Nuclear Sector Cybersecurity Framework Implementation Guidance

for U.S. Nuclear Power Reactors

2015

Homeland Security

Foreword

The National Institute of Standards and Technology (NIST) released the 2014 *Framework for Improving Critical Infrastructure Cybersecurity* (Framework) as a voluntary, risk-based set of standards and best practices to help organizations of all sizes manage cybersecurity risks in any sector. The Department of Homeland Security (DHS) recognizes that many sectors have a distinct set of existing tools and standards that can help implement the Framework's risk-based approach. With that in mind, we worked with our private sector partners and the Office of Cybersecurity and Communications to develop this sector-specific Cybersecurity Framework Implementation Guidance (hereafter Implementation Guidance) to provide organization and structure to today's multiple approaches to cybersecurity.

This Implementation Guidance aims to simplify the process for all organizations in the Nuclear Sector—regardless of their size, cybersecurity risk, or current level of cybersecurity sophistication—to apply the principles and best practices of risk management. Ultimately, the Framework and this Implementation Guidance are focused on helping individual organizations reduce and better manage their cybersecurity risks, contributing to a more secure and resilient sector overall.

The Department of Homeland Security appreciates the dedication and technical expertise of all members of the Nuclear Sector Coordinating Council who participated in the development of this Implementation Guidance, as well as all the inputs provided by public and private stakeholders.

Nuclear Sector organizations can use the Implementation Guidance to determine how best to implement the Framework, which provides a repeatable process to identify and prioritize cybersecurity improvements and choose investments that maximize the impact of each dollar spent. As you use the Implementation Guidance, I ask for your continued feedback to update and improve the document and make it a robust and valuable guide for your organization as well as sector partners and peers.

I encourage your use of and reference to the NIST Framework and this Implementation Guidance as we work together to improve the security and resilience of our Nation's critical infrastructure from cyber and other attacks.

Caitlin Durkovich
Assistant Secretary
Office of Infrastructure Protection
National Protection and Programs Directorate
Department of Homeland Security

Table of Contents

List of Figures

List of Tables

Cautionary Note

This publication is not intended for regulatory use. It is not intended to replace or subsume other cyber security-related activities, programs, processes, or approaches that nuclear sector organizations have implemented or intend to implement, including any cyber security activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this publication uses the words "adopt," "use," and "implement" interchangeably. These words are not intended to imply compliance or mandatory requirements.

Acknowledgements

The Department of Homeland Security (DHS) acknowledges the dedication and technical expertise of all the organizations and individuals who participated in the development of the *Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors*. This document is based on inputs from members of the framework guidance development workgroup under the Nuclear Sector Coordinating Council. DHS also acknowledges inputs provided by members of the government partners working group, representing different public sector organizations, as well as comments provided by other public and private stakeholders during the public comment period.

Terms in this Document

A note on the use of terms within this document:

- The terms "reactor" and "plant" are used interchangeably in this document to refer to nuclear power reactor facilities.
- The term "cyber security" rather than "cybersecurity" is used primarily in this document to reflect the norm among nuclear asset owners and operators.

1. Executive Summary and Introduction

Background

The National Institute of Standards and Technology (NIST) released the voluntary *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2014; hereafter called the "Framework") in February 2014 to provide a common language organizations can use to assess and manage cyber security risk. Developed in response to Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" of February 2013, the Framework recommends risk management processes that enable organizations to inform and prioritize decisions regarding cyber security based on business needs without additional regulatory requirements. It enables organizations—regardless of sector, size, degree of cyber security risk, or cyber security sophistication—to apply the principles and effective practices of risk management to improve the security and resilience of critical infrastructure. To encourage and assist with Framework use, the EO also established the Critical Infrastructure Cyber Community (C^3) Voluntary Program, which serves as a central repository for government and private sector tools and resources to support the use of the Framework by sector owners and operators and enhance their cyber risk management practices.

The Framework, based on a collection of cyber security standards and industry best practices:

- Provides guidance on risk management principles and best practices;
- Provides common language to address and manage cyber security risk;
- Outlines a structure for organizations to understand and apply cyber security risk management; and
- Identifies effective standards, guidelines, and practices to manage cyber security risk in a cost-effective way based on business needs.

The Framework is designed to complement, and not replace or limit, an organization's risk management process and cyber security program. Each sector and individual organization can use the Framework in a tailored manner to address its cyber security objectives.

Purpose of the Implementation Guidance

Nuclear reactors in the United States have a strong track record of working together to develop and implement cyber security standards, tools, and processes that ensure safety, security, and reliability. The U.S. Department of Homeland Security (DHS), as the Nuclear Reactors, Materials, and Waste Sector-Specific Agency, worked with the Nuclear Sector Coordinating Council to develop this Implementation Guidance specifically for nuclear power reactor owners and operators. It is informed by the nuclear reactor risk environment and existing physical and cyber security programs as well as other risk management tools used within the sector.

This Implementation Guidance is designed to assist nuclear power reactor organizations to:

- Characterize their current and target cyber security posture.
- Identify gaps in their existing cyber security risk management programs, using the Framework as a guide, and identify areas where current practices may exceed the Framework.
- Recognize that existing sector tools, standards, and guidelines may support Framework implementation.
- Effectively demonstrate and communicate their risk management approach and use of the Framework to both internal and external stakeholders.

This document describes how the practices and programs at U.S. nuclear power reactors implement the Framework. The Framework implementation at nuclear power reactors is, at present, repeatable and will be adaptive once in-progress program enhancements are complete.

Organization of this Document

Section 2 provides a history and high-level overview of cyber security programs at U.S. nuclear power reactors. Section 3 provides key Framework terminology and concepts for its application. Section 4 identifies resources that inform Framework implementation. Section 5 outlines Framework implementation for U.S. nuclear power reactors based on existing requirements and implementation programs. Section 6 describes how the Framework can support sector-level goals and guidelines. Section 7 provides conclusions. Section 8 provides a detailed list of references. Finally, Appendix A maps existing cyber security and risk management approaches to the Framework's Core and Implementation Tiers, and Appendix B provides a summary table of the inputs, activities, and outputs for each step in the Framework implementation process. Appendix C includes a table of terms found within this document. Aside from the term "organization," the glossary is excerpted verbatim from the Framework.

2. History of Nuclear Power Reactor Cyber Security

The nuclear energy industry is one of the Nation's safest industries. It is protected by multiple back-up safety systems, robust physical defenses, and plant security forces with rigorous training. Since the September 11 terrorist attacks, the industry has continued to improve its safety systems to prepare for emerging threats, such as the impact from a wide-bodied commercial airliner and cyberattacks on critical operational systems. Each U.S. nuclear power plant is equipped with extensive security measures to protect the facility from intruders and to protect the public from the possibility of exposure to radioactive releases caused by acts of sabotage. The U.S. Nuclear Regulatory Commission (NRC) calls nuclear power plants "among the best-protected private sector facilities in the nation."

The Nuclear Sector has a long history of addressing cyber security issues. In 1997, through the Nuclear Energy Institute (NEI), the industry began looking at potential issues associated with the increasing use of digital technologies at power reactors. At this time there was a concern regarding the potential impacts associated with the change in millennia—referred to at that time as the "Y2K" issue. Following the terrorist attacks of September 11, 2001, the industry turned its focus to potential cyber security-related issues. In January 2002, NEI established a Cyber Security Task Force (CSTF), initially composed of 23 members, to provide an industry-wide forum for identifying, discussing, and resolving cyber security issues. In March 2002, the NRC issued Interim Compensatory Measures (ICM) Orders that directed licensees to consider and address cyber safety and security vulnerabilities.

During 2003 and 2004, the industry was engaged in the development of guidance documents intended to support the uniform implementation of cyber security programs at power reactors. In July 2003, cyber security assessment pilots were completed at four U.S. nuclear power reactors. These pilots were designed to inform development of NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants." The project team consisted of representatives from the Pacific Northwest National Laboratory (PNNL), the NRC, and the CSTF. NUREG/CR-6847 was released in November 2004. In November 2005, NEI released NEI 04-04, "Cyber Security Program for Power Reactors," Revision 1. NEI 04-04 provides guidance on establishing and maintaining a cyber security program, and incorporates assessment methodology described in NUREG/CR-6847. The NEI 04-04 program provides for the cyber security protection of all systems in the plant including those necessary for reliable electrical generation. The guidance provides a risk-informed approach, where consequences to plant functions are considered, and provides guidance on establishing a site cyber security defensive strategy incorporating multiple defensive layers with increasing levels of security protection. NEI 04-04 also provides guidance on incorporating cyber security considerations into the procurement process. The NEI 04-04 program includes the following steps:

1. Define current cyber security program.
2. Identify Critical Digital Assets (CDAs).
3. Validate configuration.
4. Assess susceptibility.
5. Assess consequences.
6. Determine risk.
7. Refine defensive strategy.
8. Continue program management.

In December 2005, the NRC informed NEI by letter that Nuclear Energy Institute (NEI) 04-04, "Cyber Security Program for Power Reactors," Revision 1, dated November 18, 2005, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. In 2006, the North American Electric Reliability Corporation (NERC) acknowledged that the NEI 04-04 program provides cyber security protection equivalent to the NERC Critical Infrastructure Protection (CIP) Reliability Standards.

The nuclear industry established a Nuclear Strategic Issues Advisory Committee (NSIAC) that has the ability to establish initiatives binding to all nuclear power plants. The NSIAC is comprised of the Chief Nuclear Officers of each power plant site or fleet. Approved NSIAC initiatives are implemented at all U.S. nuclear power plants. In April 2006, the NSIAC established an initiative requiring nuclear power plants to implement NEI 04-04 within two years. All U.S. plants implemented the initiative by May 2008.

Power plants are required by the NRC to design, implement, and evaluate their physical and cyber security programs to defend against a Design Basis Threat (DBT). In response to the increasing threat of cyber-related attacks, the NRC amended its design basis threat requirements in 2007 to include a cyberattack as an attribute of the adversary. The NRC describes a cyberattack as:

> *“The capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls.”*

In March 2009, the NRC issued revised security requirements that included comprehensive programmatic cyber security requirements, principally codified in Title 10 of the Code of Federal Regulations (CFR), Section 10 CFR 73.54, “Protection of Digital Computer and Communication Systems and Networks” (Rule). The Rule requires power plants to submit a cyber security plan and implementation schedule for NRC review and approval. To support uniform implementation, the industry developed a template for the cyber security plan and the implementation schedule. In May 2010 the NRC endorsed NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” Revision 6. NEI 08-09 provides a template for cyber security plans and a catalog of technical, operational, and management cyber security controls tailored from the NIST Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems,” Revision 2. The template for the implementation schedule provides eight milestones—seven interim milestones and an eighth milestone for full implementation. The first seven milestones are designed to address the most prominent threats to the plant’s most important systems.

These milestones include the establishment of a cyber security assessment team, hardware-based isolation of key networks and assets, tightening controls over portable media and equipment, enhancing existing insider threat mitigation, instituting protective measures for digital equipment that could impact key safety systems, and establishing ongoing monitoring and assessment activities for implemented cyber security measures. By December 31, 2012, each plant completed the initial seven milestones.

Post-2012 activities (the eighth milestone) include the completion of policy and procedural revisions that enhance existing capabilities, the completion of any remaining design-related modifications necessary to implement the cyber security plan, and institution of protective measures for lower consequence assets.

In January 2013, the NRC began inspecting power plant cyber security program implementation of the initial seven milestones, and completed inspections at each power plant at the end of 2015.

3. Framework Implementation Overview

This section opens with an overview of key Framework terminology and concepts, followed by a subsection describing the purpose of this Implementation Guidance. The final subsection highlights some of the benefits of using the Framework. Please refer to the glossaries in the Framework (NIST 2014) for full definitions of additional terms used throughout this document.

Framework Guidance Terminology

The three main components of the Framework are the Core, the Framework Implementation Tiers (Tiers), and the Profile. These terms are frequently used in this Implementation Guidance and defined below.

The ***Core*** is a set of "cyber security activities, desired outcomes, and applicable Informative References that are common across critical infrastructure sectors." The Core comprises four elements: Functions, Categories, Subcategories, and Informative References. **Functions** provide a high-level, strategic view of the lifecycle of an organization's management of cyber security. There are five Functions: Identify, Protect, Detect, Respond, and Recover. Each Function is divided into Categories, Subcategories, and Informative References. The **Categories** are cyber security outcomes that are closely tied to programmatic needs and particular activities. The **Subcategories** are specific outcomes of technical and/or management activities that support achievement of each Category. **Informative References** are specific cross-sector standards, guidelines, and effective practices that illustrate a method to achieve the outcomes associated with each Subcategory.

Tiers describe an organization's approach to "cyber security risk and the processes in place to manage that risk," ranging from Tier 1 (Partial) to Tier 4 (Adaptive). Each Tier demonstrates an increasing degree of rigor and sophistication of cyber security risk management and integration with overall organizational needs. Progression to higher Tiers is encouraged when such a change would cost-effectively reduce cyber security risk. Tiers are associated with the overall robustness of an organization's risk management process and are *not* tied to Functions, Categories, or Subcategories. An organization may align its application of the Tiers with its desired scope for using the Framework. For example, if an organization chooses to use the Framework only for a specific business unit or process, the Tiers could be used to describe the overall robustness of risk management processes at that business unit or process level. (See the definition below for how "organization" is used in this document).

Profiles align the Framework core elements with business requirements, risk tolerance, and organizational resources. The Profile can be used to identify opportunities for improving cyber security posture by comparing a Current Profile to a Target Profile. Profiles provide a roadmap to reduce cyber security risk consistent with business practices.

This document also frequently refers to the term ***organization***, which describes an operational entity of any size that uses the same cyber security risk management program within its different components and may individually use the Framework. This may describe one corporation or one business unit or process within a multi-unit corporation. For the purposes of this Implementation Guidance, organization is synonymous with nuclear power plant.

Framework Guidance Purpose

Given the broad nature of the Framework components described above, organizations cannot simply be "compliant" with the Framework or "adopt" it. Indeed, organizations have unique cyber security risks, including different threats, vulnerabilities, and tolerances, all of which benefit from investing in cyber security risk management. Individual organizations must apply Framework principles, best practices, standards, and guidelines to their specific context and needs.

The nuclear sector embraces the flexibility offered by the Framework, but recognizes organizations' potential need for more guidance on how to apply the Framework to their suit their particular needs. With this in mind, the Sector Coordinating Council (SCC) and DHS Sector Outreach and Programs Division (SOPD) worked with sector stakeholders and the DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program to develop this Implementation Guidance which was designed to enhance understanding of:

- Framework terminology, concepts, and benefits;
- Existing sector cyber security tools and resources that support Framework use;
- A standard approach for using the Framework; and
- Suggestions for how to link organizational cyber risk management activities to the Nuclear Sector.

It is important to note that the Framework includes considerations to address **privacy and civil liberties issues** during implementation. In the Nuclear Sector, these issues are not directly applicable to safety or reliability. Although this Implementation Guidance does not directly address privacy and civil liberties issues, organizations are encouraged to review and consider using the Framework's privacy and civil liberties guidance (NIST 2014, p. 15) in alignment with other privacy guidelines and State and Federal laws.

Framework Implementation Benefits

The Framework is designed to be flexible enough to be used both by organizations with mature cyber security and risk management programs and by those with less-developed programs. Implementation of the Framework does not imply that existing cyber security and risk management approaches are ineffective or need to be replaced. Rather, implementation means that the organization wishes to take advantage of the benefits that the Framework offers.

In general, implementing the Framework provides a mechanism for organizations to:

- Assess and specifically **describe its current and targeted cyber security posture**.
- **Identify gaps** in its current programs, processes, and workforce.
- Identify and **prioritize opportunities for improvement** using a continuous and repeatable process.
- **Assess progress** toward reaching its target cyber security posture.
- **Demonstrate the organization's alignment** with the Framework's nationally recognized best practices.
- Highlight any current practices that might **surpass the Framework's recommended practices**.
- **Communicate its cyber security posture in a common, recognized language** to internal and external stakeholders—including customers, regulators, investors, and policy makers.

Implementing the Framework can help organizations to strengthen their existing cyber security risk management approach and more easily communicate their use of particular cyber security practices to internal and external stakeholders. Organizations with less-developed cyber security risk management programs can use the Framework to define and establish a program that successfully addresses cyber security risk and communications commensurate with the organization's business and critical infrastructure security objectives.

U.S. nuclear power plants have mature risk management programs. This document describes how the programs at nuclear power plants implement the Framework. The implementation detailed in Section 5 describes Framework implementation, and Appendix A maps existing cyber security and risk management approaches (e.g., standards, tools, methods, and guidelines) to the Framework's Core and Implementation Tiers. Early adoption of the Framework's principles may better position nuclear power plants to receive additional potential benefits in the future:

- **More attractive cyber security insurance coverage** — As cyber risks grow, insurance agencies are developing new and refined approaches to evaluate clients' premiums based on their use of sound cyber security practices.

Insurance coverage may increasingly encourage or require the use of nationally recognized cyber risk management processes. Framework implementation provides an additional, widely accepted means for an organization to measure its cybersecurity posture and demonstrate continuous improvement.

- **Prioritized funding or technical assistance** — The Federal Government provides several hands-on tools that will help an organization assess their current-state of cyber security practices and identify areas to grow their cyber security resilience. Commercial Facilities Sector organizations are encouraged to visit the US-CERT Critical Infrastructure Community (C^3) Voluntary Program Webpage for additional information related to both facilitated and self-service risk assessment resources. The Federal government uses this assessment to help organizations prioritize next steps, depending on their level of cyber security maturity. For example, the government offers preparedness support, assessments, training of employees, and advice on best practices. Under this incentive, the primary criteria for assistance would be criticality, security, and resilience gaps. Owners and operators in need of incident response support will never be denied assistance based on cyber security maturity and/or level of prior engagement with the use of the Framework.

- **Demonstration of commitment to cyber security —** The Framework does *not* protect any organization from liability in the event of a cyber incident. However, implementation of the Framework provides an organization with a mechanism to demonstrate its proven track record of implementing and continuously evaluating cyber risk management practices appropriate for its individual risks.

- **Government recognition** — For interested organizations, DHS seeks to recognize those organizations and sectors that use the Framework and participate in the C^3 Voluntary Program, regardless of size and maturity level.

- **Workforce development –** Organizations that use the Framework will have a better understanding of the technical capabilities their organization requires and, therefore, the skills required of their cyber workforce. A more accurate understanding of these needs can guide activities such as recruiting, workforce design, and training of existing personnel.

4. Sector Framework Guidance Resources

This section presents an overview of the NRC's risk management program and cyber security requirements and guidance.

Nuclear Sector Risk Management

The NRC was created as an independent agency by Congress in 1974 to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment. The NRC uses licensing, inspection, and enforcement of its requirements to regulate commercial nuclear power reactors and other uses of nuclear material, such as in medicine.

NRC's regulatory mission covers three main areas:

- **Reactors**—Commercial reactors for generating electric power and research and test reactors used for research, testing, and training;
- **Materials**—Uses of nuclear materials in medical, industrial, and academic settings and facilities that produce nuclear fuel; and
- **Waste**—Transportation, storage, and disposal of nuclear materials and waste, and decommissioning of nuclear facilities from service.

The NRC imposes security requirements in a risk-informed manner for their licensees with the objective of ensuring public health and safety, and common defense and security.

Overview of NRC Power Reactor Requirements and Guidance

The NRC has established requirements for cyber security programs for nuclear power reactors. The cyber security requirements are codified primarily in 10 CFR 73.54. These cyber security requirements are an integrated component of the NRC's overall physical protection program requirements that include physical security, cyber security, and personnel security. The requirements establish a comprehensive cyber security program for the protection of digital computer and communications systems and equipment against cyberattacks that would adversely impact operational safety, security, or emergency preparedness. Also protected are digital assets associated with electric power generation equipment. The program includes key cyber security program elements, including the identification of in-scope assets; implementation of security controls; defense-in-depth measures for detection, response, and recovery; managing cyber risks; training; integration of cyber security and physical security programs; development and maintenance of written policies and implementing procedures; reviewing the cyber security program; and records retention.

To support implementation of the cyber security requirements in 10 CFR 73.54, the NRC has issued and endorsed a number of approaches. Although a more complete list can be found in Section 8, notable guidance documents are summarized in Table 1.

TABLE 1.—Key U.S. Nuclear Power Reactor Cyber Security Guidance Documents.

Name	Summary	Additional Information
NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors"	NEI 08-09 provides a template for the cyber security plan. The plan includes a defensive strategy that consists of a defensive architecture and set of security controls that are based on the NIST SP 800-82, Final Public Draft, Dated September 29, 2008, "Guide to Industrial Control System Security," and NIST SP 800-53, Revision 2, "Recommended Security Controls for Federal Information Systems" standards.	Cyber Security Plan for Nuclear Power Reactors
Template for the Cyber Security Plan Implementation Schedule	Provides a template used by each operating power plant to establish the schedule for the implementation of their cyber security plans. Each operating plant has completed the first seven milestones provided in the template.	Cyber Security Plan Implementation Schedule
RG 5.71, "Cyber Security Programs for Nuclear Facilities"	RG 5.71 is similar to NEI 08-09 in that it contains a template for the plan and a catalog of security controls. RG 5.71 includes additional information not found in NEI 08-09. Certain new plants use RG 5.71, rather than NEI 08-09, as the basis for their Cyber Security Plans. Because of the similarities between RG 5.71 and NEI 08-09, this Framework mapping is applicable to new plants as well.	Cyber Security Programs for Nuclear Facilities

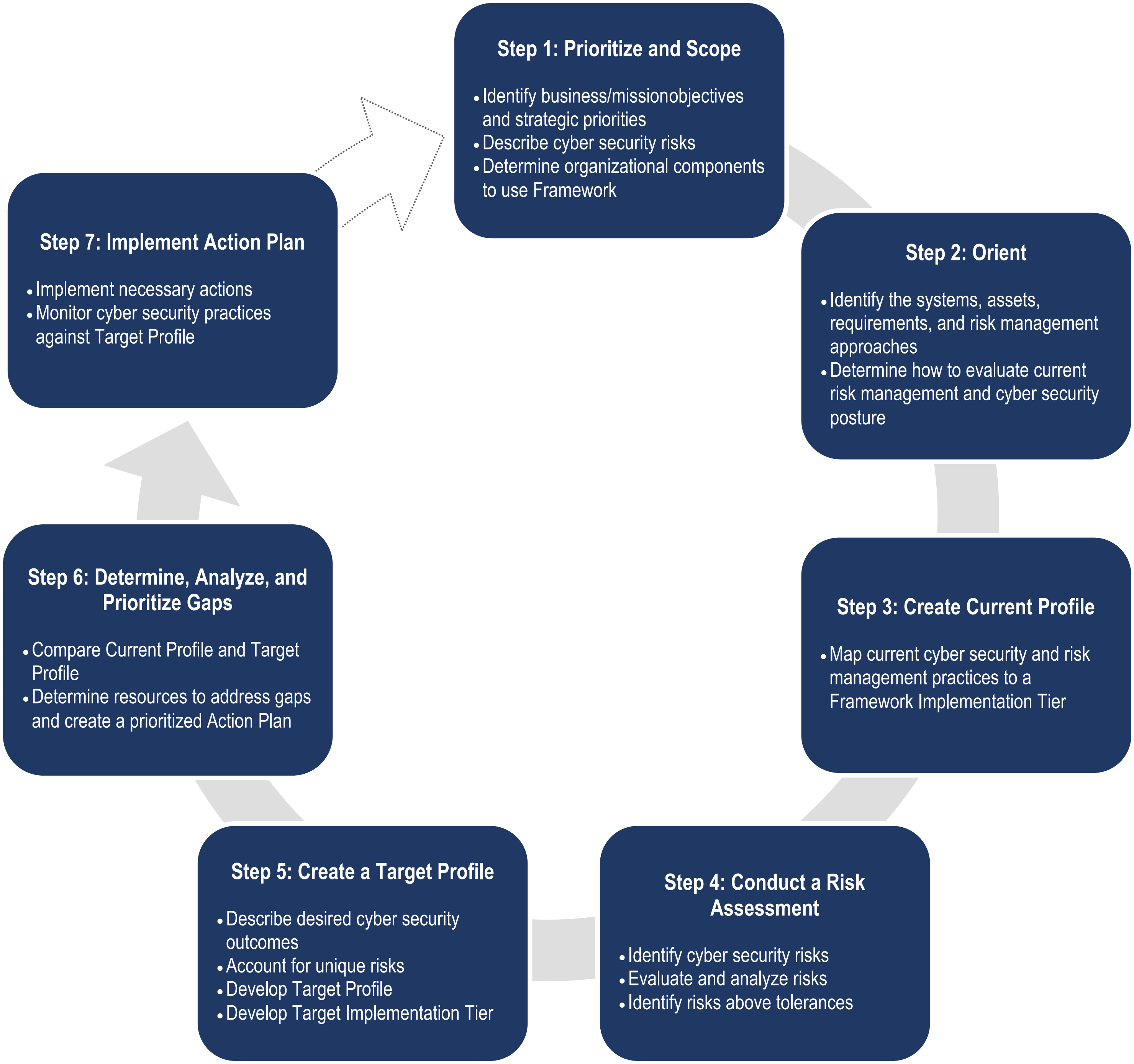
Mapping to the Framework

Section 5 details the Framework implementation using the existing practices as well as requirements and guidance applicable to nuclear power plants. A mapping of these elements to the Framework is provided in Appendix A. The mapping provides a translation between the organization's current practices and the Framework, supporting communication to external stakeholders.

5. Approach to Framework Implementation

This section describes how the seven-step process outlined in Section 3.2 in the Cybersecurity Framework was used to demonstrate how cyber security practices at U.S. nuclear power plants align to the Framework. Established practices common at plants as well as those required by regulatory requirements were used. Where possible, references to specific documents or requirements are provided.

FIGURE 1.—Framework Implementation Process.



Step 1: Prioritize and Scope

- Identify business/missionobjectives and strategic priorities
- Describe cyber security risks
- Determine organizational components to use Framework

Step 2: Orient

- Identify the systems, assets, requirements, and risk management approaches
- Determine how to evaluate current risk management and cyber security posture

Step 3: Create Current Profile

- Map current cyber security and risk management practices to a Framework Implementation Tier

Step 4: Conduct a Risk Assessment

- Identify cyber security risks
- Evaluate and analyze risks
- Identify risks above tolerances

Step 5: Create a Target Profile

- Describe desired cyber security outcomes
- Account for unique risks
- Develop Target Profile
- Develop Target Implementation Tier

Step 6: Determine, Analyze, and Prioritize Gaps

- Compare Current Profile and Target Profile
- Determine resources to address gaps and create a prioritized Action Plan

Step 7: Implement Action Plan

- Implement necessary actions
- Monitor cyber security practices against Target Profile

Each step is introduced by a table describing the step's inputs, activities, and outputs. Additional explanation is provided below each table as needed. A summary table of the inputs, activities, and outputs for each step is included in Appendix B.

An organization may repeat the steps as needed to continuously assess and improve its cyber security. For instance, organizations may find that more frequent repetition of Step 2: Orient improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also use this process to align their cyber security program with their desired Framework Implementation Tier.

U.S. nuclear power plants already have comprehensive risk management programs that establish the context for risk-based decisions by allowing them to assess risk, address identified risk, and monitor risk on an ongoing basis. The plants also use corrective action programs, assessments, and audits for continuous improvement. This section demonstrates how the activities described in these seven steps are already performed. Accordingly, this document describes how the plants implement the Framework by describing and aligning or "translating" elements of their current approach to the Framework Core and Implementation Tiers.

Step 1: Prioritize and Scope

Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cyber security capabilities	1. Framework usage scope

The Framework usage scope for nuclear power plants in the United States is well defined. To protect from those cyberattacks that would act to modify, destroy, or compromise the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data; or impact the operation of systems, networks, and associated equipment, nuclear plants implement cyber security programs for digital computer and communications systems and networks performing the following categories of functions:

1. Safety-related functions (including assets associated with electric power generation equipment out to the intertie with the offsite transmission system);
2. Security functions;
3. Emergency preparedness functions, including offsite communications; and
4. Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Step 2: Orient

Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and Informative References (e.g., cyber security and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cyber security and risk management standards, tools, methods, and guidelines 4. Evaluation approach

The NRC requires each nuclear power plant to implement a cyber security program covering the digital assets described in Step 1, "Prioritize and Scope," above. The NRC's cyber security requirements are codified primarily in 10 CFR 73.54. Each plant has submitted, and the NRC has approved, a cyber security plan (Plan) and implementation schedule (Schedule). The Plan describes how the cyber security requirements will be met, and the Schedule describes when the Plan will be implemented. The plants have used an industry-wide template for both the Plan and Schedule.

In accordance with the Schedule, each power plant identified the digital systems and equipment in scope for their cyber security programs by December 31, 2012. By the end of 2015, the NRC will complete inspecting each plant's identification of digital assets.

The in-scope cyber security and risk management standards, tools, methods, and guidelines include the physical, cyber, and personnel security requirements codified in 10 CFR 73.54, 10 CFR 73.55, and 10 CFR 73.56, respectively. Guidance most applicable to this Framework mapping include the industry's NEI 08-09, NEI 10-04, and NEI 13-10. The standards, tools, methods, and guidelines regarding information security are included within the requirements codified in 10 CFR 73.21 and 10 CFR 73.22 and their associated implementing guidance documents. A more detailed list of guidance and requirements can be found in Section 8.

Step 3: Create a Current Profile

Inputs	Activities	Outputs
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cyber security and risk management standards, tools, methods, and guidelines	1. Organization identifies its current cyber security and risk management state	1. Current Profile 2. Current Implementation Tier

U.S. nuclear power plants have advanced risk management practices that are fully integrated into both the design of the facility and its operations and oversight. With a fundamental focus on safety, risk-significant systems, structures, and components (SSCs) are identified, and the plant is physically designed to ensure that those SSCs are not adversely impacted by a range of hazards. This focus on safety is fed forward from the design into the operations and oversight of power plants.

Additionally, U.S. nuclear power plants have an approved Plan and Schedule, making their Current and Target Profiles and Implementation Tiers easily determined. The Current and Target Profiles and an assessment of the Implementation Tier are provided in Appendix A. The Profiles are informed by the uniform Plan and Schedule. Although the Current Profile recognizes that the Plans are partially implemented, the Target Profile was implemented for a subset of plant equipment by December 31, 2012. Based on the Current Profile and Implementation Tier assessment described in Appendix A, the current Implementation Tier is between Tier 3, "Repeatable," and Tier 4, "Adaptive." Upon full implementation of the Plan, the Implementation Tier will be Tier 4, "Adaptive."

Step 4: Conduct a Risk Assessment

Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy 3. Organization-defined risk assessment approach 4. In-scope regulatory requirements 5. In-scope cyber security and risk management standards, tools, methods, and guidelines	1. Perform risk assessment for in-scope portion of the organization	1. Risk assessment reports

The concepts of risks (from both natural and manmade hazards) are well understood and established for nuclear power plants. Each plant has identified sets of plant systems and equipment that are more or less risk significant. During the development of the Implementation Schedule, this inherent understanding of risk was used to prioritize implementation. The Schedule prioritized cyber security program implementation for the subset of plant equipment determined to be most important for protecting the health and safety of the public. The Schedule also prioritized the implementation of plant-wide mitigations for certain cyber threats, including network-based attacks and attacks that promulgate through the use of portable media and portable equipment. Because each plant has identified risk-significant systems and equipment and has a risk-informed implementation schedule, a separate risk assessment was not performed during the development of this document.

Step 5: Create a Target Profile

Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Organizational objectives 4. Risk management strategy 5. Risk assessment reports	1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives	1. Target Profile 2. Target Tier

As discussed in Step 3, "Create a Current Profile," the Target Profile is determined by the approved Plan and Schedule, and is documented in Appendix A. The Target Implementation Tier is Tier 4, "Adaptive."

Step 6: Determine, Analyze, and Prioritize Gaps

Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Target Profile 4. Target Tier 5. Organizational objectives 6. Impact to critical infrastructure 7. Gaps and potential Consequences 8. Organizational constraints 9. Risk management strategy 10. Risk assessment reports	1. Analyze gaps between current state and Target Profile in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) on actions 6. Prioritize actions (CBA and consequences) 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan

U.S. nuclear power plants are enhancing their cyber security programs using the Implementation Schedule. The Schedule prioritized early implementation of key cyber security controls for a subset of systems and equipment most important to protecting the health and safety of the public. These controls were in place by December 31, 2012. Moving toward full implementation of the program, plants are evaluating the less risk-significant assets and implementing appropriate cyber security controls. These activities will be completed by the plant-specific date specified in their Schedule and approved by the NRC.

Step 7: Implement Action Plan

Input	Activities	Outputs
1. Prioritized implementation plan	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks, metrics, and performance indicators 4. Report progress	1. Project tracking data 2. New security measures implemented

The Implementation Schedule driving cyber security program enhancements has been in place for many years. Plants have detailed project plans they are using to ensure they meet the commitments in the Schedule. These non-voluntary commitments are enforceable by the NRC. The details of these project plans were not reviewed during the development of this document. However, given the uniform nature of the industry-wide Cyber Security Plans and Implementation Schedules, there is sufficient knowledge of the implementation activities to form a reasonable basis for the conclusions in this document.

6. Informing Existing Sector Efforts

The Framework can be used to enhance the success of existing sector-specific programs and inform sector-level goals and guidelines. The approaches below can be used to increase knowledge and enhance cyber security practices; the Framework can make them more effective.

- **Critical Infrastructure Cyber Community (C3) Voluntary Program:** The C³ Voluntary Program is a public-private partnership that aligns business enterprises as well as Federal and State, local, tribal, and territorial (SLTT) governments to existing resources. It will assist them in using the Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. Currently, a number of DHS and government agencies provide programs and resources to critical infrastructure sectors and organizations that are looking to improve their cyber risk resilience. The C³ Voluntary Program is the coordination point within the Federal government to leverage and enhance existing capabilities and resources to promote Framework implementation. Although the Framework is based on existing guidelines and standards, organizations may still need assistance in understanding its purpose and how it may apply to them. The C³ Voluntary Program will provide assistance to organizations of all types interested in using the Framework.
- **Nuclear Sector-Specific Plan:** The *Nuclear Sector-Specific Plan* (SSP) is designed to guide the sector's efforts to improve security and resilience, and describes how the Nuclear Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21). The SSP reflects the overall strategic direction for the Nuclear Sector and represents the progress made in addressing the sector's evolving risk, operating, and policy environments. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), the SSP tailors the NIPP's strategic guidance to the unique operating conditions and risk landscape of the Nuclear Sector.

7. Conclusions

U.S. nuclear power plants operate in both the Nuclear Reactors, Materials, and Waste and the Energy Sectors. U.S. reactors are regulated for safety and security by the NRC. The NRC issues requirements and develops or endorses guidance describing methods acceptable for meeting the requirements. Section 4 provides an overview of NRC requirements and guidance.

U.S. nuclear power plants already have advanced risk management practices, which are fully integrated into the design, operations, and oversight of the facility. Nuclear reactors in the United States have a strong track record of working together to develop and implement cyber security standards, tools, and processes that ensure safety, security, and reliability.

U.S. nuclear power reactors may implement the *Framework for Improving Critical Infrastructure Cybersecurity* through their existing practices and programs. Framework implementation at nuclear power reactors is, at present, repeatable, and will be adaptive once in-progress program enhancements are complete.

8. References

Abbreviated Reference	Citation
10 CFR 73.1	NRC Regulations, *Physical Protection of Plants and Materials, Purpose and Scope*, 10 CFR §73.1, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html.
10 CFR 73.21	NRC Regulations, *Physical Protection of Plants and Materials, Protection of Safeguards Information: Performance Requirements*, 10 CFR §73.21, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0021.html.
10 CFR 73.22	NRC Regulations, *Physical Protection of Plants and Materials, Protection of Safeguards Information: Specific Requirements*, 10 CFR §73.22, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0022.html.
10 CFR 73.54	NRC Regulations, *Physical Protection of Plants and Materials, Protection of Digital Computer and Communication Systems and Networks*, 10 CFR §73.54, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html.
10 CFR 73.55	NRC Regulations, *Physical Protection of Plants and Materials, Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage*, 10 CFR §73.55, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0055.html.
10 CFR 73.56	NRC Regulations, *Physical Protection of Plants and Materials, Personnel access authorization requirements for nuclear power plants*, 10 CFR §73.56, http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0056.html.
10 CFR 73.77	NRC Regulations, *Physical Protection of Plants and Materials, Cyber Security Event Notifications,* 10 CFR §73.77, http://pbadupws.nrc.gov/docs/ML1426/ML14269A388.pdf.
Implementation Schedule Template	Nuclear Energy Institute, *Template for the Cyber Security Plan Implementation Schedule*, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML110600218.
NEI 08-09	Nuclear Energy Institute, *Cyber Security Plan for Nuclear Power Plants,* http://pbadupws.nrc.gov/docs/ML1011/ML101180437.pdf.
NEI 10-04	Nuclear Energy Institute, *Identifying Systems and Assets Subject to the Cyber Security Rule*, Revision 2, 2012, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML12180A081.
NEI 10-08	Nuclear Energy Institute. *Cyber Security Control Assessments*, Revision 2, 2014, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML14351A288. Note: this document is under active revision, updated versions may be available.
NEI 10-09	NRC Regulatory Guide, *Cyber Security Programs for Nuclear Facilities,* Revision 0, January 2010, http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.
NEI 13-10	Nuclear Energy Institute, *Cyber Security Control Assessments,* Revision 2, 2014, https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML14351A288. Note: This document is under active revision. Updated versions may be available.

Abbreviated Reference	Citation
NIST 2014	National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Security*, NIST, February 2014, http://www.nist.gov/cyberframework/index.cfm.
NIST SP 800-53	National Institute of Standards and Technology, Special Publication (SP) 800-53 (NIST SP 800-53), *Recommended Security Controls for Federal Information Systems*, Revision 2, http://csrc.nist.gov/publications/PubsSPs.html#SP 800. Note: At the time NEI 08-09 was developed, Revision 2 to NIST SP 800-53 was the currently approved standard.
NRC RG 5.71	NRC Regulatory Guide, *Cyber Security Programs for Nuclear Facilities*, Revision 0, January 2010, http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

Appendix A: Mapping to the Framework

As discussed in Section 5 of this Implementation Guidance, cyber security programs at nuclear power plants can be mapped to the Framework Core and Implementation Tiers to demonstrate their implementation of the Framework.

U.S. nuclear power reactors established comprehensive and integrated operational and security risk management programs long before cyber security concerns warranted separate risk management attention. Accordingly, and to more fully inform the Framework mapping, Table A1 provides an overview of how various programs at power reactors support implementation of the Framework. These other programs include, for example, maintenance, work management, configuration management, and corrective action programs that support safety and reliability. Power reactor physical protection programs existed before the NRC's new requirements for cyber security programs, and implement comprehensive physical security, personnel security, access controls, and information security practices. A stand-alone review of the Cyber Security Plan at U.S. nuclear power reactors would not provide an adequate representation of the comprehensive and integrated nature of established operational and security risk management programs. The cyber security programs do not necessarily establish or implement these other programs; however, the cyber security program may supplement or enhance them. Table A1 identifies these enhancements.

The overview is followed by a two-part mapping. These mappings provide detail for how plant practices meet the intent of the Framework. Table A2 maps the Framework Core and the nuclear reactor cyber security program practices. At the time of this writing, the Profile identified in Table A2 is currently achieved at all U.S. nuclear reactors for systems and equipment essential to safety and security. Progress toward the Profile is underway and will be achieved by 2017 based on each reactor's Implementation Schedule. The Profile column in Table A2 references applicable sections of the Plan and cyber security controls from NEI 08-09. The cyber security controls were tailored from the controls in NIST SP 800-53. The Plan sections and cyber security controls listed in Table A2 supplement and enhance existing programs described in Table A1. The cyber security controls listed in Table A2 are taken from Appendices A, D, and E from NEI 08-09. These controls have corollaries in Appendices A, B, and C of RG 5.71.

Table A3 maps practices at U.S. nuclear power plants to the Framework Implementation Tiers. The description of nuclear power plant implementation describes current practices in place at the time of the writing of this document and those future practices that will be in place once the enhancements to the cyber security program are fully implemented. The current practices are consistent with at least Implementation Tier 3, "Repeatable." The future practices that enhance those current practices are consistent with Implementation Tier 4, "Adaptive."

TABLE A1.—Overview of U.S. Nuclear Power Reactor Practices Mapped to the Framework Core.

Function	Category	U.S. Nuclear Power Reactor Implementation Notes
Identify (ID)	Asset Management (ID.AM)	Nuclear reactors maintain up-to-date inventories of the devices, systems software platforms, and applications within the plant. These inventories are updated as changes to the facility occur in accordance with standard configuration management, work management, and software quality assurance programs. These inventories include details on the safety and reliability importance of the assets. Safety, reliability, and security systems within a reactor do not interface with external systems such as the plant business network. Plants use a variety of communications tools that ensure effective communications with personnel and management. These tools include pre-job briefings, shift-turnover reports, daily briefings, and regular updates to management on facility activities. These practices ensure that events that could affect the plant are managed effectively. Roles and responsibilities, including those related to cyber security, are documented in site governing documents and are well understood.
Identify (ID)	Business Environment (ID.BE)	As significant contributors to the baseload generating capacity of the United States and significant consumers of electricity, nuclear power reactors are well aware of the role they play in ensuring the reliability of the electrical system. The plants focus on safety and reliability drive mission priorities, and risk and resilience management activities. The potential impacts of cyber threats to safety, security, and reliability are well established and integrated into risk management activities.
Identify (ID)	Governance (ID.GV)	Each U.S. reactor has a Cyber Security Plan that has been reviewed and approved by the NRC as meeting the NRC's cyber security requirements. The Plan includes a description of the roles, responsibilities, and authorities necessary to establish, implement, and maintain the cyber security program. The Plan describes how cyber security risk management is performed. The cyber security program is integrated into the overall nuclear power plant physical protection program and is subject to oversight by both the plants independent oversight organization and by the NRC.
Identify (ID)	Risk Assessment (ID.RA)	The Cyber Security Plan describes the risk assessment steps. The Plan includes measures for receiving and dispositioning threat and vulnerability notices, assessing and responding to risks that affect critical systems, assessing changes to facility systems to ensure cyber risk is managed, and periodically reviewing cyber risk management activities.

Function	Category	U.S. Nuclear Power Reactor Implementation Notes
Identify (ID)	Risk Management Strategy (ID.RM)	The Cyber Security Plan is implemented by site governing documents and implementing procedures that establish and govern the risk management process. Risk tolerance is driven by the performance objective of preventing, detecting, and responding to cyberattacks before those attacks could adversely impact safety and security.
Protect (PR)	Access Control (PR.AC)	Power reactors have robust access control programs. These programs are designed to ensure that individuals granted access to the plant are trustworthy, reliable, and do not constitute an unreasonable risk to the health and safety of the public. Access is granted to those individuals who have a need to access the facility in order to perform their job functions. The need for access is routinely reverified, and access is revoked when no longer needed. Assessing cyber security access controls to the plant's digital computer systems is included in the cyber security program.
Protect (PR)	Awareness and Training (PR.AT)	Training is a key component to nuclear reactor operations. All personnel, including contractors and visitors, receive training that includes both basic awareness and job-function-specific training. The training programs, based on the individual's roles and responsibilities, include a variety of cyber security training, such as basic awareness, job-function-specific, and tiered training for personnel implanting the cyber security program.
Protect (PR)	Data Security (PR.DS)	Plants have specific data security programs established to protect certain information from unauthorized disclosure. Specific requirements regarding the protection of safeguard information are codified in 10 CFR 73.21 and 10 CFR 73.22. Additionally, plants have programs in place to protect proprietary, non-safeguard, security-related information. Plants evaluate security and integrity controls applicable to the digital systems and equipment within their cyber security program. The cyber security program includes measures governing management of assets throughout the lifecycle.
Protect (PR)	Information Protection Processes and Procedures (PR.IP)	Cyber security practices are integrated into digital asset lifecycles including configuration management, work management, software quality assurance, cyber security threat and vulnerability management, and incident response and recovery programs. The cyber security program complements site contingency and emergency response procedures. Periodic testing of these programs ensures they remain effective.

Function	Category	U.S. Nuclear Power Reactor Implementation Notes
Protect (PR)	Maintenance (PR.MA)	Plants use an integration of corrective action, configuration management, and work management programs to ensure the maintenance and repair of assets are performed and logged in a timely, structured manner. Offsite access to critical systems and protected equipment relied on for safety, security, and reliability is prohibited—maintenance must be performed on site by personnel determined to be trustworthy and reliable, or by individuals escorted by personnel determined to be trustworthy and reliable, trained to perform the escort function, and generally knowledgeable of the maintenance activities to be performed.
Protect (PR)	Protective Technology (PR.PT)	Cyber security controls implement measures to protect digital systems and equipment against cyberattack. Plants have installed hardware-based network isolation devices to eliminate the potential for an external network-based attack. Comprehensive controls of portable media and equipment are implemented. Facility access controls are enhanced with computer system access controls. Audit logs are created, retained, and reviewed in accordance with the governing procedures.
Detect (DE)	Anomalies and Events (DE.AE)	Anomalous activity is detected by both cyber and non-cyber means. When anomalous system behavior is identified, documented procedures govern response, including a risk assessment and prioritization of response. Response may include an assessment of possible physical or cyber tampering. Intrusion detection systems are used.
Detect (DE)	Security Continuous Monitoring (DE.CM)	Physical access to the facility is continuously monitored in continuously manned central alarm stations. Cyber security controls are implemented to monitor systems and networks.
Detect (DE)	Detection Processes (DE.DP)	Detection process for physical security are well established and regularly tested. Cyber security detection capabilities are implemented, reviewed, and tested.
Respond (RS)	Response Planning (RS.RP)	Response to security events, including cyber security events, is governed by a facility contingency response plan that is an integrated component of the facility physical protection program.
Respond (RS)	Communications (RS.CO)	Communications in response to events is governed by site procedures and includes communications with facility operations and security, State and local officials as required, and the NRC as required. NRC Regulation 10 CFR 73.77 outlines requirements for conducting notifications and submitting follow-up reports to the NRC for cyber security events. Operating experience is shared voluntarily within the power reactor community and with external stakeholders, as appropriate.
Respond (RS)	Analysis (RS.AN)	Event response procedures govern the response to cyber and physical detection system notifications, performance of impact assessments, determination of the need for forensic analysis.

Function	Category	U.S. Nuclear Power Reactor Implementation Notes
Respond (RS)	Mitigation (RS.MI)	Event response procedures and the contingency response plan govern how events are contained. Newly identified vulnerabilities are addressed in accordance with the physical security plan or the cyber security plan, as appropriate.
Respond (RS)	Improvements (RS.IM)	Improvements based on lessons learned are handled through the facility corrective action program.
Recover (RC)	Recovery Planning (RC.RP)	Recovery plans are established for safety and security systems.
Recover (RC)	Improvements (RC.IM)	Improvements to recovery plans based on lessons learned are handled in the facility corrective action program.
Recover (RC)	Communications (RC.CO)	Communications are handled in accordance with site procedures. Reactors have an emergency plan that governs communications with external stakeholders.

TABLE A2.—U.S. Nuclear Power Reactor Practices Mapped to the Framework Core.

Function	Category	Subcategory	Profile
Identify (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	A-3.1.3 D-5.4 E-10.3, E-10.9
		ID.AM-2: Software platforms and applications within the organization are inventoried	D-5.4 E-10.3, E-10.9
		ID.AM-3: Organizational communication and data flows are mapped	D-1.4, D-1.18 E.3.4
		ID.AM-4: External information systems are catalogued	A-3.1.3 D-1.22
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	A-3.1.3 D-3.5 E-8.1
		ID.AM-6: Cyber security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	A-4.8, A-4.11 E-8.1
Identify (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cyber security roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	The cyber security program does not include specific provisions to supplement the reactors existing programs related to this activity.
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	The cyber security program does not include specific provisions to supplement the reactors existing programs related to this activity.

Function	Category	Subcategory	Profile
Identify (ID)	**Business Environment (ID.BE),** continued	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated	The cyber security program does not include specific provisions to supplement the reactors existing programs related to this activity for the organization as a whole. Mission, objectives, and activities regarding cyber security are addressed in A-4.11.
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	E-11.2
		ID.BE-5: Resilience requirements to support delivery of critical services are established	A-4.6, A-4.7 E-8.1, E-8.6
Identify (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber security risk.	**ID.GV-1:** Organizational information security policy is established	A
		ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners	A-4.11
		ID.GV-3: Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, are understood and managed	A-2.1, A-2.2
		ID.GV-4: Governance and risk management processes address cyber security risks	A-4.9
Identify (ID)	**Risk Assessment (ID.RA):** The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	A-3.1.5, A-4.4.3.2 D-5.5 E-3.2, E-3.5, E-11.5, E-11.6, E-12
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	A-4.9.1 E-3.5, E-9.8
		ID.RA-3: Threats, both internal and external, are identified and documented	A-2.1, A-4.9.1 E-3.5
		ID.RA-4: Potential business impacts and likelihoods are identified	A-3.1.3

Function	Category	Subcategory	Profile
Identify (ID)	**Risk Assessment (ID.RA),** continued	**ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	A-4.9.1,A-4.9.4
		ID.RA-6: Risk responses are identified and prioritized	A-4.2, A-4.9.4
Identify (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	The cyber security program does not include specific provisions to supplement the reactors' existing programs related to this activity.
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	The cyber security program does not include specific provisions to supplement the reactors' existing programs related to this activity.
		ID.RM-3: The organization's determination of risk tolerance is informed by their role in critical infrastructure and sector specific risk analysis	The cyber security program does not include specific provisions to supplement the reactors' existing programs related to this activity.
Protect (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	D-1.2, D-1.11 D-4.2, D-4.3, D-4.5, D-4.6, D-4.7
		PR.AC-2: Physical access to assets is managed and protected	D-4.4 E-5.4, E-5.5
		PR.AC-3: Remote access is managed	A-4.3 D-1.1 E-6
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	D-1.5, D-1.6, D-5.3
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	A-4.3 D-1.4 E-6

Function	Category	Subcategory	Profile
Protect (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cyber security awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	A-4.8 E-9.1, E-9.2, E-9.3
		PR.AT-2: Privileged users understand roles and responsibilities	A-4.8, A-4.11 E-7.2, E-8.3, E-9.1, E-9.3
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	A-4.8, A-4.11 E-11.1, E-11.2, E-11.3
		PR.AT-4: Senior executives understand roles and responsibilities	A-4.8, A-4.11 E-9.1, E-9.3
		PR.AT-5: Physical and information security personnel understand roles and responsibilities	A-4.8, A-4.11 E-9.1, E-9.3
Protect (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	D-3.19
		PR.DS-2: Data-in-transit is protected	D-3.6, D-3.7
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	E-1.6, E-10.9
		PR.DS-4: Adequate capacity to ensure availability is maintained	D-3.4
		PR.DS-5: Protections against data leaks are implemented	D-1.4, D-1.5, D-1.6, D-1.15, D-3.7, D-3.9, D-4.9, D-5.3 E-6
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	E-3.7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	D-5.4 E-10.3

Function	Category	Subcategory	Profile
Protect (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	A-3.1.3, A-3.1.5, A-4.4.1, A-4.4.2, A-4.5 D-1.18, D-5.4 E-10.3, E-10.7
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	A-4.5 E-11.3, E-11.4, E-11.5, E-11.6
		PR.IP-3: Configuration change control processes are in place	A-4.4.1 D-1.18, D-4.1, D-4.7, D-5.1, D-5.3 E-10.4, E-10.5, E-10.6, E-10.7, E-11.6
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	E-8.2, E-8.5
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	A-4.12 E-5.1
		PR.IP-6: Data is destroyed according to policy	E-1.6
		PR.IP-7: Protection processes are continuously improved	A-4.12 E-9.8
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	A-4.12
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	A-4.6, A-4.7 E-7.1, E-7.6, E-8.1
		PR.IP-10: Response and recovery plans are tested	E-7.3, E-8.2

Function	Category	Subcategory	Profile
Protect (PR)	**Information Protection Processes and Procedures (PR.IP),** continued	**PR.IP-11:** Cyber security is included in human resources practices (e.g., deprovisioning, personnel screening)	E-2.1, E-2.2, E-5.2
		PR.IP-12: A vulnerability management plan is developed and implemented	A-4.9 D-5.5 E-3.2, E-11.6, E-12
Protect (PR)	**Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	E-4.2, E-4.3
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Remote maintenance to critical safety, security, and reliability systems is prohibited by the defensive architecture described in the cyber security plan. (A-4.3)
Protect (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	D-2.1, D-2.2, D-2.3, D-2.6, D-2.7, D-2.12
		PR.PT-2: Removable media is protected, and its use restricted according to policy	D-1.2, D-1.19 E-1.4, E-1.5
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	D-1.2, D-1.3, D-1.11, D-1.16, D-5.1, D-5.4 E-10.8
		PR.PT-4: Communications and control networks are protected	A-4.3 E-6
Detect (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	D-2.6
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	D-2.6 E-7.4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	D-2.6 E-7.4, E-7.5
		DE.AE-4: Impact of events is determined	E-7.4
		DE.AE-5: Incident alert thresholds are established	D-5.2 E-3.4

Function	Category	Subcategory	Profile
Detect (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cyber security events	D-5.2 E-3.4, E-6
		DE.CM-2: The physical environment is monitored to detect potential cyber security events	D-4.4 E-5.6, E-5.7, E-5.8
		DE.CM-3: Personnel activity is monitored to detect potential cyber security events	E-2.1
		DE.CM-4: Malicious code is detected	E-3.3
		DE.CM-5: Unauthorized mobile code is detected	D-3.13
		DE.CM-6: External service provider activity is monitored to detect potential cyber security events	D-5.2 E-3.4, E-5.2
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	D-1.2, D-1.17, D-1.19 D-4.4, D-5.2, D-5.3 E-3.4, E-5.6, E-5.7, E-5.8, E-6, E-10.5
		DE.CM-8: Vulnerability scans are performed	E-12
Detect (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	A-4.6 E-3.4
		DE.DP-2: Detection activities comply with all applicable requirements	A-4.6
		DE.DP-3: Detection processes are tested	D-5.2 E-3.4
		DE.DP-4: Event detection information is communicated to appropriate parties	A-4.6 D-2.6
		DE.DP-5: Detection processes are continuously improved	A-4.6, A-4.12 E-12

Function	Category	Subcategory	Profile
Respond (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained to ensure timely response to detected cyber security events.	**RS.RP-1:** Response plan is executed during or after an event	A-4.6 E-8.1, E-8.6
Respond (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	A-4.6, A-4.8 E-7.1, E-7.6, E-8.1
		RS.CO-2: Events are reported consistent with established criteria	A-4.6
		RS.CO-3: Information is shared consistent with response plans	A-4.6 E-8.1
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	A-4.6, E-8.1
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness	A-4.6 E-3.5, E-9.8
Respond (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	D-2.6
		RS.AN-2: The impact of the incident is understood	E-7.4
		RS.AN-3: Forensics are performed	E-7.4
		RS.AN-4: Incidents are categorized consistent with response plans	E-8.1
Respond (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	A-4.6 E-7.4
		RS.MI-2: Incidents are mitigated	A-4.7 E-7.4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	A-4.9.1 E-12

Function	Category	Subcategory	Profile
Respond (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	A-4.9.3, A-4.9.4 E-3.11, E-8.1, E-7.4, E-12
		RS.IM-2: Response strategies are updated	A-4.9.4 E-7.1, E-7.4, E-7.6
Recover (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cyber security events.	**RC.RP-1:** Recovery plan is executed during or after an event	A-4.7 E-8.1
Recover (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	A-4.7, A-4.9.3, A-4.9.4 E-3.11, E-7.4, E-8.1, E-12
		RC.IM-2: Recovery strategies are updated	A-4.9.4 E-7.1
Recover (RC)	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams (CSIRTs), and vendors.	**RC.CO-1:** Public relations are managed	The cyber security program does not include specific provisions to supplement the reactors existing programs related to this activity.
		RC.CO-2: Reputation after an event is repaired	The cyber security program does not include specific provisions to supplement the reactors existing programs related to this activity.
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	A-4.7 E-8.1

TABLE A3.—U.S. Nuclear Power Reactor Practices Mapped to the Framework Tiers.

Tier Category	Characteristics: Tier 3, Repeatable	Characteristics: Tier 4, Adaptive	Nuclear Power Plant Implementation
Risk Management Process	The organization's risk management practices are formally approved and expressed as policy. Thus, organizational cyber security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.	The organization adapts its cyber security practices based on lessons learned and predictive indicators derived from previous and current cyber security activities. Through a process of continuous improvement incorporating advanced cyber security technologies and practices, the organization actively adapts to a changing cyber security landscape and responds to evolving and sophisticated threats in a timely manner.	**Current Practice:** Plants have an issued and approved Cyber Security Plan that is being implemented by an issued and approved Implementation Schedule, governing policies, and implementing procedures. The Plan establishes, implements, and maintains a cyber security program. Elements of the program were implemented by December 31, 2012, and are subject to oversight by the plant's independent oversight organization and to inspection by the NRC. The program is enhanced to address findings from oversight and inspection activities and industry lessons learned. **Future Practice:** Measures to manage evolving cyber risks to cyber systems and equipment and measures for timely detection and response to cyber security threats will be implemented. The fully implemented program will be inspected by the NRC and will be reviewed by the plant's independent oversight organization at a minimum of every two years to ensure the program remains effective. Plants will periodically review site and industry lessons learned to support program effectiveness.

Tier Category	Characteristics: Tier 3, Repeatable	Characteristics: Tier 4, Adaptive	Nuclear Power Plant Implementation
Integrated Risk Management Program	There is an organization-wide approach to manage cyber security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	There is an organization-wide approach to managing cyber security risk that uses risk-informed policies, processes, and procedures to address potential cyber security events. Cyber security risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.	**Current Practice:** The Plan is issued and approved. Implementing procedures for interim milestones are developed and issued. Cyber awareness training is provided to all plant personnel and vendor personnel performing maintenance on plant equipment. Job-function-specific training is provided for individuals performing duties associated with the interim milestones. Plants evaluate and manage cyber security risks for existing and new digital equipment using established policies and procedures. Attack detection and incident response measures are implemented. **Future Practice:** Cyber security training for specialized job skills will be provided.

Tier Category	Characteristics: Tier 3, Repeatable	Characteristics: Tier 4, Adaptive	Nuclear Power Plant Implementation
External Participation	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cyber security before a cyber security event occurs.	**Current Practice:** It is standard nuclear practice to share and receive lessons learned and operating experience from across the fleet of power plants. This sharing includes information on a range of topics that includes physical and cyber security. Certain cyber events are reported voluntarily to DHS, NERC, and the NRC in accordance with applicable requirements. DHS, NERC, and the NRC have the ability to disseminate information to plants and other stakeholders as necessary. Plants also voluntarily participate in a teleconference every other week that reviews of relevant threat and vulnerability notices, monthly DHS-coordinated unclassified teleconferences, and quarterly classified threat briefings. **Future Practice:** Current practices will be enhanced with implementing procedures directing the regular review of threat and vulnerability notices from credible sources.

Appendix B: Summary of Framework Use Steps

TABLE B1.—Summary of Framework Use Steps.

Step 1: Prioritize and Scope		
Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cyber security capabilities	1. Framework usage scope
Step 2: Orient		
Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and Informative References (e.g., cyber security and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cyber security and risk management standards, tools, methods, and guidelines 4. Evaluation approach
Step 3: Create a Current Profile		
Inputs	Activities	Outputs
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cyber security and risk management standards, tools, methods, and guidelines	1. Organization identifies its current cyber security and risk management state	1. Current Profile 2. Current Implementation Tier
Step 4: Conduct a Risk Assessment		
Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy 3. Organization-defined risk assessment approach 4. In-scope regulatory requirements 5. In-scope cyber security and risk management standards, tools, methods, and guidelines	1. Perform risk assessment for in-scope portion of the organization	1. Risk assessment reports

Step 5: Create a Target Profile		
Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Organizational objectives 4. Risk management strategy 5. Risk assessment reports	1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives	1. Target Profile 2. Target Tier
Step 6: Determine, Analyze, and Prioritize Gaps		
Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Target Profile 4. Target Tier 5. Organizational objectives 6. Impact to critical infrastructure 7. Gaps and potential consequences 8. Organizational constraints 9. Risk management strategy 10. Risk assessment reports	1. Analyze gaps between current state and Target Profile in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) on actions 6. Prioritize actions (CBA and consequences) 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan
Step 7: Implement Action Plan		
Inputs	Activities	Outputs
1. Prioritized implementation plan	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks, metrics, and performance indicators 4. Report progress	1. Project tracking data 2. New security measures implemented

Appendix C: Glossary

Aside from the term "organization," the following glossary is excerpted verbatim from the Framework.

Term	Definition
Category	The subdivision of a Function into groups of cyber security outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cyber security, national economic security, national public health or safety, or any combination of those matters.
Cyber Security	The process of protecting information by preventing, detecting, and responding to attacks.
Cyber Security Event	A cyber security change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Detect (Function)	Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
Framework	A risk-based approach to reducing cyber security risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cyber security activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cyber security risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cyber security activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (Function)	Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Organization	An operational entity of any size that uses the same cyber security risk management program within its different components, and may individually use the Framework.
Protect (Function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform.

Term	Definition
Recover (Function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.
Respond (Function)	Develop and implement the appropriate activities to take action regarding a detected cyber security event.
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.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

Homeland Security