

Third-Party Relationship Risks	Potential Impact	Mitigation
Failure to incorporate security requirements in RFPs.	Acquisition of products that do not meet security requirements or ones for which security features are misunderstood.	Ensure that your organization's security requirements are reflected in the RFPs.
Failure to request results of independent security testing of hardware and software prior to procurement.	Acquisition of products that do not meet security requirements or ones for which security features are misunderstood.	Ask hardware and software vendors to have their products reviewed by third-party security experts and to share the report with your organization.
Failure to request evidence from a third party of its risk management and security practices.	Acquisition of products or consumption of services with an insufficient security posture.	Review your vendor's risk management and security practices and ensure that they adhere to your own standards.
Failure to request information from a third party on its secure SDLC process.	A SDLC process that does not follow security development practices will likely result in insecure software.	Secure software is the product of a secure software development process. Make sure that your software vendor follows one.

[24] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Addressing Technology Risks

Information technology (IT) is at the heart of the smart grid. As its spreading use helps the smart grid achieve higher operational efficiencies, it also makes the electrical grid more vulnerable to cyber security attacks. It is therefore important to ensure that the way in which IT is used does not inadvertently provide new avenues of attack to an adversary. Further, IT itself should be applied to institute security controls that will help guard the smart grid ecosystem against successful attacks, as well as enhance the system's ability to detect, isolate, and recover from breaches of security.

Network Risks

Networks are the communication pipes that connect everything together, enabling the flow of information. Networks are at the heart of the smart grid because without the information flow that they enable, smart behavior is not possible. For instance, a system load cannot be adjusted if information from smart meters does not find its way to the SCADA system. Therefore, the energy savings that result from adjusting a load cannot be realized, unless an action is taken based on reliable information that made its way from the smart meters to the SCADA via a communications network. On the other hand, if an adversary is able to tamper with meter data in a way that cannot be detected and to thus feed incorrect data to the SCADA, an incorrect action may be taken by the grid, resulting in undesired consequences.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Restrict user-assigned devices to specific network segments.	Least privilege through network segmentation.
	Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic moving from network segment to another of a different security level should default to a "deny all" stance.	Provide security by default.
	Requests for allowing additional services through a firewall or other boundary protection mechanism should be approved by the information security manager.	Centrally manage access according to business need.
	The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external	Confine sensitive electronic communication to established trust zones.

	systems, but should use an intermediate system in your organization's DMZ. The flow of traffic should be enforced through boundary protection mechanisms.	
	Protect data in transit.	Preserve the confidentiality and integrity of data in transit.
	Protect domain name service (DNS) traffic.	Ensure that data is routed to the right parties.
	Use secure routing protocols or static routes.	Avoid the disclosure of information on internal routing.
	Deny use of source routing.	Prevent denial-of-service attacks.
	Use technologies like firewalls and virtual local area networks (VLANs) to properly segment your organization's network in order to increase compartmentalization (e.g., machines with access to business services like e-mail should not be on the same network segment as your SCADA machines). Routinely review and test your firewall rules to confirm expected behavior.	Achieve network segmentation to achieve compartmentalization.
	Separate development, test, and production environments.	Avoid production data leaks into test environments. Have controls in place around access to and changes in the production environment.
	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 your network.	Secure data in transit.
	Ensure that proper certificate and key management practices are in place. Remember that 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.	Ensure that cryptographic protection is not undermined through improper certificate or key management.
	Ensure confidentiality of data traversing your networks. If channel-level encryption is not	Secure data in transit.

	possible, apply data-level encryption to protect the data traversing your network links.	
	Ensure integrity of data traversing your 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.	Preserve data integrity.
	Ensure availability of data traversing your networks. If a proper acknowledgement (ACK) is not received from the destination node, ensure that provisions are in place to resend the packet. If that still does not work, reroute the packet via a different network link. Implement proper physical security controls to make your network links harder to compromise.	Detect failures and promote fault tolerance.
	Ensure that only standard, approved, and properly reviewed communication protocols are used on your network.	Use proven protocols that have been examined for security weaknesses.
	Use intrusion detection systems (IDSs) to detect any anomalous behavior on your network. If anomalous behavior is encountered, have a way to isolate the potentially compromised nodes on your network from the rest of the network.	Detect intrusions.
	Ensure that sufficient number of data points exist from devices on your network before the smart grid takes any actions based on that data. Never take actions based on the data coming from network nodes that may have been compromised.	Avoid taking actions based on incorrect data.
	Ensure that all settings used on your network hardware have been set to their secure settings and that you fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.	Secure configuration.
	Disable all unneeded network services.	Reduce attack surface.
	Routinely review your network logs for anomalous / malicious behavior via automated and manual techniques.	Detect intrusion.

	Ensure that sufficient redundancy exists in your network links so that rerouting traffic is possible if some links are compromised.	Ensure continuity of operations.
	Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., nonshared) credentials.	Enforce accountability.
	Limit remote access to your networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPNs, IPSec) to create a secure tunnel after properly authenticating the connecting party using their individual credentials. In addition to a user name and password, also use an RSA ID-like device to provide an additional level of authentication.	Prevent unauthorized access.
	Implement remote attestation techniques for your field devices (e.g., smart meters) to ensure that their firmware has not been compromised	Prevent unauthorized modification of firmware on field equipment.
	Require a heartbeat from your field equipment at an interval known to the piece of equipment and to the server on your internal network. If a heartbeat is missed or comes at the wrong time, consider treating that piece of equipment as compromised / out of order and take appropriate action.	Detect tampering with field equipment.
	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.	Maintain accurate network time.
	Document the network access level that is needed for each individual or role at your organization and grant only the required level of access to these individuals or roles. All exceptions should be noted.	Maintain control over access to network resources and keep it to a necessary minimum.
	All equipment connected to your network should be uniquely identified and approved for use on your organization's network.	Control hardware that gets connected to your organization's network.

Network Connection Control

- **Restrict user-assigned devices to specific network segments**

  Devices should be authorized for connection to one network segment, but should not be authorized to connect to other network segments (e.g., segments where information of a higher security classification is stored, processed, and/or transmitted and the user of that device has not been granted access to information assets of that classification).

  User devices should be specifically prohibited from cross-connecting (i.e., acting as a router) between any two networks.

- **Firewall**

  Your organization's firewalls should be configured in accordance with the firewall configuration standard and the policy elements below:

  - Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic from one network segment to another of a different security level should default to a "deny all" status.
  - Firewalls should be configured to deny any of the following traffic types:
    - Invalid source or destination address (e.g., broadcast addresses, RFC 1918 address spaces on interfaces connected to public networks, addresses not assigned by IANA on interfaces connected to public networks).
    - Those destined for the firewall itself, unless the firewall provides a specific service (e.g., application proxy, VPN).
    - Source routing information.
    - Directed broadcasts that are not for the subnet of the originator (these can be used to create broadcast storms in denial-of-service attacks against third parties).
    - Those destined for internal addresses or services that have not been approved for access from external sources.
  - Requests for allowing additional services through a firewall or other boundary protection mechanisms should be approved by the information security manager.

- **Flow of electronic communications**

  The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external systems, but should use an intermediate system in your organization's DMZ. The flow of traffic should be enforced through boundary protection mechanisms.

- **Protecting data in transit**

  When any nonpublic classified data transits a network and the confidentiality and integrity of that data cannot be guaranteed because of the use of protocols which do not provide a mechanism for protecting the data payload, encryption should be used to guard against disclosure and modification of the data.

- **Protecting DNS traffic**

  The domain name service (DNS) should be deployed in a multitier architecture that protects internal systems from direct manipulation. Internal client resolvers should direct their queries to internal DNS servers, which forward all queries for external resource records to DNS server(s) in a DMZ. The flow of traffic should be enforced through boundary protection mechanisms.

Network Routing Control

- **Use of secure routing protocols or static routes**

  When exchanging routing information with external parties, secure routing protocols or static routes should be used. If possible, network address translation should be employed to prevent accidental leakage of internal routing information.

- **Deny use of source routing**

  Source routing should not be allowed. Users and devices should not be allowed to specify the routing of network traffic.

The list below summarizes some of the security controls that need to be in place to protect against network-based risks:

- Use technologies like firewalls and virtual local area networks (VLANs) to properly segment your organization's network and to increase its compartmentalization (e.g., machines with access to business services like e-mail should not be on the same network segment as your SCADA machines). Routinely review and test your firewall rules to confirm expected behavior.
- Separate development, test, and production environments.
- 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 your network.
- Ensure that proper certificate and key management practices are in place. Remember that 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.
- Ensure confidentiality of data traversing your networks. If channel-level encryption is not possible, apply data-level encryption to protect the data traversing your network links.[25]
- Ensure the integrity of data traversing your networks through use of digital fingerprints and signed hashes. If TLS is not used, ensure that other protections man in the middle attacks exist. Use time stamps to protect against replay attacks.[26]

[25] Leverage security extensions to the MultiSpeak® protocol.

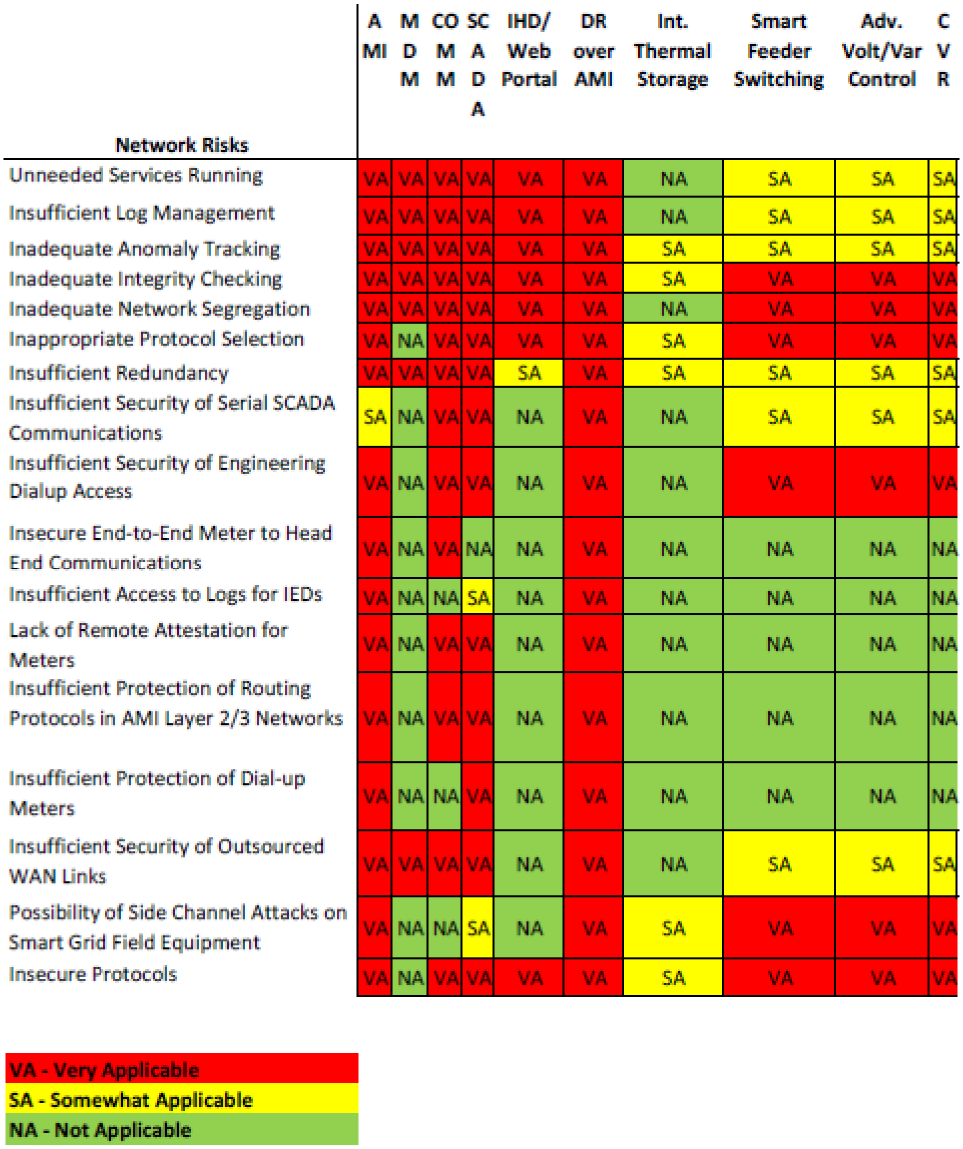
- Ensure the availability of data traversing your networks. If a proper acknowledgement (ACK) is not received from the destination node, ensure that provisions are in place to resend the packet. If that still does not work, reroute the packet via a different network link. Implement proper physical security controls to make your network links harder to compromise.
- Ensure that only standard, approved, and properly reviewed communication protocols are used on your network.
- Use Intrusion Detection Systems (IDSs) to detect any anomalous behavior on your network. If anomalous behavior is encountered, have a way to isolate the potentially compromised nodes on your network from the rest of the network.
- Ensure that a sufficient number of data points exist from devices on your network before the smart grid takes any actions based on that data. Never take actions based on the data coming from network nodes that may have been compromised.
- Ensure that all settings used on your network hardware have been set to their secure settings and that you fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.
- Disable all unneeded network services.
- Routinely review your network logs for anomalous / malicious behavior via automated and manual techniques.
- Ensure that sufficient redundancy exists in your network links so that rerouting traffic is possible if some links are compromised.
- Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., nonshared) credentials.
- Limit remote access to your networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPNs, IPSec) to create a secure tunnel after properly authenticating the connecting party using their individual credentials. In addition to user name and password, also use an RSA ID-like device to provide an additional factor of authentication.
- Implement remote attestation techniques for your field devices (e.g., smart meters) to ensure that their firmware has not been compromised.
- Require a heartbeat from your field equipment at an interval known to the piece of equipment and to the server on your internal network. If a heartbeat is missed or comes at the wrong time, consider treating that piece of equipment as compromised / out of order and take appropriate action.

[26] Leverage security extensions to the MultiSpeak® protocol.

- 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.
- Document the network access level that is needed for each individual or role at your organization and grant only the required level of access to these individuals or roles. All exceptions should be noted.
- All equipment connected to your network should be uniquely identified and approved for use on your organization's network.

The tables below summarize network security risks, impacts, and mitigations.

Table 12. Summary of Network Risks[27]



Network Risks	AMI	MDM	COMM	SCADA	IHD/ Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Adv. Volt/Var Control	CVR
Unneeded Services Running	VA	VA	VA	VA	VA	VA	NA	SA	SA	SA
Insufficient Log Management	VA	VA	VA	VA	VA	VA	NA	SA	SA	SA
Inadequate Anomaly Tracking	VA	VA	VA	VA	VA	VA	SA	SA	SA	SA
Inadequate Integrity Checking	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Inadequate Network Segregation	VA	VA	VA	VA	VA	VA	NA	VA	VA	VA
Inappropriate Protocol Selection	VA	NA	VA	VA	VA	VA	SA	VA	VA	VA
Insufficient Redundancy	VA	VA	VA	VA	SA	VA	SA	SA	SA	SA
Insufficient Security of Serial SCADA Communications	SA	NA	VA	VA	NA	VA	NA	SA	SA	SA
Insufficient Security of Engineering Dialup Access	VA	NA	VA	VA	NA	VA	NA	VA	VA	VA
Insecure End-to-End Meter to Head End Communications	VA	NA	VA	NA	NA	VA	NA	NA	NA	NA
Insufficient Access to Logs for IEDs	VA	NA	NA	SA	NA	VA	NA	NA	NA	NA
Lack of Remote Attestation for Meters	VA	NA	VA	VA	NA	VA	NA	NA	NA	NA
Insufficient Protection of Routing Protocols in AMI Layer 2/3 Networks	VA	NA	VA	VA	NA	VA	NA	NA	NA	NA
Insufficient Protection of Dial-up Meters	VA	NA	NA	VA	NA	VA	NA	NA	NA	NA
Insufficient Security of Outsourced WAN Links	VA	VA	VA	VA	NA	VA	NA	SA	SA	SA
Possibility of Side Channel Attacks on Smart Grid Field Equipment	VA	NA	NA	SA	NA	VA	SA	VA	VA	VA
Insecure Protocols	VA	NA	VA	VA	VA	VA	SA	VA	VA	VA

VA - Very Applicable

SA - Somewhat Applicable

NA - Not Applicable

[27] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Table 13. Impacts and Mitigations for Network Risks[28]

Network Risks	Potential Impact	Mitigation
Unneeded services running.	Many operating systems are shipped and installed with a number of services running by default: for example, in the UNIX case, an installation may automatically offer telnet, ftp, and http servers. Every service that runs is a security risk, partly because intended use of the service may provide access to system assets, and partly because the implementation may contain exploitable bugs. Services should run only if needed, and an unneeded service is a vulnerability with no benefit.	Perform analysis to identify all services that are needed, and only have these enabled. Establish a process for obtaining permission to enable additional services. Conduct periodic reviews to ensure that the services are running as expected.
Insufficient log management.	• Failure to detect critical events. • Removal of forensic evidence. • Log wipes.	Events from all devices should be logged to a central log management server. Alerts should be configured according to the criticality of the event or a correlation of certain events. For instance, when the tamper-detection mechanism on a device is triggered, an alert should be delivered to the appropriate personnel. When a remote power disconnect command is issued to *x* number of meters within a certain time, alerts should also be sent.

[28] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Network Risks	Potential Impact	Mitigation
Inadequate anomaly tracking.	Failure to understand the normal behavior of the system and tracking of anomalous behavior will reduce the ability to detect attacks on the system in real time.	Alerts and logging are two useful techniques for detecting and mitigating the risk of anomalous events but can present security risks or become vulnerabilities if not instituted thoughtfully. The appropriate reaction to an event will vary according to the criticality of the event or a correlation of certain events. The event may also need to be logged, and a central logging facility may be necessary for correlating events. Appropriate event reactions could include automatic paging of relevant personnel in the event of persistent tamper messages or may require positive acknowledgement to indicate supervisory approval has been attained before executing a potentially disruptive command (e.g., simultaneously disconnecting many loads from the electrical grid or granting control access rights to hundreds of users).
Inadequate integrity checking.	• Compromise of smart device, head node, or utility management servers. • Buffer overflows. • Covert channels. • Man-in-the-middle. • Denial of service or distributed denial of service (DoS / DDoS). Failure to apply integrity and confidentiality services where needed can result in vulnerabilities such as exposure of sensitive customer data, unauthorized modification of telemetry data, transaction replay, and audit manipulation.	The integrity of message protocol and message data should be verified before routing or processing. Devices receiving data not conforming to the protocol or message standard should not act on such traffic (e.g., forwarding to another device or changing its own internal state) as though the data were correctly received. Such verification should be done before any application attempts to use the data for internal processes or routing to another device. Additionally, special security devices acting as application-level firewalls should be used to perform logical bounds checking, such as preventing the shutdown of all power across an entire neighborhood area network (NAN). Most functions of the smart grid, such as demand response (DR), load shedding, automatic meter reading (AMR), time of use (TOU), and distribution automation (DA), require that data confidentiality and/or data integrity be maintained to ensure grid reliability, prevent fraud, and enable reliable auditing.

Network Risks	Potential Impact	Mitigation
Inadequate network segregation.	• Direct compromise of any portion of the network from any other portion of the network. • Compromise of the utility network from a NAN network. • VLAN hopping. • Network mapping. • Service / device exploit. • Covert channels. • Back doors. • Worms and other malicious software. • Unauthorized multihoming.	Network architectures often do a poor job of defining security zones and controlling traffic between security zones, thus providing what is considered to be a flat network, wherein traffic from any portion of the network is allowed to communicate with any other portion of the network. Smart grid examples of inadequate network segregation might include failure to install a firewall to control traffic between a head node and the utility company or failure to prevent traffic from one NAN to another NAN. It is important to plan your network carefully and utilize network segregation techniques to compartmentalize your network appropriately. For instance, workstations used to program PLCs should be segregated from all other systems.
Inappropriate protocol selection.	• Compromise of all authentication and payload data being passed. • Session hijacking. • Authentication sniffing. • Man-in-the-middle attacks. • Session injection. Use of unencrypted network protocols or weakly encrypted network protocols exposes authentication keys and data payload. This may allow attackers to obtain credentials to access other devices in the network and decrypt encrypted traffic using those same keys. The use of clear text protocols may also permit attackers to perform session hijacking and man-in-the-middle attacks, allowing the attacker to manipulate the data being passed between devices.	Ensure that appropriate protocols are used in order to provide adequate protection for the communication links. Either message-level or channel-level protection can be used. It is important to use proven protocols and proven implementation of these protocols. Before using any protocol, ensure that the security controls that it provides are sufficient to meet the security requirements that need to be enforced.
Insufficient redundancy.	Architecture does not provide for sufficient redundancy, thus exposing the system to intentional or unintentional denial of service.	Make proper use of redundancy in order to ensure continuity of operations in the event of a disaster or failure.

Network Risks	Potential Impact	Mitigation
Insufficient security of serial SCADA communications.	Insufficient message confidentiality and integrity may lead to sensitive data and grid operations being compromised.	Ensure that SCADA messages are protected for confidentiality and integrity where appropriate. The scheme used to provide these guarantees should not unacceptably impact performance.
Insufficient security of engineering dial-up access.	Weak authentication and shared credentials used in dial-up connections may impact confidentiality, integrity, and availability.	Ensure strong authentication and authorization for dial-up access with individual access credentials.
Insecure end-to-end meter to head end communications.	Insecure communication between meters and head ends may allow an attacker to modify messages or put their own message on the bus. For demand response over AMI, this may for instance mean that an attacker is able to set the temperature on the thermostats at people's homes to whatever he or she wants, thus affecting the households and the overall load on the electrical grid.	Secure end-to-end communications protocols such as TLS and IPSec ensure that the confidentiality and integrity of communications is preserved regardless of intermediate hoops. End-to-end security between meters and AMI head ends is desirable, and even between HAN devices and DR control services.
Insufficient access to logs for IEDs.	Not all IEDs create access logs. Due to limited bandwidth to substations, even where access logs are kept, they are often stranded in the substation. In order for a proper security event management (SEM) paradigm to be developed, these logs will need to become centralized and standardized so that other security tools can analyze their data. This is important in order to detect malicious actions by insiders as well as systems deeply penetrated by attackers that might have subtle misconfiguration as part of a broader attack.	A solution is needed that can operate within the context of the bandwidth limitations found in many substations as well as the massively distributed nature of the power grid infrastructure.
Lack of remote attestation for meters.	Lack of remote attestation for meters may enable compromised meters that are running tampered software to send fabricated information to the SCADA system. It may also be possible for attackers to use meters running tampered software to launch attacks against SCADA systems.	Remote attestation provides a means to determine whether a remote field unit has an expected and approved configuration. For meters, this means the meter is running the correct version of untampered firmware with appropriate settings and has always been running untampered firmware. Remote attestation is particularly important for meters, given the easy physical accessibility of meters to attackers.

Network Risks	Potential Impact	Mitigation
Insufficient protection of routing protocols in AMI layer 2/3 networks.	Insufficient channel level security on AMI networks may result in loss of data confidentiality, integrity, and availability.	In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless connectivity suffers from several well-known and often easily exploitable attacks, partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like the IEEE 802.11i and 802.11w security standards have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, because it is outside of the scope of routing protocols. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without end-to-end security (like IPsec), attacks such as eavesdropping, impersonation, and man-in-the-middle attacks could be easily mounted on AMI traffic. With end-to-end security in place, routing security is still required to prevent denial-of-service attacks.
Insufficient protection of dial-up meters.	Reusing older, time-proven technologies such as dial-up modems to connect to collectors or meters without understanding the subtle differences in application may provide loss of service or worse. Dial-up technology using plain old telephone service has been a preferred method for connecting to network gear, particularly where a modem bank providing 24, 48, or even 96 modems / phone numbers and other antiattack intelligence is used. However, dialing into a collector or modem and connecting, even without a password, can tie up a line and effectively become a denial-of-service attack. Consider a utility which, for the sake of manageability, places all its collectors or modems on phone numbers in a particular prefix. Every collector then can be hit by calling 202-555-WXYZ.	Assess the use of dial-up technology as a means for communication with meters. Consider alternate approaches to communicate with meters that reduce the risk of denial-of-service attacks.

Network Risks	Potential Impact	Mitigation
Insufficient security of outsourced wide area network (WAN) links.	Using external WAN links may facilitate network layer attacks unless the confidentiality and integrity of traffic is properly protected.	Consider where it is appropriate to use external WAN links and make sure that security trade-offs are understood. To provide a layer of channel security, leverage technologies like VPN, SSL, etc.
Possibility of side channel attacks on smart grid field equipment.	Side channel attacks may undermine the use of cryptography by extracting all or part of an encryption key from accessible field equipment.	Vendors of grid field equipment can employ various software and hardware techniques to make it more difficult to obtain cryptographic information from the device via side channel attacks. Vendors should be asked to describe what they have done to protect against these attacks during the procurement phase. Use physical security controls to make it more difficult to gain physical access to smart grid field equipment. If unauthorized physical access is gained, have controls in place to detect that.
Insecure protocols	Network protocols used as part of the smart grid may have been developed at different times and may have different levels of security. Use of insecure protocols may leave the data being transferred susceptible to eavesdropping, impersonation, or replay attacks.	Ensure that the network protocol being used meets the security requirements for data exchange between smart grid components. This protocol should have been reviewed and approved for use by your organization.

Platform Risks

Each accessible host on your organization's network is a potential target for attack. Adversaries will try to compromise these hosts via methods that cannot be mitigated through network security controls alone. It is imperative to ensure that the platform software running on your hosts is secure, including (but not limited to) operating system software, database software, Web server software, and application server software. Together these form a software stack on top of which your organization's custom applications run.

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure the latest security patches are applied to all software running on your network hosts.	Patch known weaknesses so that they cannot be exploited.
	Ensure that the latest antivirus / antimalware software runs regularly.	Detect known viruses and/or malware.
	Ensure that all unneeded services and interfaces (e.g., USB) are turned off on hosts.	Minimize the attack surface.
	Ensure that the hosts only run services and applications that are absolutely necessary.	Minimize the attack surface.
	Ensure that system logs are checked regularly and any abnormalities investigated.	Detect intrusions / attack attempts (both external and internal).
	Run software like tripwire to monitor for file system changes. Make sure that these changes are monitored.	Detect system infections with malware.
	Ensure that all access attempts and any elevation of privilege situations are properly logged and reviewed.	Detect intrusions / attack attempts (both external and internal).
	Ensure that passwords are of sufficient complexity and are changed periodically.	Prevent unauthorized access.
	Ensure that all security settings on your hosts are configured with security in mind.	Prevent unauthorized access.
	Ensure that shared (nonindividual) passwords are not used to access hosts or applications running on these hosts.	Allow for accountability; prevent unauthorized access.
	Ensure that authentication is required prior to gaining access to any services / applications running on your network hosts and that it cannot be bypassed.	Prevent unauthorized access.

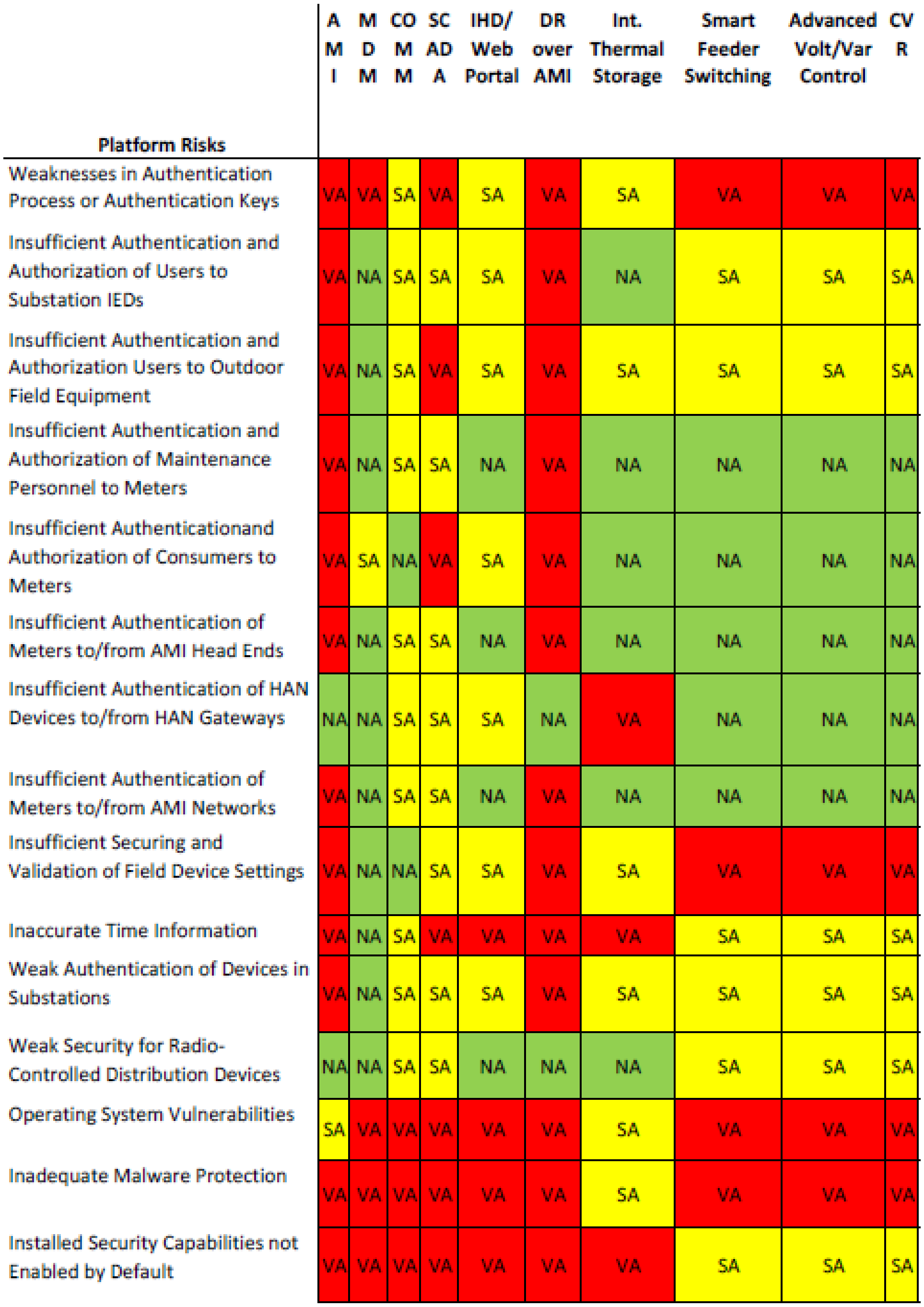
✓	Activity / Security Control	Rationale
	Make use of a centralized directory like LDAP to manage user credentials and access permissions. Ensure that users have only the minimum privileges needed for their job functions. If an elevation of privilege is needed, grant it for the minimum amount of time needed and then return the privileges to normal.	Enforce the principle of least privilege; prevent unauthorized access; make it easy to change passwords; make it easy to revoke access; and make it easy to enforce password complexity.
	Ensure that all software updates are properly signed and coming from a trusted source.	Set up malware protection.
	Prevent the ability to change field device settings without proper authentication. Changes to field device settings should be reported and logged in a central location. These logs should be reviewed frequently.	Maintain confidence in data coming from field devices by ensuring that they have not been tampered with.
	If possible, verify integrity of firmware running on field equipment via remote attestation techniques. Consult with the equipment vendor for assistance. If remote attestation fails, the affected field device should be considered compromised and should be isolated.	Maintain confidence in data coming from field devices by ensuring that they have not been tampered with.

The list below summarizes some of the security controls to mitigate platform-based risks:

- Ensure the latest security patches are applied to all software running on your network hosts.
- Ensure that the latest antivirus / antimalware software runs regularly.
- Ensure that all unneeded services and interfaces (e.g., USB) are turned off on hosts.
- Ensure that the hosts only run services and applications that are absolutely necessary.
- Ensure that system logs are checked regularly and any abnormalities investigated.
- Run software like tripwire to monitor for file system changes. Make sure that these changes are monitored.
- Ensure that all access attempts and any elevation of privilege situations are properly logged and reviewed.
- Ensure that passwords are of sufficient complexity and changed periodically.
- Ensure that all security settings on your hosts are configured with security in mind.
- Ensure that shared (nonindividual) passwords are not used to access hosts or applications running on these hosts.
- Ensure that authentication is required prior to gaining access to any services / applications running on your network hosts and that it cannot be bypassed.
- Make use of a centralized directory like LDAP to manage user credentials and access permissions. Ensure that users have only the minimum privileges needed for their job functions. If an elevation of privilege is needed, grant it for the minimum amount of time needed and then return the privileges to normal.
- Ensure that all software updates are properly signed and coming from a trusted source.
- Prevent the ability to change field device settings without proper authentication. Changes to field device settings should be reported and logged in a central location; these logs should be reviewed frequently.
- If possible, verify the integrity of firmware running on field equipment via remote attestation techniques. Consult with the equipment vendor for assistance. If remote attestation fails, the affected field device should be considered compromised and should be isolated.

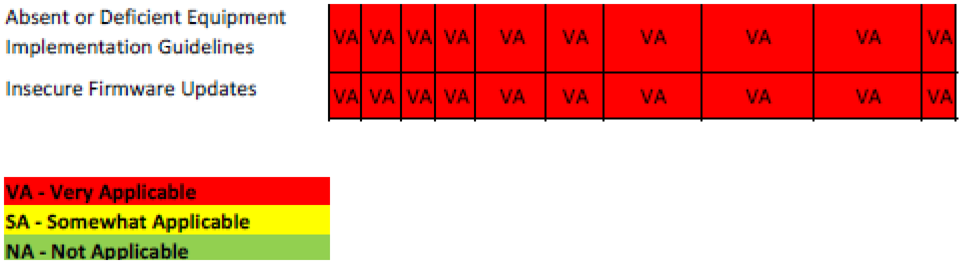
The tables following summarize platform security risks, impacts, and mitigations.

Table 14. Summary of Platform Risks[29]



Platform Risks	AMI	MDM	COMM	SCADA	IHD/ Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Weaknesses in Authentication Process or Authentication Keys	VA	VA	SA	VA	SA	VA	SA	VA	VA	VA
Insufficient Authentication and Authorization of Users to Substation IEDs	VA	NA	SA	SA	SA	VA	NA	SA	SA	SA
Insufficient Authentication and Authorization Users to Outdoor Field Equipment	VA	NA	SA	VA	SA	VA	SA	SA	SA	SA
Insufficient Authentication and Authorization of Maintenance Personnel to Meters	VA	NA	SA	SA	NA	VA	NA	NA	NA	NA
Insufficient Authenticationand Authorization of Consumers to Meters	VA	SA	NA	VA	SA	VA	NA	NA	NA	NA
Insufficient Authentication of Meters to/from AMI Head Ends	VA	NA	SA	SA	NA	VA	NA	NA	NA	NA
Insufficient Authentication of HAN Devices to/from HAN Gateways	NA	NA	SA	SA	SA	NA	VA	NA	NA	NA
Insufficient Authentication of Meters to/from AMI Networks	VA	NA	SA	SA	NA	VA	NA	NA	NA	NA
Insufficient Securing and Validation of Field Device Settings	VA	NA	NA	SA	SA	VA	SA	VA	VA	VA
Inaccurate Time Information	VA	NA	SA	VA	VA	VA	VA	SA	SA	SA
Weak Authentication of Devices in Substations	VA	NA	SA	SA	SA	VA	SA	SA	SA	SA
Weak Security for Radio-Controlled Distribution Devices	NA	NA	SA	SA	NA	NA	NA	SA	SA	SA
Operating System Vulnerabilities	SA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Inadequate Malware Protection	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Installed Security Capabilities not Enabled by Default	VA	VA	VA	VA	VA	VA	VA	SA	SA	SA

[29] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.



Absent or Deficient Equipment Implementation Guidelines	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Insecure Firmware Updates	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA

VA - Very Applicable

SA - Somewhat Applicable

NA - Not Applicable

Table 15. Impacts and Mitigations for Platform Risks[30]

Platform Risks	Potential Impact	Mitigation
Weaknesses in authentication process or authentication keys.	• DoS / DDoS • Man-in-the-middle attacks • Session hijacking • Authentication sniffing • Session injection	Enforce the appropriate lifespan for authentication credentials. Institute sound key management practices. Ensure secure key exchange. Ensure that the authentication process cannot be bypassed.
Insufficient authentication and authorization of users to substation IEDs.	An adversary may gain access to the IEDs if authentication passwords are weak, shared by all IEDs at the same company, and are seldom changed. Also, if all users use the same password to authenticate (i.e., not individual passwords), accountability becomes difficult to enforce.	Institute sound authentication and authorization practices for all field equipment.
Insufficient authentication and authorization of users to outdoor field equipment.	An adversary may gain access to outdoor field equipment if authentication passwords are weak, shared by all IEDs at the same company, and are seldom changed. Also, if all users use the same password to authenticate (i.e., not individual passwords), accountability becomes difficult to enforce.	Institute sound authentication and authorization practices for all field equipment.
Insufficient authentication and authorization of maintenance personnel to meters.	An adversary may gain access to meters if authentication passwords are weak, shared by all IEDs at the same company, and are seldom changed. Also, if all users use the same password to authenticate (i.e., not individual passwords), accountability becomes difficult to enforce. Commercially available meter configuration software does not provide a means to maintain distinct user and meter passwords.	Institute sound authentication and authorization practices to all field equipment.

[30] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Platform Risks	Potential Impact	Mitigation
Insufficient authentication and authorization of consumers to meters.	Failure to properly protect meters from consumers may result in incorrect data being reported to the control systems. For instance, billing accuracy could be jeopardized. Additionally, mass reporting of incorrect information from the meters may result in incorrect responses / behavior by the grid. Further, meters may be used as a footstep to attack other parts of the grid.	Ensure that consumers are not able to elevate their privileges in accessing the meters. Implement strong authentication and authorization techniques on the meters.
Insufficient authentication of meters to/from AMI head ends.	If AMI heads are not properly authenticated by the data being received from the meters, it may be possible to provide bogus data to the grid. This can affect billing, operations, etc.	It is important for a meter to authenticate any communication from an AMI head end in order to ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is important for an AMI head end to authenticate the meter, since usage information retrieved from the meter will be used for billing, and commands must be assured of delivery to the correct meter. As utilities merge and service territories change, a utility will eventually end up with a collection of smart meters from different vendors. Meter to/from AMI head end authentication should be interoperable to ensure that authentication and authorization information need not be updated separately on different vendor's AMI systems.

Platform Risks	Potential Impact	Mitigation
Insufficient authentication of HAN devices to/from HAN gateways.	Without such authentication, coordinated falsification of control commands across many HAN devices and/or at rapid rates could lead to grid stability problems.	Demand response (DR) HAN devices must be securely authenticated to the HAN gateway, and vice versa. It is important for a HAN device to authenticate any DR commands from the DR head end in order to prevent control by an adversary. It is important that the DR head end authenticate the HAN device both to ensure that commands are delivered to the correct device and that responses from that device are not forged. Interoperability of authentication is essential in order to ensure competition that will lead to low-cost consumer devices. This authentication process must be simple and fairly automatic, since to some degree it will be utilized by consumers who buy/rent HAN devices and install them. HAN devices obtained by the consumer from the utility may be preprovisioned with authentication information. HAN devices obtained by the consumer from retail stores may require provisioning through an Internet connection or may receive their provisioning through the HAN gateway. Should a HAN device fail to authenticate, it will presumably be unable to respond to DR signals. It should not be possible for a broad denial-of-service attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

Platform Risks	Potential Impact	Mitigation
Insufficient authentication of meters to/from AMI networks.	Meters and AMI networks are more susceptible to widespread compromise and denial-of-service attacks if no authentication and access control is provided in AMI access networks such as NANs and HANs.	Network access authentication tied with access control in the AMI access networks can mitigate the threat by ensuring that only authenticated and authorized entities can gain access to the NANs or HANs. In mesh networks, this "gatekeeper" functionality must be enforced at each node. The network access authentication must be able to provide mutual authentication between a meter and an access control enforcement point. A secure relationship between the meter and the enforcement point may be dynamically established using a trusted third party such as an authentication server.
Insufficient securing and validation of field device settings.	Numerous field devices contain settings. A prominent example is relay settings that control the conditions such as those under which the relay will trip a breaker. In microprocessor devices, these settings can be changed remotely. One potential form of attack is to tamper with relay settings and then attack in some other way. The tampered relay settings would then exacerbate the consequences of the second attack. The ability to tamper with field device settings is likely to facilitate many other types of attacks as well.	Mechanisms need to be in place to protect field device settings from unauthorized modification, as well as the ability to recognize when a particular field device may have had an unauthorized change in settings. Proper configuration management practices and ongoing verification of settings will be important.
Inaccurate time information.	Inaccurate time information will have an effect on: security protocols, synchrophasors, PKI certificates, event logs and forensics, etc.	Ensure that the absolute time source for the grid cannot be tampered with to provide inaccurate time.
Weak authentication of devices in substations.	An attacker who gains physical access to an external component can then eavesdrop on the communication bus and obtain (or guess) the MAC addresses of components inside the substation. Indeed, the MAC addresses for many components are often physically printed or stamped on the component. Once obtained, the attacker can fabricate packets that have the same MAC addresses as other devices on the network. The attacker may therefore impersonate other devices, reroute traffic from the proper destination to the attacker, and perform man-in-the-middle attacks on protocols that are normally limited to the inside of the substation.	Provide for strong network authentication among devices in substations.

Platform Risks	Potential Impact	Mitigation
Weak security for radio-controlled distribution devices.	Remotely controlled switching devices that are deployed on pole tops throughout distribution areas have the potential to allow for faster isolation of faults and restoration of services to unaffected areas. Some of these products that are now available on the market transmit open and close commands to switches over radio with limited protection of the integrity of these control commands. In some cases, no cryptographic protection is used, while in others the protection is weak, since the same symmetric key is shared among all devices. It may be possible for an adversary to spoof commands sent over the radio waves. An adversary may also try to jam certain radio frequencies in order to conduct a denial-of-service attack.	Ensure that any commands sent over the radio waves can be properly authenticated and authorized by the receiving party. Ensure that man-in-the-middle attacks or replay attacks are not possible. Additionally, having alternate modes of operation is of key importance to ensure continued operation if the radio frequencies being used are jammed.
Operating system vulnerabilities.	Vulnerabilities at the operating system level may help undermine the other security controls in place.	Ensure that you keep up with all the security patches issued by vendors.
Inadequate malware protection.	Malicious software can result in performance degradation; loss of system availability; and the capture, modification, or deletion of data. Malicious software may also affect the operation of grid hardware.	Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software. Additionally, be sure to keep up to date with all vendor security patches, apply sufficient network segregation, and conduct security awareness training for employees.
Installed security capabilities not enabled by default.	Security capabilities must obviously be turned on to be useful. There are many examples of operating systems (particularly pre-Vista Microsoft operating systems) where protections such as firewalls are configured but not enabled out of the box. If protections are not enabled, the system may be unexpectedly vulnerable to attacks. In addition, if the administrator does not realize that protections are disabled, the system may continue in an unprotected state for some time until the omission is noticed.	Take the time to understand the security features of all hardware and software products that are purchased by your organization and ensure that security features are configured correctly and are enabled as appropriate.

Platform Risks	Potential Impact	Mitigation
Absent or deficient equipment implementation guidelines.	Unclear implementation guidelines can lead to unexpected behavior.	A system needs to be configured correctly if it is to provide the desired security properties. This applies to both hardware and software configuration. Different inputs and outputs, both logical and physical, will have different security properties, and an interface that is intended for internal use may be more vulnerable than an interface designed for external use. As such, guidelines for installers, operators, and managers must be clear about the security properties expected of the system and how the system is to be implemented and configured in order to obtain those properties. When acquiring software or hardware, ensure that the vendor provides implementation guidelines that include security properties.

Platform Risks	Potential Impact	Mitigation
Insecure firmware updates.	Insecure firmware updates may allow the introduction of malware into critical grid equipment. As this malware can potentially alter the behavior of that equipment, the consequences can be grave.	The ability to perform firmware updates on meters in the field allows for the evolution of applications and the introduction of patches without expensive physical visits to equipment. However, it is critical to ensure that firmware update mechanisms are not used to install malware. This can be addressed by a series of measures that provide a degree of defense in depth. First, measures can be taken to ensure that software is created without flaws such as buffer overflows that can enable protection measures to be circumvented. Techniques for programming languages and static analysis provide a foundation for such measures. Second, principals attempting updates must be properly authenticated and authorized for this function at a suitable enforcement point such as on the meter being updated. Third, software can be signed in such a way that it can be checked for integrity at any time. Fourth, remote attestation techniques can provide a way to assess existing and past software configuration status so that deviations from expected norms can generate a notification or alarm event. Fifth, there must be a suitable means to detect a penetration of a meter or group of meters in a peer-to-peer mesh environment and isolate and contain any subsequent attempts to penetrate other devices. This is important, as it must be assumed that if an attacker has the capability to reverse-engineer a device, then any in-built protections can eventually be compromised as well. It is an open and challenging problem to conduct intrusion detection in a peer-to-peer mesh environment.

Application Layer Risks

In the platform risks section the discussion focused mainly on operating systems and other software making up the software stack on top of which your organization's custom applications run. If your organization develops or purchases custom software, it is important that it is developed with security in mind from the get-go to help ensure that it does not contain any software security weaknesses that may be exploited by adversaries to compromise your system. To do so your organization needs to makes your software development process security aware. The secure SDLC activities for doing so are documented in the "Insecure SDLC Risks" section under "Process Risks" earlier in this document.

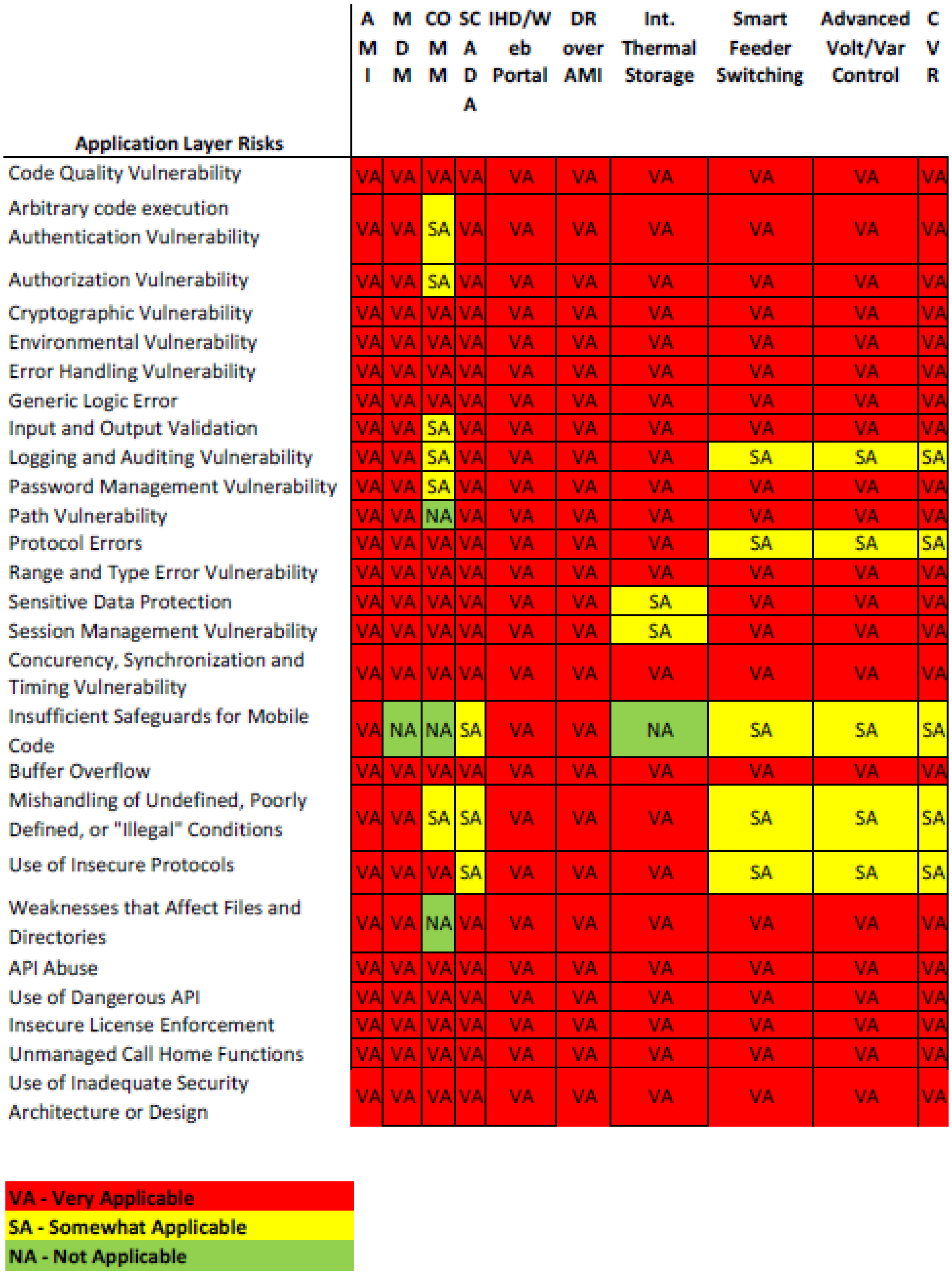
The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Implement security activities and gates into your organization's SDLC (please refer to the checklist in the "Insecure SDLC Risks" section for additional details).	Your organization develops software that does not have security weaknesses.
	Request independent party software security assessments of the applications being purchased to gauge the security posture of the software being purchased.	Gain confidence that the third-party software your organization purchases does not have security weaknesses.

At minimum, your organization should apply secure design practices and secure implementation practices (captured in secure development guidelines) to ensure that the security weaknesses enumerated in the table below are not introduced into your application. Further, you should establish regular secure design and code review practices, along with third-party penetration testing services to ensure that your system possesses an appropriate software security posture.

Ensure that all vendors building your software follow a secure development process. Request independent party software security assessments of the applications being purchased to gauge the security posture of the software being purchased. Please refer to the "Third-Party Relationship Risks" section under "Process Risks" earlier in this document.

Table 16. Summary of Application Layer Risks[31]



Application Layer Risks	AMI	MDM	COMM	SCADA	IHD/Web Portal	DR over AMI	Int. Thermal Storage	Smart Feeder Switching	Advanced Volt/Var Control	CVR
Code Quality Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Arbitrary code execution Authentication Vulnerability	VA	VA	SA	VA	VA	VA	VA	VA	VA	VA
Authorization Vulnerability	VA	VA	SA	VA	VA	VA	VA	VA	VA	VA
Cryptographic Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Environmental Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Error Handling Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Generic Logic Error	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Input and Output Validation	VA	VA	SA	VA	VA	VA	VA	VA	VA	VA
Logging and Auditing Vulnerability	VA	VA	SA	VA	VA	VA	VA	SA	SA	SA
Password Management Vulnerability	VA	VA	SA	VA	VA	VA	VA	VA	VA	VA
Path Vulnerability	VA	VA	NA	VA	VA	VA	VA	VA	VA	VA
Protocol Errors	VA	VA	VA	VA	VA	VA	VA	SA	SA	SA
Range and Type Error Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Sensitive Data Protection	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Session Management Vulnerability	VA	VA	VA	VA	VA	VA	SA	VA	VA	VA
Concurency, Synchronization and Timing Vulnerability	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Insufficient Safeguards for Mobile Code	VA	NA	NA	SA	VA	VA	NA	SA	SA	SA
Buffer Overflow	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Mishandling of Undefined, Poorly Defined, or "Illegal" Conditions	VA	VA	SA	SA	VA	VA	VA	SA	SA	SA
Use of Insecure Protocols	VA	VA	VA	SA	VA	VA	VA	SA	SA	SA
Weaknesses that Affect Files and Directories	VA	VA	NA	VA	VA	VA	VA	VA	VA	VA
API Abuse	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Use of Dangerous API	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Insecure License Enforcement	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Unmanaged Call Home Functions	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA
Use of Inadequate Security Architecture or Design	VA	VA	VA	VA	VA	VA	VA	VA	VA	VA

VA - Very Applicable

SA - Somewhat Applicable

NA - Not Applicable

[31] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Table 17. Impacts and Mitigations for Application Layer Risks[32]

Risks	Potential Impact	Mitigation
All application layer risks.	Exploitation of application layer weaknesses may result in a confidentiality, integrity, or availability impact on the system. For detailed assessment of potential impact for each individual weakness, refer to the Common Weakness Enumeration at http://cwe.mitre.org.	Ensure that all vendors building your software follow a secure development process. Request a third-party software security assessment of the applications being purchased. Defensive programming techniques to counteract weaknesses can be found in the Common Weakness Enumeration at http://cwe.mitre.org. For any software developed in-house, ensure that your organization follows a security-aware software development process as summarized in the "Insecure SDLC Risks" section under "Process Risks" section earlier in this guide.

[32] From NIST IR7628, Vol. 3, *Supportive Analyses and References*.

Unique Security Requirements and Controls For Each Smart Grid Activity Type

The remainder of this document walks through each of the 10 activity types that are part of the NRECA smart grid demonstrations and highlights the security / privacy requirements that are unique to each. Along with requirements, the sections also describe specific security best practices and controls needed to meet these requirements. Although many of these best practices and controls had already been noted earlier in this document (e.g., using color maps to show what risks are applicable to what activity types), our goal here is to specifically highlight unique security attributes for each smart grid activity type.

Advanced Metering Infrastructure (AMI)

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ask software and hardware (with embedded software) vendors for evidence (e.g., third-party assessment) that their software is free of software weaknesses.	Ensure that smart meters and their data is not compromised.
	Perform remote attestation of smart meters to ensure that their firmware has not been modified.	Ensure that smart meters and their data is not compromised.
	Make use of the communication protocol security extensions (e.g., MultiSpeak® security extensions) to ascertain the data integrity and origin integrity of smart meter data.	Ensure that smart meters and their data is not compromised.
	Establish and maintain secure configuration management processes (e.g., when servicing field devices or updating their firmware).	Ensure that smart meters and their data is not compromised.
	Ensure that all software (developed internally or procured from a third party) is developed using security-aware SDLC.	Ensure that smart meters and their data is not compromised.
	Apply a qualified third-party security penetration testing to test all hardware and	Ensure that smart meters and their data is not compromised.

	software components prior to live deployment.	
	Decouple identifying end-user information (e.g., household address, global positioning system [GPS] coordinates, etc.) from the smart meter. Use a unique identifier instead.	Preserve user privacy.
	Implement physical security controls and detection mechanisms when tampering occurs.	Ensure that smart meters and their data is not compromised.
	Ensure that a reliable source of network time is maintained.	Ensure that timely smart grid decisions are taken based on fresh field data.

Overview of Component / Solution

NIST states in the NIST IR7628, Vol. 3, that "the advanced metering infrastructure (AMI) consists of the communications hardware and software, together with the associated system and data management software, that creates a bi-directional network between advanced metering equipment and utility business systems, enabling collection and distribution of information to customers and other parties, such as competitive retail suppliers or the utility itself. AMI provides customers with real-time (or near-real-time) pricing of electricity and may help utilities achieve necessary load reductions."

Table 18. AMI Overview

Activity Type	**Advanced Metering Infrastructure (AMI)**	
Activity category:	Enabling technology for demand response (DR).	
Description of objectives:	AMI systems comprise state-of-the-art electronic and digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information as well as frequent collection and transmittal of such information to various parties.	
Major applications:	• A1—AMI Head-end • A3—Meter Data Management • A5—EA	• A6—Distribution State Estimation • A7—OMS • A9—GIS • A13—CIS

Key components:	• C8—PLC transceiver • C11—Meter (PLC)	• C10—Meter (PLC)
Standards / protocols:	• MultiSpeak • IEC 61968, Part 9 • Proprietary vendor AMI PLC protocols	• ANSI C12.22 • ZigBee Pro and SEP • Proprietary vendor AMI RF protocols

Unique Security Requirements and Controls

One fundamental security requirement for using AMI is to establish the trustworthiness of the meter from which the data originates. Since smart meters in the field are readily available, with few if any physical security controls, an attacker gaining physical access to the smart meter may "patch" their firmware, thereby compromising the smart meter. From this point on, any data supplied by the smart meter to the SCADA can no longer be trusted. If the attacker can repeat the same ploy on a broader scale, it may be possible for the adversary to induce the SCADA system to take incorrect action based on meter readings from compromised meters. Consequently, the ability of the SCADA to detect when a meter has been compromised and isolate it is of paramount importance.

It is important to note that an attacker need not gain physical access to many meters. Since meters are networked together, it would suffice for an attacker to gain access to one smart meter, download its firmware, reverse engineer the firmware to look for software vulnerabilities (e.g., buffer overflow), and then create a root kit that can exploit that vulnerability to modify the functionality of the smart meter. A worm can then be used to propagate that root kit from one smart meter to another via a network that connects them. An attacker may then have a botnet of compromised smart meters that he or she can activate at any time to achieve the attack goal (e.g., cause a blackout).

Many of the controls described earlier in this document can help to mitigate this vulnerability. The following actions are particularly applicable:

- Ask software and hardware vendors (with embedded software) vendors for evidence (e.g., third-party assessment) that their software is free of security weaknesses.
- Perform remote attestation of smart meters to ensure that their firmware has not been modified.
- Make use of communication protocol security extensions (e.g., MultiSpeak® security extensions) to ascertain the integrity, including the origin integrity, of smart meter data.
- Establish and maintain secure configuration management processes (e.g., when servicing field devices or updating their firmware).

- Ensure that all software (developed internally or procured from a third party) is developed using security-aware SDLC.
- Apply a qualified third-party security penetration test to all hardware and software components prior to live deployment.
- Ensure that the software running on the smart meter is free of software weaknesses, especially if they are remotely exploitable. Otherwise, an attacker may be able take control of a user's smart meter to begin manipulating the climate in the user's home. When done on a large scale, this may result in blackouts.
- Implement physical security controls and detection mechanisms when tampering occurs.
- Ensure that a reliable source of network time is maintained.
- Disable the remote disconnect feature that allows electricity to be remotely shut down using a smart meter.

One fundamental privacy requirement of AMI is to decouple specific smart meter information from end-user information in order to safeguard end-user privacy. For identifying the meter, a generic identification number should be used wherever possible rather than a specific household address, GPS location, etc.

Meter Data Management (MDM)

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Data arriving to be stored in the MDM system does not come from a compromised meter.	Only data from uncompromised meters is stored in the MDM system.
	Data arriving to be stored in the MDM system is syntactically and semantically valid.	Prevent storing bad data in the MDM system and prevent potentially harmful / malicious data from compromising the system.
	The system parsing the data arriving in the MDM system should make use of all the appropriate data validation and exception-handling techniques.	Prevent storing bad data in the MDM system and prevent potentially harmful / malicious data from compromising the system.

	The MDM system has been designed and implemented using security-aware SDLC.	Prevent storing bad data in the MDM system and prevent potentially harmful / malicious data from compromising the system.
	The MDM system has passed a security penetration test conducted by a qualified third party.	Prevent storing bad data in the MDM system and prevent potentially harmful / malicious data from compromising the system.
	Cleanse data stored in the MDM system from all private information.	Promote user privacy.
	Gracefully handle denial-of-service attempts (from compromised meters).	Protect the MDM system from attacks originating from smart meters.

Overview of Component / Solution

The MDM system processes and stores usage data and event information. This information can later be used for important analytics and data-mining purposes.

Table 19. MDM Overview

Activity Type	**Meter Data Management (MDM)**	
Activity category:	Enabling technology for demand response (DR).	
Description of objectives:	An MDM system performs long-term data storage and management of the data that is now being delivered by smart metering systems. This data consists primarily of usage data and events that are imported from AMI systems. An MDM system will typically import the meter data and then validate, edit, and evaluate (VEE) cleanse the data before making it available to end users.	
Major applications:	• A1—AMI Head-End • A2—Distribution SCADA • A3—Meter Data Management • A4—DR • A5—Engineering Analysis (DMS)	• A6—Distribution State Estimation (DMS) • A7—OMS • A13—CIS • A16—Load Forecast
Key components:	• None (component interfaces are via the AMI Head-End, Distribution SCADA, and DR systems)	
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9	• ANSI C12.19 • ZigBee SEP (1.0, 2.0)

Unique Security Requirements and Controls

It is important to ensure that the data that gets imported into the MDM system is thoroughly validated on a syntactic and semantic level. Your organization should ensure that:

- Data arriving to be stored in the MDM system does not come from a compromised meter.
- Data arriving to be stored in the MDM system is syntactically and semantically valid.
- The system parsing the data arriving in the MDM system should make use of all the appropriate data validation and exception-handling techniques.
- The MDM system has been designed and implemented using security-aware SDLC.
- The MDM system has passed a security penetration test by a qualified third party.
- Denial-of-service attempts (from compromised meters) are handled gracefully.

Further, it is important that the data stored in the MDM system is cleansed from all private information.

Communication Systems (COMM)

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure data integrity.	Secure communications.
	Ensure origin integrity.	Secure communications.
	Use proven communications protocols with built-in security capabilities.	Secure communications.
	Ensure confidentiality of data where appropriate.	Secure communications.
	Ensure proper network segmentation.	Promote compartmentalization, least privilege, isolation, fault tolerance.
	Have a third party perform network security penetration testing.	Receive greater assurance that communications are secure.
	Implement sufficient redundancy.	Fault tolerance.
	Protect from man-in-the-middle attacks.	Secure communications.

	Protect from replay attacks.	Secure communications.
	Use proven encryption techniques.	Secure communications.
	Use robust key management techniques.	Secure communications.

Overview of Component / Solution

The communication (COMM) system is responsible for networking all the smart grid devices together via a variety of different communication protocols.

Table 20. COMM Overview

Activity Type	**Communications System**	
Activity category:	Enabling technology for demand response (DR) and distribution automation (DA).	
Description of objectives:	Communication is the means of getting information from one piece of equipment to another. This could be using microwave, unlicensed spread spectrum, licensed UHF, and so on.	
Major applications:	Means of data transmission for HANs or LANs, for example, within substation or AMI RF mesh, and via WANs to support AMI backhaul from substation to operations office and / or communications to field distribution automation devices.	
Key components:	• UHF/VHF radios • Microwave radios • Unlicensed spread spectrum radios • ZigBee radios	• Fiber optics • Telco (for example, DSL) • Cellular
Standards / Protocols:	• ZigBee Pro / SEP • CDMA/GSM • Proprietary vendor licensed and unlicensed radios	• WiMAX • SONET (Telcordia GR-253-CORE) • Etc.

Unique Security Requirements and Controls

Please refer to the **Network Risks** section earlier in this document for a detailed description of network security risks and associated controls. There are a few particularly important security requirements associated with COMM:

- Ensure data integrity.

- Ensure origin integrity.
- Use proven communications protocols with built-in security capabilities.
- Ensure confidentiality of data where appropriate.
- Ensure proper network segmentation.
- Have a third party perform network security penetration testing.
- Implement sufficient redundancy.
- Protect from man-in-the-middle attacks.
- Protect from replay attacks.
- Use proven encryption techniques.
- Use robust key management techniques.

Supervisory Control and Data Acquisition (SCADA)

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Appoint a senior security manager with a clear mandate.	Make security somebody's responsibility.
	Conduct personnel security awareness training.	Help improve the people aspect of security.
	Apply basic network and system IT security practices (e.g., regular security patches, run antivirus software, etc.).	Make your SCADA environment more difficult to compromise.
	Ensure that software running in the SCADA environment (e.g., either internal or external) has been built with security in mind and reviewed for security by a qualified third party.	Protect from the perils of insecure software.
	Enforce the principle of least privilege when it comes to granting user access to SCADA resources.	Least privilege of access
	Ensure proper physical security controls.	Supplement IT security controls with physical

		controls.
	Perform monitoring and logging, and ensure that people can be held accountable for their actions.	Intrusion detection, forensic analysis, holding people accountable.
	Avoid taking critical control decisions without human confirmation.	Put the human operator in control.
	Avoid taking critical control decisions based on too few data points.	Avoid taking erroneous actions at the SCADA level.
	Avoid taking critical control decisions based on data points from compromised field devices or based on data that has been tampered with.	Avoid taking erroneous actions at the SCADA level.
	Ensure proper network segmentation in the SCADA environment.	Segregate critical control systems from the rest of your organization's corporate environment to promote compartmentalization.
	Ensure sufficient fault tolerance and redundancy in the SCADA environment.	Plan for failure and continuation of operations.
	Develop and test business continuity and disaster recovery plans.	Plan for failure and continuation of operations.
	Use individual (rather than shared) user login accounts with strong passwords.	Prevent unauthorized access and promote accountability.
	Ensure that all hardware authentication settings have been changed from their default values.	Prevent unauthorized access.

Overview of Component / Solution

Supervisory control and data acquisition (SCADA) forms the central control center of the smart grid that helps realize substation and distribution system automation. SCADA allows taking of real-time actions based on real-time data from the smart field devices.

Table 21. SCADA Overview

Activity Type	**Supervisory Control and Data Acquisition (SCADA)**	
Activity category:	Enabling technology for distribution automation (DA).	
Description of objectives:	SCADA provides the basic infrastructure to deploy basic and advanced substation and distribution system automation. It has the potential to vastly improve operational efficiencies, and provides the tools required by operators and engineers to become more productive in their jobs. It is a key component in the process of evolving the smart grid.	
Major applications:	• A2—Distribution SCADA • A4—DR • A5—Engineering Analysis • A6—Distribution State Estimation	• A7—OMS • A8—Distribution Automation
Key components:	• C1—Remote Terminal Unit (RTU) • C2—Automated Switch • C3—Capacitor Bank Controller	• C4—Voltage Regulator Control • C5—Intelligent Electronic Devices (IED) • C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850

Unique Security Requirements and Controls

Security requirements and needed controls for SCADA have already been covered earlier in this document. The following steps are particularly applicable:

- Appoint a senior security manager with a clear mandate.
- Conduct personnel security awareness training.
- Apply basic network and system IT security practices (e.g., regular security patches, run antivirus software, etc.).
- Ensure that software running in the SCADA environment (e.g., either internal or external) has been built with security in mind and reviewed for security by a qualified third party.
- Enforce the principle of least privilege when it comes to granting user access to SCADA resources.
- Ensure proper physical security controls.

- Perform monitoring and logging, and ensure that people can be held accountable for their actions.
- Avoid taking critical control decisions without human confirmation.
- Avoid taking critical control decisions based on too few data points.
- Avoid taking critical control decisions based on data points from compromised field devices or based on data that has been tampered with.
- Ensure proper network segmentation in the SCADA environment.
- Ensure sufficient fault tolerance and redundancy in the SCADA environment.
- Develop and test business continuity and disaster recovery plans.
- Use individual (rather than shared) user login accounts with strong passwords.
- Ensure that all hardware authentication settings have been changed from their default values.

In-Home Display (IHD) / Web Portal Pilots

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure that the software running on IHDs is free of weaknesses, especially if it is remotely exploitable.	Ensure that attackers cannot remotely control the IHDs of users.
	Ensure the integrity of data shown on users' IHDs.	Protect the integrity of data sent to the user.
	If the IHD can send data upstream (an unusual configuration), ensure the integrity of such communication.	Protect the integrity of data received from the user.
	Ensure the anonymity and privacy of data (where appropriate) pertaining to electricity usage patterns such that it cannot be tied back to the consumer.	Protect the privacy of users' electrical usage data.
	Perform remote the attestation of IHDs to	Know when IHDs have been tampered with

	alert the control center when unauthorized firmware updates occur.	and should no longer be trusted.
	Request third-party security penetration testing of IHDs.	Ensure that the deployed system has an adequate security posture.

Overview of Component / Solution

IHD/ Web portal pilots aim to capture adjustments in consumer behavior (e.g., in electricity usage) in cases where instantaneous information on electricity usage and pricing is available to the consumer.

Table 22. IHD/Web Portal Overview

Activity Type	**IHD / Web Portal Pilot**	
Activity category:	Demand response (DR).	
Description of objectives:	This program will study the consumer behavior modifications resulting from varying the energy price signals of residential electricity consumers. Critical peak pricing (CPP), time-of-use pricing (TOU), and a combination of these two rate signals will be studied. We will conduct an additional study on the interaction between these dynamic pricing signals and the existence of in-home energy-use displays and Internet-based energy-use Web portals. This program will also study the consumer behavior modifications resulting from the availability of data detailing users' electricity use.	
Major applications:	• A1—AMI • A3—MDM • A4—DR • A8—Distribution Automation • A13—CIS • A14—DRAS Server	• A15—Demand Management • A16—Load Forecast • A18—Market Services • A20—EMC
Key components:	• C9—Energy Services Interface • C10—Meter (RF) and / or C11—Meter (PLC) • C12—Customer EMS and IHD	• C13—Thermal Storage • C14—Thermostat • C17—Customer Appliances / Equipment
Standards / protocols:	• MultiSpeak® • IEC 61968, Part 9 • ANSI C12.19 and C12.22	• NAESB and OASIS • ZigBee SEP (1.0, 2.0) • HomePlug

Unique Security Requirements and Controls

Many of the security requirements and controls captured earlier in this document also relate to IHDs / Web portals. The following steps are particularly applicable:

- Ensure that the software running on IHDs is free of software weaknesses, especially if it is remotely exploitable. Otherwise, an attacker may be able take control of a user's IHD to begin manipulating the climate in the user's home. When done on a large scale, this may result in blackouts due to overloads.
- Ensure the integrity of data shown on the user's IHD.
- Ensure the integrity of data sent from the user's IHD to the control center.
- Ensure the anonymity and privacy of data (where appropriate) pertaining to electricity usage patterns such that it cannot be tied back to the consumer.
- Perform remote attestation of IHDs to alert the control center when unauthorized firmware updates occur.
- Request third-party security penetration testing of IHDs.

Demand Response over Advanced Metering Infrastructure (AMI) Networks

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Same activities and security controls as those described in the "AMI" section above.	
	Authenticate and validate all control signals coming from the control center to the smart meters.	Prevent unauthorized control of electric devices in the consumer's home.
	Provide consumers a feature to turn off remote control of in-house electric devices via smart meters. Since this capability would likely lead to some consumers turning off DM when conditions are extreme, such as in an extended heat wave, measures must be implemented to protect against this, such as disabling the turn-off function during such times.	Consumers should have a choice and also default overwrite ability if their smart meters become compromised.

Overview of Component / Solution

Demand response (DR) over AMI networks enables cooperatives to directly control the electrical devices of end users (e.g., water heaters, air conditioners) during high-cost periods by remotely adjusting their temperature or even shutting them down via smart meters. This could result in cost savings for the customer and better peak-load management for the cooperative.

Table 23. Demand Response over AMI Networks

Activity Type	**Demand Response over AMI Networks**	
Activity category:	Demand response (DR).	
Description of objectives:	This program will study the load impacts resulting from cooperative direct control of consumer water heaters and air conditioners. During high-cost periods, cooperatives will be able to remotely shut off end-users' water heaters and air conditioners.	
Major applications:	• A1—AMI • A3—Meter Data Management • A4—DR	• A13—CIS • A15—Demand Management • A15—Load Forecast
Key components:	• C8—PLC Transceiver • C9—Energy Services Interface • C10—Meter (RF) and / or C11—Meter (PLC) • C12—Customer EMS and IHD	• C13—Thermal Storage • C14—Thermostat • C16—Load Control Switch • C17—Customer Appliances / Equipment
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9 • ANSI C12.19 and C12.22	• ZigBee SEP (1.0, 2.0) • HomePlug

Unique Security Requirements and Controls

Many of the same security requirements and security controls that were outlined in the *Advanced Metering Infrastructure (AMI)* section also apply here. It is important to make sure that no remotely exploitable software weaknesses are present in the smart meter software that would allow an adversary to take control of the user's home electrical devices controlled by the smart meter. If that happens, it would certainly effect the consumer, and if done on a mass scale would affect the smart grid itself.

Also, it is important that all control commands coming from the control center to the smart meter that control consumer electrical devices are properly authenticated and validated.

Interactive Thermal Storage

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure that the software running on the device controlling electric water heaters is free of software weaknesses, especially if they are remotely exploitable.	Ensure that attackers cannot remotely control the electric water heaters of users.
	Request third-party security assessment of all software used to control electric water heaters.	Ensure that attackers cannot remotely control the electric water heaters of users.
	Conduct a security penetration test.	Ensure that attackers cannot remotely control the electric water heaters of users.
	Build in a mechanism to authenticate and validate control signals for electric water heaters.	Ensure that attackers cannot remotely control the electric water heaters of users.
	Build safeguards into the operation of electric water heaters (e.g., to prevent them from rising above a certain temperature, etc.).	Ensure human safety.
	Provide a manual override mechanism whereby users can prevent their electric water heaters from being controlled remotely.	Ensure human safety.

Overview of Component / Solution

The goal of this activity is to evaluate the potential of an electric water heater equipped with sophisticated control technology to serve as a distributed thermal storage unit.

Table 24. Interactive Thermal Storage

Activity Type	Interactive Thermal Storage	
Activity category:	Demand response (DR).	
Description of objectives:	This demonstration activity will test and study the potential of using electric water heaters equipped with sophisticated control technology as distributed thermal storage units. The core conflict in direct load management is that consumers will perceive service degradation (in the form of increased household temperatures or of running out of hot water on demand). Historically, one approach to extending the control period without inconvenience to the end user was to encourage larger units with heavy insulation and high efficiencies. New technologies are superior in providing much more sophisticated control by preheating water to 170 degrees ahead of the desired control period. Coupled with cold-water mixing valves, this substantially extends water heater control periods. If proven effective, this technology could serve to firm up wind generation or be bid into ancillary services markets.	
Major applications:	• A1—AMI • A4—DR	• A14—DRAS Server
Key components:	• C9—Energy Services Interface • C12—Customer EMS and IHD	• C13—Thermal Storage • C17—Customer Appliances / Equipment
Standards / Protocols:	• MultiSpeak® • IEC 61968, Part 9	• Proprietary PLC • ZigBee SEP • Home Plug

Unique Security Requirements and Controls

The main security concern is an adversary gaining unauthorized control of a user's electric water heater and causing it to overheat and possibly explode. A human life can be on the line if this technology is abused. There is also the possibility of impacting the grid itself if an adversary is able to remotely control the electric water heaters of many users at once.

It is important to ensure that central control signals arriving at the consumer's electric water heater are sufficiently validated and authenticated. Further, the software running on the device needs to be free of security weaknesses, especially those that can be exploited remotely.

It is also important for users to have a manual override mechanism to prevent their electric water heaters from being controlled by remote control signals. Further, some safeguards need to be in place for the operation of the water heater, such as those that prevent it from heating above a certain temperature, regardless of the control signals.

Smart Feeder Switching

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure that the software controlling smart feeder switching is free of security weaknesses.	Prevent unauthorized electrical power grid reconfiguration.
	Implement physical security controls and detection mechanisms when tampering occurs.	Prevent unauthorized electrical power grid reconfiguration.
	Perform sufficient authentication and validation of all control data used to reconfigure the electrical distribution network.	Prevent unauthorized electrical power grid reconfiguration.
	Ensure that a human(s) has to review and authorize any electrical distribution network reconfiguration.	Prevent unauthorized electrical power grid reconfiguration.
	Build safeguards into the hardware.	Ensure safe behavior when failures occur.

Overview of Component / Solution

Smart feeder switching technology is used to improve system reliability and fault tolerance by redirecting electrical power from a route where some failure occurs (e.g., when a power line is down due to fallen trees) via an alternate route.

Table 25. Smart Feeder Switching

Activity Type	**Smart Feeder Switching**	
Activity category:	Distribution automation (DA).	
Description of objectives:	Smart feeder switching entails the automated network reconfiguration of electrical distribution networks to minimize interruptions and improve system reliability. Technically known as fault location, isolation, and service restoration (FLISR), this system should produce substantial improvements in the System Average Interruption Duration Index (SAIDI) and other indices.	
Major applications:	• A2—Distribution SCADA	• A8—Distribution Automation
Key components:	• C2—Automated Switch	
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850

Unique Security Requirements and Controls

It is important to prevent adversaries from being able to exploit smart feeder switching to perform unauthorized reconfiguration of the electrical grid, as this may have a possibly catastrophic impact on both the grid and human life. While many other relevant security controls have been described earlier in this document, here are few specific ones:

- Ensure that the software controlling smart feeder switching is free of security weaknesses.
- Implement physical security controls and detection mechanisms in case tampering occurs.
- Perform sufficient authentication and validation of all control data used to reconfigure the electrical distribution network.
- Ensure that a human(s) has to review and authorize any electrical distribution network reconfiguration.
- Be sure that safeguards are built into the hardware.

Advanced Volt/VAR Control

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure that the software controlling distribution feeders is free of security weaknesses.	Prevent unauthorized control of distribution feeders.
	Implement physical security controls and detection mechanisms when tampering occurs.	Prevent unauthorized control of distribution feeders.
	Perform sufficient authentication and validation of all control data bound for distribution feeders.	Prevent unauthorized control of distribution feeders.
	Design automatic control systems to operate with a human "in the loop" when time permits.	Prevent unauthorized control of distribution feeders.
	Be sure that safeguards are built into the hardware.	Ensure safe behavior in case failures occur.

Overview of Component / Solution

Advanced volt/VAR control of distribution feeders facilitates improvement in power delivery while minimizing energy losses.

Table 26. Advanced Volt/VAR

Activity Type	Advanced Volt/VAR	
Activity category:	Distribution automation (DA).	
Description of objectives:	Volt/VAR control of distribution feeders will result in improved voltage support on long distribution feeders while also minimizing distribution line energy losses.	
Major applications:	• A2—Distribution SCADA • A6—Distribution State Estimation	• A8—Distribution Automation

Key components:	• C3—Capacitor Bank Controller	• C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850

Unique Security Requirements and Controls

One key security requirement for advanced volt/VAR control is to prevent adversaries from making unauthorized changes that may impact the reliability or correct operation of the smart grid (e.g., energy losses, unwanted voltage changes, etc.). As such, all control signals to distribution feeders need to be properly authenticated and validated. Additionally, any software used to control volt / VAR needs to be free of security weaknesses, and sufficient physical security controls should be in place.

Conservation Voltage Reduction (CVR)

The following checklist summarizes the various security best practices and controls that you should consider implementing. For more details on any of the activities / security controls, please refer to the descriptions that follow the checklist in the body of the section.

✓	Activity / Security Control	Rationale
	Ensure that the software controlling voltage regulators and monitors is free of security weaknesses.	Prevent unauthorized voltage reduction behavior.
	Implement physical security controls and detection mechanisms in case tampering occurs.	Prevent unauthorized voltage reduction behavior.
	Perform sufficient authentication and validation of all control data bound for voltage regulators and coming from voltage monitors.	Prevent unauthorized voltage reduction behavior.
	Ensure that a human(s) has to review and authorize any changes to voltage.	Prevent unauthorized voltage reduction behavior.
	Be sure that safeguards are built into the hardware.	Ensure safe behavior when failures occur.

Overview of Component / Solution

Conservation voltage reduction (CVR) is used to reduce peak voltage to a slightly lower (yet acceptable) level to achieve cost savings during high-price energy peaks.

Table 27. Conservation Voltage Reduction (CVR)

Activity Type	**Conservation Voltage Reduction (CVR)**	
Activity category:	Distribution automation (DA).	
Description of objectives:	Conservation voltage reduction is typically employed to accomplish the reduction of peak demand during certain times of the day. Peak demand reduction during coincident peaks results in substantial wholesale power demand cost savings for utilities.	
Major applications:	• A2—Distribution SCADA	• A8—Distribution Automation
Key components:	• C4—Voltage Regulator Control	• C7—Voltage Monitor
Standards / Protocols:	• MultiSpeak® • ICCP IEC 60870-6/TASE.2	• DNP3 • IEC 61850

Unique Security Requirements and Controls

One key security requirement for CVR is to prevent adversaries from making unauthorized changes that may impact the reliability or correct operation of the smart grid (e.g., significant voltage reduction). As such, all requests to voltage regulator control need to be properly authenticated and validated. It is also important to ensure that data from voltage monitors has not been tampered with since an adversary may attempt to make the system mistakenly believe that voltage can be reduced.

In addition, any software used to control voltage regulators and voltage monitors needs to be free of security weaknesses, and sufficient physical security controls should be in place.

Appendix A: Reference Documentation

Security Standards

International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005. Specification for an information security management system. Must be purchased. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

International Organization for Standardization/International Electrotechnical Commission 27002, *Code of Practice for Information Security Management,* 2005. Best practices for developing and deploying an information security management system. Must be purchased. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. Categorizing impact levels of information assets, deriving system-level security categorization. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. Guidelines for using the security profiles and controls cataloged in NIST SP800-53; families of security controls, minimum requirements for high-, moderate-, and low-impact systems. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

National Institute of Standards and Technology Special Publications

National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995. Elements of security, roles and responsibilities, common threats, security policy, program management. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. Learning-continuum model, security literacy and basics, role-based training. http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002. Risk management, assessment, mitigation. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009. Security control fundamentals, baselines by system-impact level, common controls, tailoring guidelines, catalog of controls in 18 families. http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf.

National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008. Security objectives and types of potential losses, assignment of impact levels and system security category. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf.

National Institute of Standards and Technology Special Publication 800-82 (Final Public Draft), *Guide to Industrial Control Systems (ICS) Security*, September 2008. Overview of industrial control systems (ICS), threats and vulnerabilities, risk factors, incident scenarios, security program development. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf.

National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006. Governance, awareness and training, capital planning, interconnecting systems, performance measures, security planning, contingency planning. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

National Institute of Standards and Technology Special Publication 800-122 (Draft), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, January 2009. Identifying, PII, impact levels, confidentiality safeguards, incident response. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

National Institute of Standards and Technology Special Publication 800-39(Final Public Draft), *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View*, December 2010. http://csrc.nist.gov/publications/drafts/800-39/draft-SP800-39-FPD.pdf.

Other Guidance Documents

Gary McGraw, *Software Security: Building Security In,* 2006, Addison-Wesley.

National Institute of Standards and Technology IR 7628, Guidelines for Smart Grid Cyber Security, August 2010. Four PDFs available at http://csrc.nist.gov/publications/PubsNISTIRs.html:

- *Introduction to NISTIR 7628*, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf.
- Vol. 1, *Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.
- Vol. 2, *Privacy and the Smart Grid*, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.
- Vol. 3, *Supportive Analyses and References*, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.

North American Electric Reliability Corporation Critical Infrastructure Protection Standards CIP-002 through CIP-009, 2009–10. Available at http://www.nerc.com/page.php?cid=2|20:

- CIP-002-3, Critical Cyber Asset Identification
- CIP-003-3, Security Management Controls
- CIP-004-3, Personnel and Training
- CIP-005-3, Electronic Security Perimeter(s)
- CIP-006-3, Physical Security of Critical Cyber Assets
- CIP-007-3, Systems Security Management
- CIP-008-3, Incident Reporting and Response Handling
- CIP-009-3, Recovery Plans f or Critical Cyber Assets

The CIP standards are also included in the collected *Reliability Standards for the Bulk Electric Systems of North America,* June 2010, http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf.

North American Electric Reliability Corporation Glossary of Terms Used in Reliability Standards, February 2008, http://www.nerc.com/files/Glossary_12Feb08.pdf.

Appendix B: Glossary

Adequate security	A set of minimum security requirements that the system is expected to meet.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources.
Authorization	Verifying a user's permissions (after the user had been authenticated) for accessing certain resources or functionality.
Availability	Ensuring timely and reliable access to and use of resources.
Attestation	The validation of all aspects of a component that relate to its safe, secure, and correct operation.
Boundary protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Contingency	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element.
Critical assets	Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.
Cyber asset	Programmable electronic devices and communication networks including hardware, software, and data.
Cyber security incident	Any malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the electronic security perimeter or physical security perimeter of a critical cyber asset. • Disrupts, or was an attempt to disrupt, the operation of a critical cyber asset.
Electronic security perimeter	The logical border surrounding a network to which critical cyber assets are connected and access is controlled.
Identity-based access control	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.
Impact	Damage to an organization's mission and goals due to the loss of confidentiality, integrity, or availability of system information or operations.
Impact level	The assessed degree (high, medium, low) of potential damage to an organization's mission and goals.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information security policy	An aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Note: information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.)
Integrity	Guarding against improper information modification or destruction; includes ensuring the nonrepudiation and authenticity of information.
Management controls	The security controls (i.e., safeguards or countermeasures) of an information system that focus on the management of risk and of information system security.
Network access	Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., LAN, WAN, Internet).
Nonrepudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message.
Operational controls	The security controls (i.e., safeguards or countermeasures) of an information system that are primarily implemented and executed by people (as opposed to systems).
Physical security perimeter	The physical, completely enclosed (“six-wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled.
Programmable logic controller (PLC)	A digital computer used for the automation of electromechanical processes. An example of a real-time system, since output results must be produced in response to input conditions within a bounded time, otherwise unintended operations will result.
Potential impact	The loss of confidentiality, integrity, or availability that might be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Security risks related to information security arise from the loss of confidentiality, integrity, or availability of information or information systems with potential adverse impacts on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.
Risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk category	People and policy risks, process risks, and technical risks.
Risk level (severity)	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization's mission and goals if it does occur.
Risk management	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation, resulting from the operation of an information system; includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Role-based access control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Security category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the nation.
Security control	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security policy	A set of high-level criteria for people, process, and technological guidance that relates to security of an organization, its systems, and its data.

Security requirements	Requirements levied on an information system that are derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Sensitive information	Information of which the loss, misuse, unauthorized access, or modification could adversely affect the organization, its employees, or its customers.
System security plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Technical controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. An alternate definition of threat is an actor / adversary who may carry out an attack against the organization.
Vulnerability	A specific weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability assessment	Formal description and evaluation of the vulnerabilities in an information system.

Appendix C: Acronyms

CIP	Critical Infrastructure Protection
DOD	Department of Defense
DOE	Department of Energy
DHS	Department of Homeland Security
EISA	Energy Independence and Security Act
FERC	Federal Energy Regulatory Commission
ISO	International Standards Organization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards
RMF	Risk Management Framework

Appendix D: Security Requirements for Federal Data Systems

The following summaries of minimum security requirements are from NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. IT systems at cooperatives NEED NOT meet these requirements. However, these requirements represent best practice in IT system-level security. They are presented here as a guide to building better systems.

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information-security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse. Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Appendix E: Procedures

Elements of a System Definition

An early step in creating security plans and establishing risk management programs is to strictly define the system in question by outlining the:

- Unique identifier for that installation.
- Primary function or purpose of that installation.
- Architecture diagrams (physical, logical, and security) and data flow diagrams.
- Installation inventory.
- Details for interfaces and protocols.
- Data types processed and the sensitivity of each.
- Version or SKU numbers for all physical and logical components, along with the criticality of each component.
- Vendors and contact information.
- Installation location and local cooperative contact information.
- Assignment of local security responsibilities.
- Any special interoperability or security concerns (e.g., modems, Web interfaces, remote administrative access).
- Emergency contact information and procedures for personnel involved in incident response, disaster recovery, and continuity of operations activities.

For each existing and new system, it is important to document the associated major management, technical, operational, and physical security controls.

Identifying and Protecting Private Data

To ensure that you have comprehensively addressed the handling of data privacy, build a checklist and apply it to each type of data. The answers will guide decisions in architecture, access controls, procedures, assignment of criticality labels, and mitigation strategies.

- Do I really need this information about an individual or group of individuals? Do I know how I will use it?
- Do the people whose information I hold know that I have it, and are they likely to understand how it will be used?
- Am I satisfied the information is being held securely, whether it's on paper or on computer? Is my Web site secure?
- Am I sure the personal information is accurate and up to date?
- Must or should I delete/destroy personal information as soon as I no longer need it?
- Is access to personal information limited only to those with a strict need to know?
- If I want to put staff details on our Web site, have I consulted with them about this?
- If I use CCTV or other personal surveillance, is it covered by any law I must follow? If so, am I displaying notices telling people why I have such surveillance? Are the cameras or other devices in the right place, or do they intrude on anyone's privacy?
- If I want to monitor staff, for example, by checking their use of e-mail, have I told them about this and explained why? Is the policy consistent with all laws, posted warnings, etc.?
- Have I trained my staff in their duties and responsibilities under applicable privacy laws, and are they putting them into practice?
- If I am asked to pass on personal information to any other group or agency, am I and my staff clear when the law allows me to do so?
- Would I know what to do if one of my employees or individual customers asked for a copy of information I hold about them?
- Do I have a policy for dealing with data protection issues?
- Do I need to notify any agency or group about the monitoring I am performing? If I have already notified, does my notification need amending or removal? (This also pertains to any monitoring or recording of telephone and/or radio communications.)
- Whom do I notify if there is, or if I suspect there is, a security breach associated with any such data?

Additional Guidance

- NIST SP800-122, *Guide to Protecting the Confidentiality of PII*[33]

Steps in Vulnerability Assessments

We conduct assessments to attain several objectives. Perhaps the most important is to identify all critical vulnerabilities in physical and cyber components, as well as in their interdependencies. However, the process also gives us the opportunity to identify and rank key assets, to develop the business case for cyber security investment, and to enhance the awareness of all cyber security stakeholders.

At a high level, a vulnerability assessment can be divided into preassessment, assessment, and postassessment phases, which comprise the following activities:

- Preassessment:
  - Define scope of assessment
  - Establish information protection procedures
  - Identify and rank critical assets
- Assessment:
  - Analyze network architecture
  - Assess threat environment
  - Conduct penetration testing
  - Assess physical security
  - Conduct physical asset analysis
  - Assess operations security
  - Examine policies and procedures
  - Conduct impact analysis
  - Assess infrastructure dependencies
  - Conduct risk characterization
- Postassessment:
  - Prioritize recommendations
  - Develop action plan
  - Capture lessons learned and best practices
  - Conduct training

[33] NIST SP800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

Additional Guidance

- NIST SP800-30, *Risk Management Guide for IT Systems.*
- DOE Vulnerability Assessment Methodology—Electric Power Infrastructure.[34]
- ISACA IS Auditing Procedure, Security Assessment—Penetration Testing and Vulnerability Analysis.[35]

Incident Response Planning Items

Effective response planning addresses a variety of personnel, process, and technology decisions. Planning activities include the following:

- Creating an incident response policy and plan.
- Developing procedures for performing incident handling and reporting, based on the incident response policy.
- Setting guidelines for communicating with outside parties regarding incidents.
- Selecting a team structure and staffing model.
- Establishing relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies).
- Determining what services the incident response team should provide.
- Staffing and training the incident response team.

Ongoing vigilance is key to preparedness. Recurring activities that help maintain incident response capability include:

- Establishing, documenting, maintaining, and exercising on-hours and off-hours contact and notification mechanisms for individuals and groups within the organization (e.g., chief information officer [CIO], head of information security, IT support, business continuity planning) and outside the organization (e.g., US-CERT, incident response organizations, counterparts at other organizations).
- Documenting guidelines for the prioritization of incident response actions based on changing business impacts.
- Assigning and training team leads to gather information from the incident handlers and other parties, and distribute relevant information to the parties that need it.
- Regularly practicing the handling of large-scale incidents through exercises and simulations. Such incidents happen rarely, so incident response teams often lack experience in handling them effectively.

[34] DOE Vulnerability Assessment Methodology—Electric Power Infrastructure (http://www.esisac.com/publicdocs/assessment_methods/VA.pdf).

[35] ISACA IS Auditing Procedure, Security Assessment—Penetration Testing and Vulnerability Analysis.

Disaster Response Planning Items

Interim measures that are likely applicable across a broad range of disruptions include:

- Relocation of information systems and operations to an alternate site.
- Recovery of information system functions using alternate equipment.
- Performance of information system functions using manual methods.

Planning generally follows a seven-step process:

2. **Develop the recovery planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective recovery plan.
3. **Conduct business impact analysis (BIA)**. The BIA helps identify and prioritize information systems and components critical to supporting the organization's business functions.
4. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce recovery life-cycle costs.
5. **Create recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
6. **Develop an information system recovery plan.** The recovery plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
7. **Ensure plan testing, training, and exercises.** Testing validates recovery capabilities, training prepares recovery personnel for plan activation, and exercising the plan identifies planning gaps. Combined, the activities improve plan effectiveness and overall organization preparedness.
8. **Ensure plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.