Technical Issues for Consideration Regarding the Fuel Cycle Cyber Security Proposed Rulemaking

Developed by the Cyber Security Working Group to support the
Public Meeting Scheduled for
December 10, 2015

Enclosure 1

Document Purpose

This document addresses a number of technical issues relevant to the proposed fuel cycle cyber security rulemaking that will be discussed during the scheduled December 10, 2015, public meeting. The technical issues are presented as questions that the NRC cyber security working group is evaluating. The considerations which follow each question represent the working group's current thoughts on the technical issue. These questions and the subsequent considerations are being provided in advance of the public meeting to facilitate the discussion, enhance stakeholders' understanding of the technical issues being considered by the NRC staff, and provide stakeholders opportunity for input on technical issues.

Note 1: This document supersedes the similar document issued to support the public meeting held on October 22, 2015. This document addresses many of the comments received at that meeting and provides additional discussion on several issues.

Note 2: The issues identified for discussion in this document are not intended to specifically or comprehensively address stakeholder comments on the draft regulatory basis received during the comment period which closed October 5, 2015. The NRC staff is evaluating and will address those comments separately in the development of the final regulatory basis. This approach is subject to change based upon review of the public comments on the draft regulatory basis, future public meetings, and internal staff reviews.

Table of Contents

Technical Issues and Considerations

1. **What is the U.S. Nuclear Regulatory Commission (NRC) staff trying to prevent?**

   - A cyber attack that:
     - directly results in a safety consequence of concern (active); or
     - compromises a function needed to prevent, mitigate, or respond to a safety/security/safeguards event associated with a consequence of concern (latent).

2. **What are the consequences of concern for safety, security, and safeguards (3S) functions?**

   - Significant exposures to workers or members of the public (e.g., exposures as a result of releases of radioactive materials or chemicals and nuclear criticalities). [safety]
   - Radiological sabotage and theft or diversion of formula quantities of strategic special nuclear material (SSNM). [safety]
   - Loss of control and accounting of formula quantities of SSNM. [security and safeguards]
   - Unauthorized removal of special nuclear material (SNM) of moderate strategic significance [security]
   - Loss of control and accounting of SNM of moderate strategic significance. [security and safeguards]
   - Loss or unauthorized disclosure of classified information. [security]

   See Table 1, "Consequences of Concern and Scope," for additional description of each of these areas.

3. **What are the thresholds related to the consequences of concern for 3S functions?**

   The threshold to determine a consequence of concern consists of any of the criteria listed below.

   - Radiological exposure of 25 rem or greater to a worker; 25 rem or greater or 30 mg or greater intake of uranium in soluble form to any individual outside the controlled area. [safety]
   - Acute chemical exposure that could lead to irreversible or other serious, long lasting health effects to a worker or any individual located outside the controlled area. [safety]
   - Loss of the capability to protect against the DBTs as defined in 10 CFR 73.1(a)(1) Radiological Sabotage and 10 CFR 73.1(a)(2) Theft or Diversion of Formula Quantities of SSNM. [security]
   - Loss of the capability to: timely detect the possible abrupt loss (see 10 CFR 74.4) of a formula quantity of SSNM (see 10 CFR 74.51(a)) from an individual unit process; rapidly determine whether an actual loss of five or more formula kilograms occurred; continually confirm the presence of SSNM in assigned locations; timely generate information to aid in the recovery of SSNM in the event of an actual loss. [security and safeguards]
   - Loss of the capability to detect, assess and respond to unauthorized access or activities within controlled areas containing SNM of moderate strategic significance. [security]
   - Loss of the capability to: maintain accurate, current, and reliable information on, and confirm, the quantities and locations of SNM; permit rapid determination of whether an actual loss of a significant quantity of SNM has occurred (more than one formula kilogram of strategic SNM, or 10,000 grams or more of uranium-235 contained in uranium enriched up to 20.00 percent); generate information to aid in the investigation and recovery of missing SNM in the event of an actual loss. [security and safeguards]
   - Loss of the capability to protect classified information. [security]

See Table 1, "Consequences of Concern and Scope," for additional information.

4. How does the NRC staff propose to prevent these consequences from occurring?

- Establishing a risk-informed, performance-based, and graded regulatory framework for the various types of fuel cycle facilities.
- Establishing appropriate cyber security regulations informed by:
  - The power reactor cyber security rule (10 CFR 73.54) and the lessons learned during its implementation (see Question 14);
  - The consideration of the uniqueness of fuel cycle facilities;
  - Insights learned from site visits (see Question 15); and
  - Industry standards.

5. How is the draft approach risk-informed and consequence based?

The NRC intends to develop cyber security requirements for fuel cycle facilities, taking into account the safety significance of digital assets at these facilities and the risk resulting from a compromise of these assets. This approach will require the protection of those digital assets important to assuring (1) the health and safety of the public and the environment and (2) the common defense and security.

The staff envisions that the licensees will perform an analysis to identify those digital assets within the scope of the rule. The thresholds for identifying digital assets within scope (i.e., that if compromised could result in a consequence of concern) are consequence based. Question 11 provides additional information on how to perform the consequence analyses.

Licensees implement 3S programs to comply with existing risk-informed regulations in 10 CFR Parts 40, 70, 73, 74, and 95. The existing integrated safety analysis (ISA), security, and MC&A programs would be utilized to inform the cyber security program, identify which digital assets could be within scope of the rule, and inform the screening process. Each of the following programs uses a risk-informed, consequence based structure and will be used to inform the cyber security analysis.

- The ISA is implemented to prevent or mitigate significant exposure events (exposures in excess of the performance requirements) which could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public.
- The ISA requirements include prevention of nuclear criticalities. Criticalities are events in which large quantities of radiation are released and could endanger the life of workers.
- Physical security and MC&A programs are required to prevent the loss, theft or diversion of significant quantities of SNM. The requirements in the regulations are based on the protection of specific SNM quantities of concern for the three categories of facilities (i.e., Categories I, II, and III).
- Information security programs are required to prevent the loss/theft of classified information, which could cause damage to the United States.

See Table 1, "Consequences of Concern and Scope," for additional information.

Note: The definition of risk-informed regulation and active and latent consequence of concern can be found in the Glossary of Terms.

6. How is the draft approach graded and performance-based?

The staff is considering a number of options to ensure that the regulations will be graded and performance-based, including providing:

- A facility-type grading approach, as described in Table 2, "Draft Facility Type Approach Matrix for Cyber Controls," where the safety and security risks will be considered for each type of facility (e.g., Categories I, II, III, and source materials). The controls applied would be commensurate with the safety and security risks at each type of facility.
- A screening methodology that will reduce the number of digital assets that would require cyber security controls, which is illustrated in Figure 3, "Screening – Determine the Applicable Digital Assets," and Figure 6, "Screening Methodology for Digital Assets with a Latent Consequence of Concern."
- The NRC staff does not plan to address specific cyber security controls within the proposed regulation, but rather the staff is planning to develop guidance that uses/endorses industry recognized and consensus standards which will allow for a more flexible approach to implementation of programs and controls. Licensees would be able to analyze and justify why certain controls are not applicable to certain digital assets. This approach would also allow licensees to take credit for existing controls and/or use alternative controls.
- Licensees would be able to apply controls to entire networks as opposed to individual digital assets on networks.
- This approach will be incorporated into a Regulatory Guide being developed concurrent with the proposed rule.

Note: The definition of performance-based regulation can be found in the Glossary of Terms.

7. What digital assets are currently anticipated to be evaluated as part of the rule?

The initial set of digital assets for analysis is expected to include:

- Digital assets associated with significant exposure events (i.e., radiological or chemical thresholds from Question 3) which may include:
  - Operational and process controls (if analysis determines that compromise results in a significant exposure event). [Active]
  - Digital assets associated with preventing and mitigating significant exposure events (e.g., IROFS). [Latent]
  - Digital assets with a nexus to a significant exposure event (e.g., Security, MC&A). Security digital assets required in response to Security Orders (e.g., ICM, ASM). [Latent]
- Digital assets associated with protecting against the DBTs. [Latent]
  - Security Plans
  - Security Orders
- Digital assets associated with control and accounting of Formula Quantities of SSNM. [Latent]
  - Security Plans
  - FNMC Plan
  - Security Orders
- Digital assets associated with preventing unauthorized removal of SNM of moderate strategic significance. [Latent]
  - Security Plans
  - FNMC Plan
  - Security Orders

- Digital assets associated with control and accounting of SNM of moderate strategic significance. [Latent]
  - Security Plans
  - FNMC Plan
  - Security Orders
- Digital assets associated with physical security of classified information. [Latent]
  - Standard Practices and Procedures Plan
  - Security Plans
- Digital assets associated with support systems and equipment which, if compromised, would adversely impact 3S functions (i.e., availability, reliability, core functionality, or capability of in-scope assets),
  - Digital assets used as support systems may be in the IROFS boundary package and maintained through the existing configuration management program.
  - For example, an IROFS that depends upon data from the material control and accounting (MC&A) database would make the MC&A database a support system.
- Cyber security features needed to meet commitments in the cyber security program.

The staff intends to develop a screening process that will reduce the number of digital assets within the scope of the rule by allowing licensees to take credit for alternate controls. This draft screening process is illustrated in Figure 3, "Screening – Determine the Applicable Digital Assets," and Figure 6, "Screening Methodology for Digital Assets with a Latent Consequence of Concern."

The remaining subset of digital assets would have cyber security controls applied as described in Table 2, "Draft Facility Type Approach Matrix for Cyber Controls."

Additional description of digital assets currently anticipated to be within the scope of the proposed rule can be found in Table 1, "Consequences of Concern and Scope."

8. How does the NRC staff plan to use consensus standards in the guidance associated with the rule (Regulatory Guide)?

The staff plans to issue a Regulatory Guide that will reference applicable National Institute of Standards and Technology (NIST) standards, with limited exceptions where necessary. The two main NIST standards the staff plans to use are NIST Special Publication (SP) 800-37, Revision (Rev.) 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," and NIST SP 800-53, Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

The staff envisions the Regulatory Guide will follow the six steps in the risk management framework discussed in NIST SP 800-37, Rev. 1, as an acceptable means of meeting the proposed rule.

The Regulatory Guide will provide specifics as to what digital assets need to be protected. The Regulatory Guide will also contain a screening methodology that considers the impact of the loss/compromise of the digital assets and the availability of any alternative controls. This screening will reduce the number of digital assets that require cyber controls to be applied.

The Regulatory Guide will also provide guidance on the programmatic elements of the licensee's cyber security program (e.g., training, configuration management, and reporting requirements).

The staff understands that some licensees may already be following other industry standards or are required to meet other government requirements (via contract or regulation). The staff will provide guidance on how licensees can demonstrate equivalency with the guidance in the Regulatory Guide.

9. How will the risk management framework in NIST SP 800-37, Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," be modified in the Regulatory Guide?

See Figure 5, "Risk Management Framework" for the risk management framework. The NRC's proposal differs from the specific "Steps" of the NIST framework in the following respects:

- NIST Step 1 - The NIST risk management framework calls for a risk assessment of the information system/digital assets being protected be performed. In this case, the Regulatory Guide will provide a risk assessment by facility type for each of the different 3S controls (i.e., ranking of controls).

- NIST Step 2 - Instead of using the recommended baseline controls in NIST SP 800-53, Rev. 4, the Regulatory Guide will contain the baseline controls for each 3S category at a specific facility type. An overlay of controls will be included for those digital assets identified as being in place to address the DBTs. The Regulatory Guide will provide guidance on how the applicability evaluation of controls will be conducted.

- NIST Step 2 - The Regulatory Guide will recommend that a System Security Plan (SSP) be developed for each digital asset within scope. The SSP may be utilized to document the evaluation of applicable controls and how each applicable control will be implemented.

- NIST Step 4 - The Regulatory Guide will provide guidance that will allow the licensees to perform the independent analysis of security control implementation. Guidance on the performance of the evaluation will also be provided.

- NIST Step 5 - The Regulatory Guide will recommend that a senior licensee official be designated as the authorizing official. The Regulatory Guide will also address how plans of action and milestone documents are tracked, reviewed, and updated.

10. How are the DBTs factored into the determination of digital assets within scope of the rule?

Similar to 10 CFR 73.54, the NRC staff envisions that the proposed rule will require Category I licensees to provide high assurance that computer and communications systems and networks are adequately protected against cyber attacks, up to and including the DBTs. Category I licensees will need to do an evaluation to identify which digital assets are required to support the licensee's strategy to protect SNM from threats up to and including the DBTs of radiological sabotage and theft and diversion. The staff envisions that these digital assets, due to their consequences of concern, will require the highest level of cyber security controls.

Note: Digital assets on a classified network authorized to operate by another government agency would not be within scope and would not require additional controls.

11. How is the consequence analysis performed?

The consequence analysis consists of two considerations: latent and active.

Latent Analysis (including DBT)

The purpose of a "latent analysis" is to identify those digital assets that, if compromised, could fail to prevent, mitigate, or respond to a 3S event associated with a consequence of concern. The threshold for the applicable consequence of concern can be found in Table 1, "Consequences of Concern and Scope."

The licensee is encouraged to use any of the following to identify those digital assets that perform or support a 3S function from the:

- ISA;
- Security order commitments and physical security plan;
- Standard Practices and Procedures Plan; and
- Fundamental Nuclear Material Control Plan.

For this analysis, a licensee will group the digital assets based on the function type (e.g., safety, security and safeguards of SSNM (or DBT), security and safeguards of SNM of moderate significance, and security of classified information).

A licensee will then determine the need to address cyber security controls by utilizing Figure 6, "Screening Methodology for Digital Assets with a Latent Consequence of Concern." If the need to address cyber security controls has been identified, the applicable cyber security control set can then be determined through Table 2, "Draft Facility Type Approach Matrix for Cyber Controls."

Active Analysis

The purpose of an "active analysis" is to identify those digital assets that, if compromised, could directly lead to an event with a safety consequence of concern. Because most fuel cycle facility safety regulations do not require the consideration of malicious actions, some additional analysis is necessary. Identifying active consequence scenarios through the analysis of cyber attack vectors may not be effective given the complexity of evaluating the potential compromise of a 3S function (e.g., potential for multi-node failure, ineffectiveness of existing cyber security measures, detection and effects of compromise). An efficient approach for conducting the active analysis may begin by identifying the potential on-site sources that could result in a safety consequence of concern. To identify these potential sources, a licensee is encouraged to use existing analyses such as:

- ISA;
- Process hazards analysis;
- Previously considered malicious digital impacts;
- Vulnerability analysis; or
- Other safety or security information.

Once these on-site sources are identified, further analysis should be performed to determine if a barrier is present to prevent a cyber attack from resulting in a safety consequence of concern. Acceptable barriers to consider include:

- non-digital features, of an acceptable quality[1], that can withstand the actions resulting from a cyber attack;
- digital assets with cyber security controls applied via the "latent analysis" (note - when credited in an "active analysis," a higher cyber security control set may now be applicable to these assets, see Table 2, "Draft Facility Type Approach Matrix for Cyber Controls"); or
- digital assets with cyber security controls applied via other "active analyses."

In performing an "active analysis," no cyber security controls should be assumed to be in place other than those established via the "latent analysis" or other "active analyses". Cyber security controls applied via other analyses (i.e., not related to NRC cyber security regulations) should only be considered as defense-in-depth.

If no existing barrier can be identified, cyber security controls are needed for the digital asset under consideration. The applicable cyber security control set can be determined through Table 2, "Draft Facility Type Approach Matrix for Cyber Controls." Providing the applicable cyber security control set establishes an acceptable barrier to prevent the cyber attack from actively causing a consequence of concern. Once an acceptable barrier is identified or established, no additional cyber security controls are needed and the requirements are met.

*See screening method for determination of adequate equivalent function criteria.

12. What does the NRC staff mean by a phased implementation of the rule?

Instead of a single implementation date, the staff currently envisions implementation with two milestones, as follows:

- Milestone 1 (completion of step 2 in the Risk Management Framework (RMF))
    - Develop programmatic elements;
    - Identify digital assets in scope, apply screening methodology for latent consequence digital assets, and select security controls and develop SSPs, including applicability evaluations;
- Milestone 2 (completion of step 5 in the RMF)
    - Implementation of security controls to digital assets;
    - Independent assessment; and
    - Authorization to operate.

See Figure 2, "Phased Implementation Approach," for a draft diagram of the phased implementation approach.

Phased implementation is a lesson learned from the power reactor rule implementation. Phased implementation facilitates the early identification of issues and ensures a consistent

[1] The non-digital feature should be sufficiently reliable and adequately implemented through appropriate management measures for the application under analysis. The non-digital feature should be implemented to a level consistent with other similar designated controls (i.e., IROFS). An acceptable evaluation may utilize the guidance in the facility-specific ISA for the management and assurance measure criteria for passive engineering controls, active engineering controls, or administrative controls. An acceptable evaluation may also compare the non-digital feature to an IROFS or designated control of a similar type. The non-digital control should be a formally maintained control and should be reliable. The results of the management and assurance measure affecting the non-digital feature should be documented, if applicable to the type of measure.

application of the regulations. The rule will include a date by which full implementation will be required.

13. How is the NRC staff keeping safety/security in mind to ensure that there are no unintended consequences?

The proposed approach would not require the ISA or existing Standard Practices and Procedures Plan, Physical Security Plan, or MC&A Plan to be modified as a result of the new cyber requirements. The existing ISA, security, and MC&A programs would be utilized to inform the cyber security program, identify which digital assets could be within scope of the proposed rule, and inform the screening process.

Applying cyber security controls will prevent a cyber attack from directly causing a consequence of concern and will protect digital assets needed to prevent, mitigate, or respond to a consequence of concern.

14. How have you incorporated the lessons learned from the power reactor cyber security rule implementation?

The fuel cycle cyber security working group has incorporated a number of lessons learned from the reactor cyber security rulemaking, including:

- The guidance provided for identification of within scope digital assets will be more specific;
- Screening methodology will use a risk-informed process to reduce the number of digital assets within the scope of the rule;
- Focus licensees on satisfying the security objective, rather than the exact wording of the control, by adding flexibility to:
  - tailor cyber security controls to account for system functionality/capability, similar to the approach taken with NEI 13-10 Appendices, and
  - take credit for existing programs and alternate controls that perform equivalent functions;
- Phased implementation will follow the NIST Risk Management Framework – less focus on specific control implementation and more focus on ensuring licensee programs and processes are sound prior to focusing on technical implementation; and
- Implementation schedule will have a shorter timeline with firm deadlines.

15. What insights did you learn from the site visits?

NRC staff visited four FCFs, including Honeywell - conversion facility, Westinghouse fuel fabrication facility, Global – fuel fabrication facility, and BWXT – Category I fuel facility. A conference call was also conducted with Areva – fuel fabrication facility.

All licensees were being proactive with their cyber security efforts. The NRC staff observed areas of improvement over the previous visits several years ago, however, the licensees all have plans for further improvement.

NEI voluntary initiative implementation

- Formation of cyber security assessment team (CSAT)
- Training appropriate personnel on cyber security program
- Establishing controls for portable media and devices
- Establishing a cyber security incident response and recover capability

- Implementation summary – no licensee had completed all of the items and implementation approaches varied

16. What should be done after the final set of digital assets are identified to determine the appropriate cyber security controls?

Consistent with guidance in NIST SP 800-53, Rev. 4, the NRC plans to issue regulatory guidance that encourages licensees to identify a set of controls common to all digital assets and document those in a separate plan.

Common controls are security controls whose implementation results in a security capability that is *inheritable* by one or more organizational information systems. Examples of common controls include: physical and environmental protection controls, personnel security controls, etc.

Common controls are generally documented in the organization-wide *system security plan* unless implemented as part of a specific information system, in which case the controls are documented in the system security plan for that system. Organizations have the flexibility to describe common controls in a single document or in multiple documents with references or pointers, as appropriate.

Once this is complete, a licensee would then move on to evaluating each digital asset according to its designated control set (i.e., applicability determination evaluation).

Security controls not designated as common controls are considered *system-specific* or *hybrid* controls. System-specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a *hybrid* status to security controls when one part of the control is common and another part of the control is system-specific. For example, an organization may choose to implement the Incident Response Policy and Procedures security control (IR-1) as a hybrid control with the policy portion of the control designated as common and the procedures portion of the control designated as system-specific.

See NIST SP 800-37, Rev. 1, section 3.2, and NIST SP 800-53, Rev. 4, sections 2.3 and 2.4.

17. How is the control applicability determination evaluation performed?

Once the control set is identified for a digital asset determined to be in scope (facility type matrix), each control in the set should be evaluated for applicability as follows:

- Implement the security control
- If the security control cannot be implemented, apply compensating security controls that eliminate threats and attack paths associated with the security control by:
  - documenting the technical rationale for the need to use compensating security controls
  - describing the compensating security controls to be employed
  - documenting the technical rationale for how the compensating security controls:
    - meet the intent of the security control
    - provide equivalent or greater protection as the security control
  - implementing the compensating security controls

- If neither the security control nor compensating security controls can be implemented, designate the control as "Not Applicable" by:
  - documenting the technical rationale for the inability to apply the security control and compensating security controls
  - conducting a threat and attack path analysis of the digital asset
  - provide documented justification demonstrating that an attack path does not exist
  - documenting the residual cyber security risk to the digital asset

Note that although NIST allows entities to disregard a control based on a risk evaluation, this will not be permitted under the process envisioned for this rule. Each control will have to be addressed through the process described above.

Compensating controls are alternative security controls employed by organizations in lieu of specific controls in the baselines—controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems.

Examples of compensating controls include:

AC-11 SESSION LOCK
The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures.

- Justification for inability to apply control: System does not have integrated identification and authentication - if powered on, it may be operated by anyone with physical access.

- Compensating control: System is located in an area with physical access control. Access to the area requires an approved badge with membership in critical group. Area is surveilled by active camera system and door alarms. This satisfies the control intent of preventing unauthorized access and operation of the system.

AU-2 AUDIT EVENTS
The organization determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];….etc.

- Justification for inability to apply control: System does not have physical capability to record commands and operator actions.

- Compensating control: System access, usage, and activity is monitored by active camera system. Video feeds are maintained for 180 days. This satisfies the control intent of providing non-repudiation of activity and support for after-the-fact investigations of security incidents.

RA-5 VULNERABILITY SCANNING
The organization scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;…remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk….etc.

- Justification for inability to apply control: System utilizes a proprietary protocol for which no commercial vulnerability scanning tool is available.

- Compensating controls: Vendor support contracts require vendor to: notify licensee within one week of the discovery of a confirmed security vulnerability. This satisfies the control intent of timely identification of potential security risks. Vendor support contracts require vendor to: provide patches, workarounds, or security fixes in a timely manner to address confirmed security vulnerabilities. This satisfies the control intent of timely remediation/mitigation of potential security risks.

SC-8 TRANSMISSION CONFIDENTIALITY
The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.

- Justification for inability to apply control: System utilizes a proprietary protocol that does not support encryption.

- Compensating control: The system has a wired serial connection which runs from Building 1 to the Plant Control System (PCS) in Building 3. The coaxial communications cable is housed in a secure conduit to prevent unauthorized access.

This process will be discussed in the Regulatory Guide.

See Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," section C.3.3; NIST SP 800-53, Rev. 4, "Recommended Security Controls for Federal Information Systems," section 3.2, and NIST SP 800-82, Rev. 2, "Guide to Industrial Control Systems (ICS) Security," section 6.2

18. Since the proposed control sets only list the control names, how is a licensee to determine the necessary robustness of the control?

A description and supplemental guidance for each control is provided in Appendix F of NIST SP 800-53, Rev. 4. The security controls in the catalog, with few exceptions, have been designed to be policy- and technology-neutral. Therefore, the guidance is not sufficiently detailed to provide specific implementation details.

However, the guidance does provide sufficient information regarding the intent of the control. This intent informs the application of the fundamental measures or countermeasures necessary to protect information during processing, while in storage, and during transmission. To meet acceptable levels of assurance, the licensee must apply the concepts/intent of the security controls to the specific technologies in use at their facility. Additional control guidance for industrial control systems is provided in NIST SP 800-82, Rev. 2.

The licensee must document each control in the SSP, using sufficient detail to facilitate inspection and assessment. Appendix F of NIST SP 800-53A, Rev. 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," describes the assessment objective for each control, including assessment methods and assessment objects. Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling/producing the evidence necessary to make the determination associated with each assessment objective.

The robustness of the control will be evaluated in accordance with the level of assurance required by the rule for the system/facility type. This evaluation will compare the control implementation against well-accepted guidance from credible sources, such as NIST, the SANS Institute, the Department of Homeland Security (DHS), the National Security Agency (NSA), the International Society for Automation (ISA) and others.

See NIST SP 800-53, Rev. 4, Appendix F; NIST SP 800-53A, Rev. 4, Appendix F; NIST SP 800-82, Rev. 2, Appendix G

19. What information is needed in a System Security Plan (SSP)?

The intent of the SSP(s) is to list and describe the digital assets (systems) that fall within the scope of the rule (i.e., require the application of security controls) and identify their risk categories (dictated by rule/guidance language using the facility-type approach) and document the application of controls to the digital assets (systems). An individual should be able to review the SSP(s) and understand what digital assets (systems) have been identified through the screening process as requiring security controls; what control sets are applied based on the facility-type approach; and the end state of each security control (e.g., description of control implementation, justification and analysis for non-application, use of compensating control, residual risk, etc.). In addition, the SSP(s) may include a description of the following for each digital asset (system):

- Function (e.g., Safety, Security)
- Purpose
- Environment and location
- Responsible individuals
- Support systems
- Interconnections
- Inventory (hardware, software)
- Monitoring strategy
- Plan of Actions and Milestones (POAMs) as a companion to the SSP
- Control status table (partial example)
- Controls template (partial example)

Control status table (partial) example:

Control Number and Name	Satisfied	Not Satisfied	Not Applicable	Inherited / Common
AC-1 Access Control Policy	X			
AC-2 Account Management		E3 (M, E1)	E2	
AC-3 Access Enforcement	X			
AC-4 Information Flow	X			
Percent of controls / category	**75%**	**25%**		

Controls template (partial) example (AC-1 Access Control Policy and Procedures):

System:	ACME Access Control Enhanced Security System (AACESS)
Function:	Security
Risk category:	High
Control set:	1
Location:	See attached diagram
Responsible individual:	Wile E. Coyote
Support systems and interconnections:	See attached diagram
Inventory:	See attached list

Description:	AACESS is a major application owned by the ACME Security department. AACESS consists of 2 systems: Badge issuance which controls creating and issuing badges with credentials; and the physical access control system which controls utilization of the badge credentials for physical access to the plant and other controlled areas.	
Control:	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
Supplemental Guidance:	The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	
Control Enhancements:	None	
Common Control Identification, Scoping Guidance, and Responsibility for Implementation		
ACME provides a plant-wide access control policy for all systems. System owners may develop a system specific access control policy to address system-specific requirements. System owners are responsible for developing formal, documented system-specific procedures to facilitate policy-compliant implementation of the access control policy and associated controls.		
System Specific Implementation Detail	**Status:**	**Satisfied**
The ACME plant-wide access control policy fully meets the needs for AACCESS. The system depends on the ACME Information Technology Policy Standards & Training Team to develop, coordinate training for, and maintain the ACME IT security policies. In addition, the ACME Security Organization has documented the access control procedures within the AACCESS Security Policy and Procedures document and the Systems Security Plan. Access control is based on a role-based protocol. The role-based user profile ensures that individuals have system access privileges that do not exceed the scope of their duties.		

See NIST SP 800-37, Rev. 1, section 3.3; NIST SP 800-18, “Guide for Developing Security Plans for Federal Information Systems”

20. What is meant in “Step 4 – Assess Security Controls” by an independent assessment?

Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

The information system owner relies on the technical expertise and judgment of assessors to: (i) assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings are an unbiased, factual reporting of the weaknesses and deficiencies discovered during the security control assessment.

An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to an entity outside of the organization.

The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the *security assessment report*. The security assessment report is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings.

The security assessment report identifies specific weaknesses and deficiencies in the security controls employed within or inherited by the information system that could not reasonably be resolved during system development or that are discovered post-development. Such weaknesses and deficiencies are potential vulnerabilities if exploitable by a threat source. The findings generated during the security control assessment provide important information that facilitates a disciplined and structured approach to mitigating risks in accordance with organizational priorities and regulatory requirements.

NRC regulatory guidance will discuss the robustness of the security assessment report, likely by referencing NIST SP 800-53A, Rev. 4. Under the current approach, NRC expects to focus inspection on the verification of the independence and qualifications of the assessor and that the identified weaknesses and deficiencies have been addressed by the licensee.

Organizations review assessor findings and determine the severity or seriousness of the findings and whether the findings are sufficiently significant to be worthy of further investigation or remediation. Senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions and business functions for the organization or correcting the deficiencies that pose the greatest degree of risk. If weaknesses or deficiencies in security controls are corrected, the security control assessor reassesses the remediated controls for effectiveness.   The security plan is updated and reflects the actual state of the security controls after the initial assessment and any modifications by the information system owner or common control provider in addressing recommendations for corrective actions.

Security control assessments and privacy control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits – rather, such assessments are the principal vehicle used to verify that implemented security controls and privacy controls are meeting their stated goals and objectives. NIST SP 800-53A, Rev. 4 is written to facilitate security control assessments and privacy control assessments conducted within an effective risk management framework.

See NIST SP 800-37, Rev. 1, section 3.4; NIST SP 800-53A, Rev. 4.

21. What is the purpose of authorizing an information system to operate (approval of SSP)?

The explicit acceptance of *risk* is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to organizational operations, organizational assets, individuals, or other organizations, is acceptable. The authorizing official reviews the *security authorization package* which contains: (i) the security plan; (ii) the security assessment report; and (iii) the POAM. The authorization package provides relevant information on the security state of the information system including the ongoing effectiveness of the security controls employed within or inherited by the system. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The authorizing official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials.

The *authorization decision document* conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date. The security *authorization decision* indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The *terms and conditions* for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires. Note that the NRC plans to recommend a 3 year period for authorization in the Regulatory Guide.

See NIST SP 800-37, Rev. 1, section 3.5

22. What is the purpose of a Plan of Action and Milestones (POAM) and how should the licensees track the actions?

The POAM, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The POAM identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. The POAM is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment. POAM entries are *not* required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the authorizing official.

Organizations define a strategy for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is consistent across the organization. The strategy helps to ensure that organizational plans of action and milestones are based on: (i) the security categorization of the information system; (ii) the specific weaknesses or deficiencies in the security controls; (iii) the importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system, and hence on the risk exposure of the organization, or ability of the organization to perform its mission or business functions); and (iv) the organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources).

For the tracking of the items in the POAM, the NRC will recommend that the licensee use its corrective action program. For those licensees without an NRC approved corrective action program, the guidance will recommend that the plans of action and milestones be reviewed and updated every 90 days.

In addition, during initial implementation of the rule, the NRC expects licensees will implement all of the security controls for each digital asset within scope. However, the NRC recognizes that with the expected short implementation period, regulatory guidance will be necessary to address some of the potentially longer implementation timeframes that may be captured in a POAM.

Also, as this will be a cyber security program with continuous monitoring, changes will be made over time and may result in additional actions needing to be captured in a POAM.

See NIST SP 800-37, Rev. 1, section 3.5

23. What is meant by Step 6 in the risk management framework (monitor security controls)?

Step 6 of the RMF, “Monitor Security Controls,” is a well-executed plan that continually assesses risks and vulnerabilities while monitoring and managing changes to digital assets (systems) and their respective security controls in order to maintain an effective Cyber Security Program. The following six guidelines can be used to help develop an effective program for monitoring security controls:

1. <u>Digital Asset (Systems) and Environment Changes</u>
   Digital assets (systems) in some cases are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the assets/systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to the assets/systems or its environment of operation is an essential element of an effective security control monitoring program.

2. <u>Ongoing Security Control Assessments</u>
   Organizations assess all security controls employed within and inherited by the digital assets (systems) during the initial security authorization. Subsequent to the initial authorization, the organization assesses a subset of the security controls (including management, operational, and technical controls) on an ongoing basis during continuous monitoring. Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors.

3. <u>Ongoing Remediation Actions</u>
   The assessment information produced by an assessor during continuous monitoring is provided to the digital asset (system) owner and common control provider in an updated *security assessment report*. The digital asset (system) owner and common control provider initiate remediation actions on outstanding items listed in the POAM and findings produced during the ongoing monitoring of security controls.

4. Key Updates
   To facilitate the near real-time management of risk associated with the operation and use of the digital assets (systems), the organization updates the system security plan, security assessment report, and POAM on an ongoing basis.

5. Security Status Reporting
   The results of monitoring activities are recorded and reported to the authorizing official on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be: (i) event-driven (e.g., when the digital asset (system) or its environment of operation changes or the system is compromised or breached); (ii) time-driven (e.g., weekly, monthly, quarterly); or (iii) both (event- and time-driven).

6. Ongoing Risk Determination and Acceptance
   The authorizing official or designated representative reviews the reported security status of the digital assets (systems) (including the effectiveness of deployed security controls) on an ongoing basis, to determine the current risk to organization and assets. The authorizing official determines, with inputs as appropriate, whether the current risks are acceptable and forwards appropriate direction to the digital asset (system) owner or common control provider.

   See NIST SP 800-37, Rev. 1, section 3.6

Glossary of Terms

3S function:

An action or activity that makes use of assets, personnel, policies, procedures, or programs to meet a safety, security, or safeguards licensing basis commitment (e.g., protect, assess, detect, respond, communicate, or provide control and accounting).

Performance-based regulation:

A regulatory approach that focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. Performance-based regulation leads to defined results without specific direction regarding how those results are to be obtained. At the NRC, performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety margin and offer incentives for licensees to improve safety without formal regulatory intervention by the agency.

Risk-informed regulation:

An approach to regulation taken by the NRC, which incorporates an assessment of safety significance or relative risk. This approach ensures that the regulatory burden imposed by an individual regulation or process is appropriate to its importance in protecting the health and safety of the public and the environment.

Consequence of concern:

Revise to be consistent with new table, see Table 1, "Consequence of Concern and Scope," for additional information.

Safety:
Significant exposure events which could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals).

Security and Safeguards of SSNM:

- Radiological Sabotage and Theft or Diversion of Formula Quantities of SSNM.
- Loss of control and accounting of Formula Quantities of SSNM

Security and Safeguards of SNM of Moderate Strategic Significance:

- Unauthorized removal of special nuclear material of moderate strategic significance
- Loss of control and accounting of SNM of moderate strategic significance

Security of Classified Information:

- Loss or unauthorized disclosure of classified information

Active consequence digital asset:

Digital asset whose compromise could directly result in a safety consequence of concern.

Latent consequence digital asset:

Digital asset associated with safety/security/safeguards functions needed to prevent, mitigate, or respond to an event associated with a consequence of concern.

Table 1 – Consequences of Concern and Scope

Function and (Applicability)	Consequence of Concern	Thresholds	Examples of Digital Assets*
Safety (Applies to all FCFs)	Significant exposure events which could endanger the life of workers or could lead to irreversible or other serious, long-lasting health effects to workers or members of the public (e.g., nuclear criticalities and releases of radioactive materials or chemicals).	Radiological exposure: - 25 rem or greater worker; - 25 rem or greater or 30 mg or greater intake of uranium in soluble form outside the controlled area (any individual). Acute chemical exposure: - Could lead to irreversible or other serious, long lasting health effects to a worker or any individual located outside the controlled area	Digital assets associated with significant exposure events which may include: - Operational and process controls (i.e., analysis determines that compromise results in a significant exposure event). [Active] - Digital assets associated with preventing and mitigating significant exposure events (e.g., IROFS). [Latent] - Digital assets with a nexus to a significant exposure event (e.g., Security, MC&A). Security digital assets required in response to Security Orders (e.g., ICM, ASM). [Latent]
Security (Applies to Cat I's)	Radiological Sabotage and Theft or Diversion of Formula Quantities of SSNM.	Loss of the capability to protect against the DBTs as defined in: - 10 CFR 73.1(a)(1) Radiological Sabotage - 10 CFR 73.1(a)(2) Theft or Diversion of Formula Quantities of SSNM.	Digital assets associated with protecting against the DBTs. [Latent] - Security Plans - Security Orders

Function and (Applicability)	Consequence of Concern	Thresholds	Examples of Digital Assets*
Safeguards of SSNM (Applies to Cat I's)	Loss of control and accounting of Formula Quantities of SSNM	Loss of the capability to: -Timely detect the possible abrupt loss of five or more formula kilograms of SSNM from an individual unit process; - Rapidly determine whether an actual loss of five or more formula kilograms occurred; - Continually confirm the presence of SSNM in assigned locations; and - Timely generate information to aid in the recovery of SSNM in the event of an actual loss.	Digital assets associated with control and accounting of Formula Quantities of SSNM. [Latent] - Security Plans - FNMC Plan - Security Orders
Security (Applies to Cat I and II)	Unauthorized removal of special nuclear material of moderate strategic significance	Loss of the capability to: - Detect, assess and respond to unauthorized access or activities within controlled areas containing SNM of moderate strategic significance.	Digital assets associated with unauthorized removal of SNM of moderate strategic significance. [Latent] - Security Plans - FNMC Plan - Security Orders

Function and (Applicability)	Consequence of Concern	Thresholds	Examples of Digital Assets*
Safeguards of SNM of Moderate Strategic Significance (Applies to Cat I and II)	Loss of control and accounting of SNM of moderate strategic significance	Loss of the capability to: - Maintain accurate, current, and reliable information on, and confirm, the quantities and locations of SNM; - Permit rapid determination of whether an actual loss of a significant quantity of SNM has occurred, with significant quantity being either: More than one formula kilogram of strategic SNM; or 10,000 grams or more of uranium-235 contained in uranium enriched up to 20.00 percent. - Generate information to aid in the investigation and recovery of missing SNM in the event of an actual loss.	Digital assets associated with control and accounting of SNM of moderate strategic significance. [Latent] - Security Plans - FNMC Plan - Security Orders
Physical Security of Classified Information (Applies to FCF's with a Part 95 FSC or NRC is the CSA)	Loss or unauthorized disclosure of classified information	Loss of the capability to protect classified information.	Digital assets associated with physical security of classified information. [Latent] - Standard Practices and Procedures Plan - Security Plans

*The digital assets within scope may also include: support systems equipment which, if compromised, would adversely impact 3S functions; and cyber security features needed to meet commitments in the cyber security program.

Table 2 – Draft Facility Type Approach Matrix for Cyber Controls

Facility Type	Asset Function	Cyber Security Controls	
		Set I[1]	Set II[1]
Category I Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	applicable for all – add DBT overlay[4]	-
Category II Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable for all
Category III Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable only for response to security orders and physical protection of classified[5]
Part 40 Conversion / Deconversion Facilities	Safety	applicable only for active consequence[2]	applicable only for latent consequence[3]
	Security & Safeguards	-	applicable only for response to security orders

[1] Set I or II refer to a baseline set of cyber security controls (see NRC Regulatory Guide for Fuel Cycle Cyber Security and NIST SP 800-53, Rev. 4)
Set I ≈ “high control baseline” and Set II ≈ “moderate control baseline”; both Set I and Set II include common programmatic controls

[2] Active consequence – asset function needed to prevent a cyber attack from directly causing a safety consequence of concern

[3] Latent consequence – asset function needed to prevent, mitigate, or respond to a safety/security/safegaurds event associated with a consequence of concern

[4] DBT overlay – additional cyber security controls specific to the design basis threats (from the NRC Regulatory Guide for Fuel Cycle Cyber Security)

[5] Physical protection of classified – asset function needed for the physical protection of classified information or matter

Figure 1 – General Overview of Implementation and Oversight

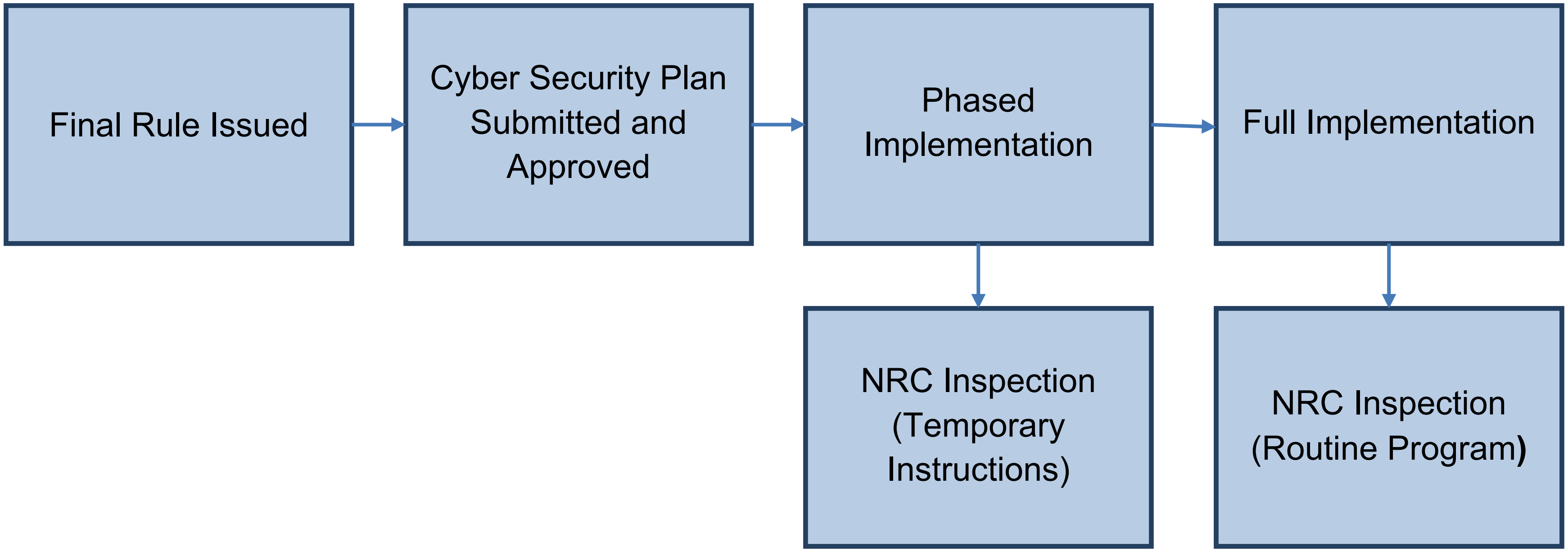

Final Rule Issued
Cyber Security Plan Submitted and Approved
Phased Implementation
Full Implementation
NRC Inspection (Temporary Instructions)
NRC Inspection (Routine Program)

Figure 2 – Phased Implementation Approach

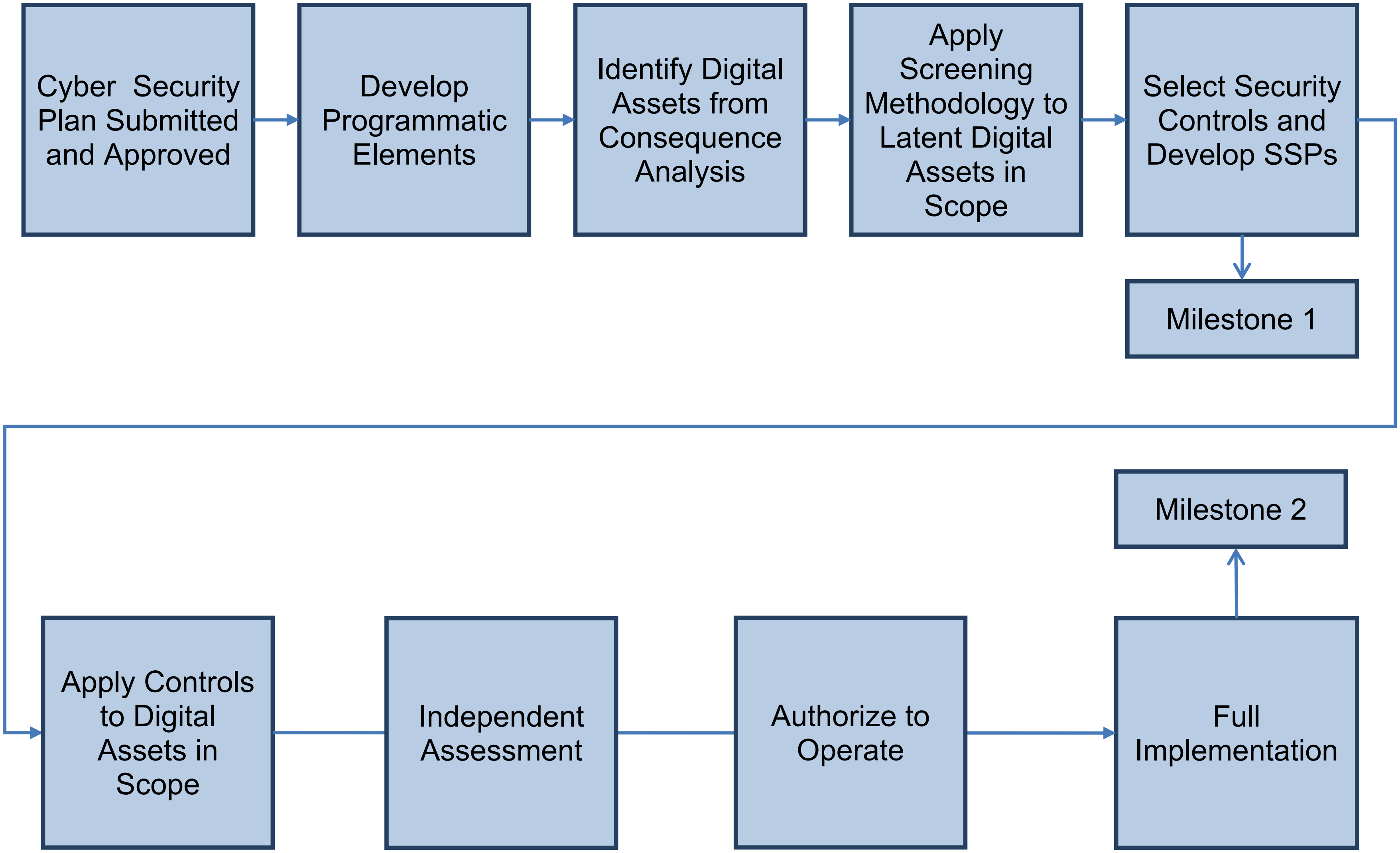
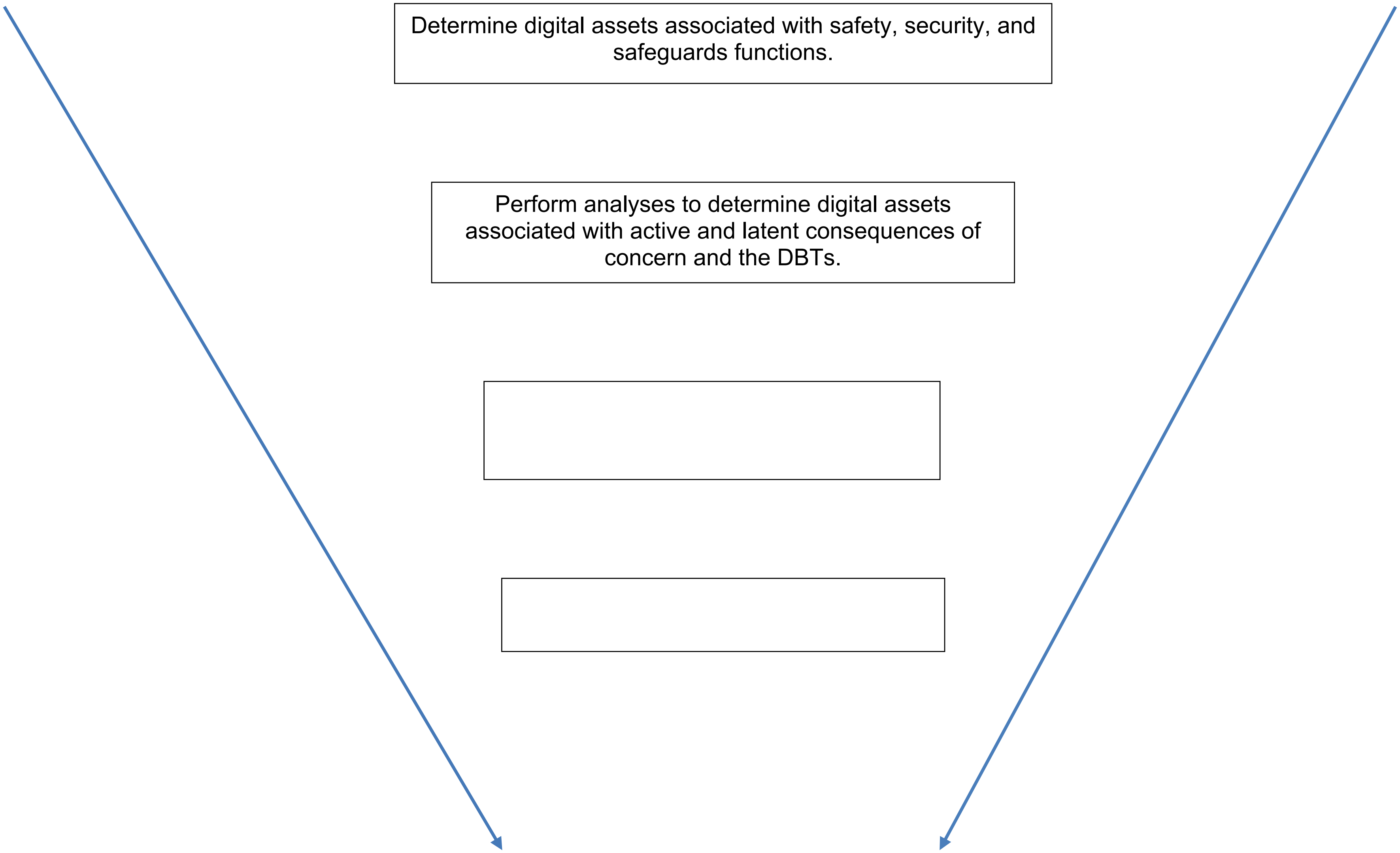

Cyber Security Plan Submitted and Approved
Develop Programmatic Elements
Identify Digital Assets from Consequence Analysis
Apply Screening Methodology to Latent Digital Assets in Scope
Select Security Controls and Develop SSPs
Milestone 1
Milestone 2
Apply Controls to Digital Assets in Scope
Independent Assessment
Authorize to Operate
Full Implementation

Figure 3 – Screening - Determine the Applicable Digital Assets



Determine digital assets associated with safety, security, and safeguards functions.

Perform analyses to determine digital assets associated with active and latent consequences of concern and the DBTs.

Figure 4 – Cyber Security Program with Ongoing Evaluations and Improvements

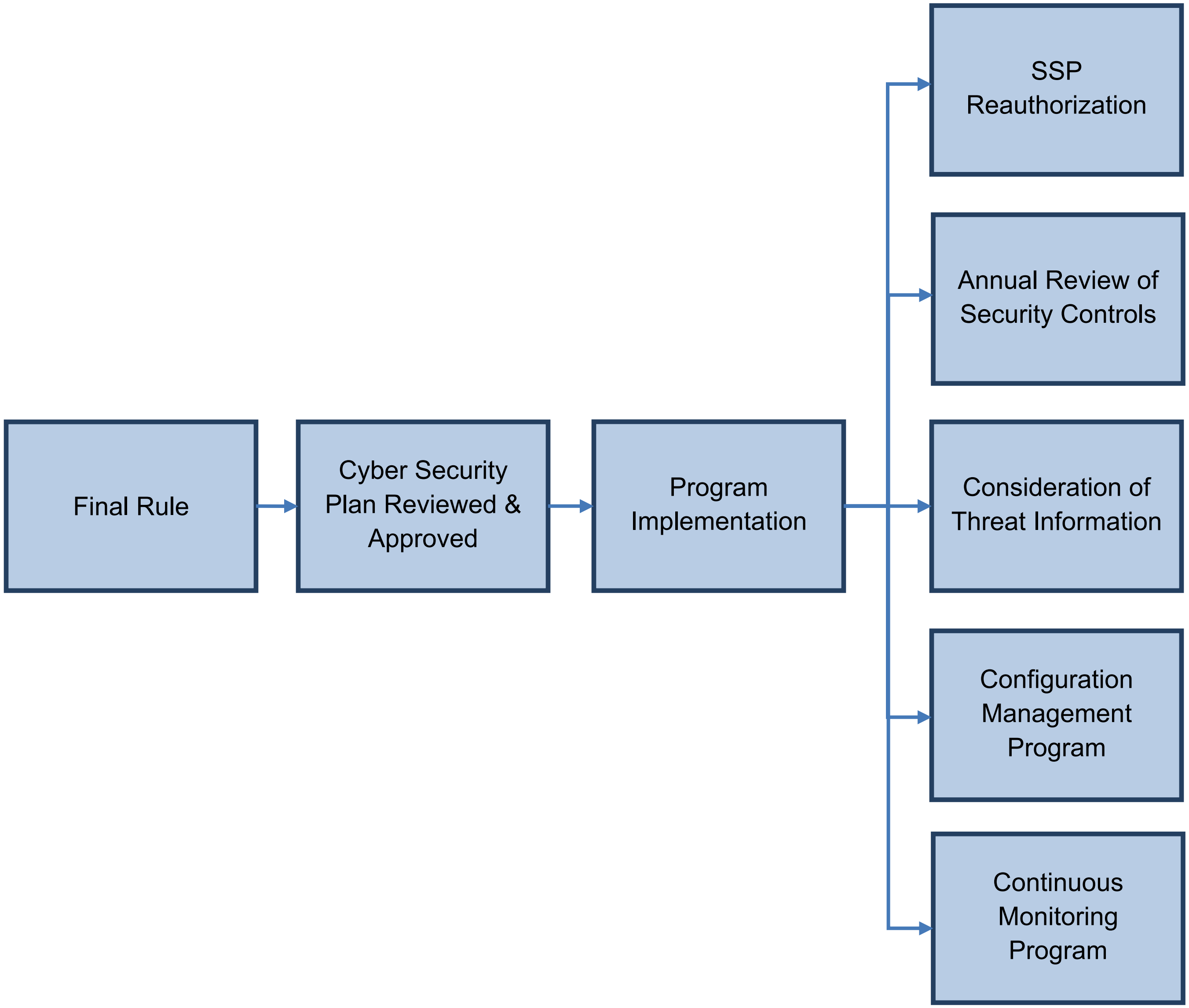
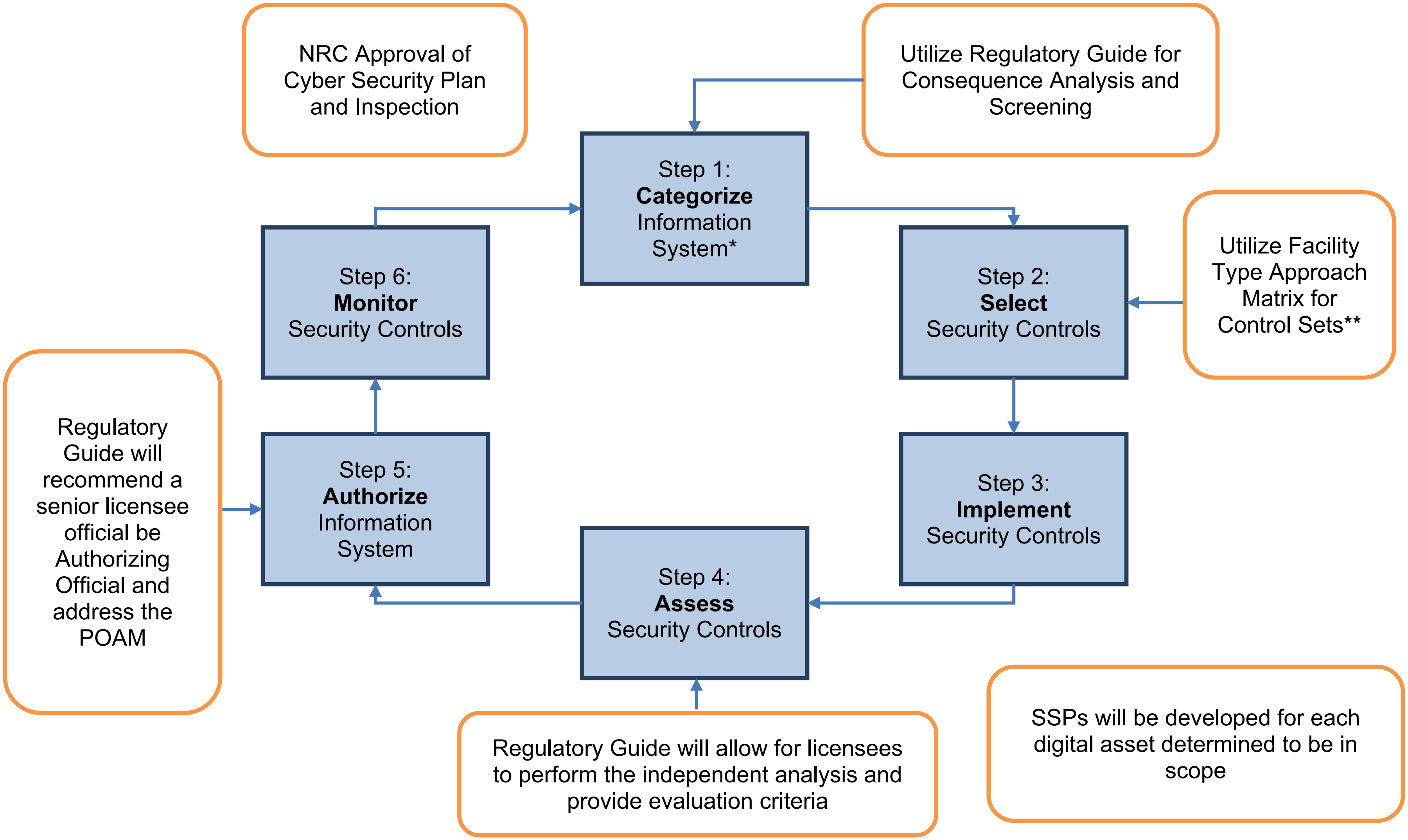

Final Rule
Cyber Security Plan Reviewed & Approved
Program Implementation
SSP Reauthorization
Annual Review of Security Controls
Consideration of Threat Information
Configuration Management Program
Continuous Monitoring Program

Figure 5 – Risk Management Framework



NRC Approval of Cyber Security Plan and Inspection

Utilize Regulatory Guide for Consequence Analysis and Screening

Step 1: **Categorize** Information System*

Step 2: **Select** Security Controls

Utilize Facility Type Approach Matrix for Control Sets**

Step 3: **Implement** Security Controls

Step 4: **Assess** Security Controls

Step 5: **Authorize** Information System

Step 6: **Monitor** Security Controls

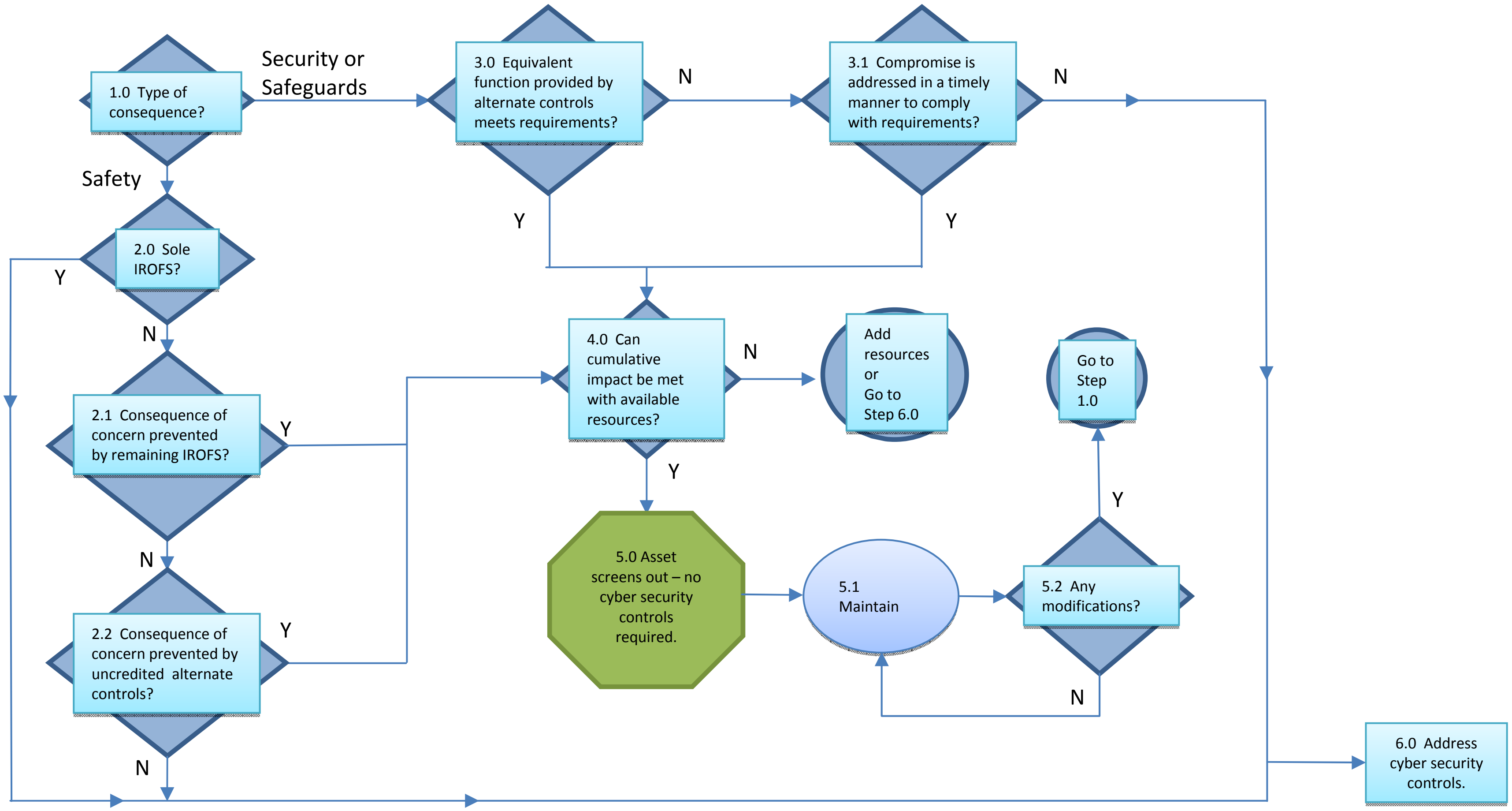
Regulatory Guide will recommend a senior licensee official be Authorizing Official and address the POAM

Regulatory Guide will allow for licensees to perform the independent analysis and provide evaluation criteria

SSPs will be developed for each digital asset determined to be in scope

*Evaluate each digital asset, group of digital assets, or information system. **Tailor each control consistent with NIST guidance.

Figure 6 – Screening Methodology for Digital Assets with a Latent Consequence of Concern


1.0 Type of consequence?
Security or Safeguards
3.0 Equivalent function provided by alternate controls meets requirements?
N
3.1 Compromise is addressed in a timely manner to comply with requirements?
N
Safety
Y
Y
2.0 Sole IROFS?
Y
N
4.0 Can cumulative impact be met with available resources?
N
Add resources or Go to Step 6.0
Go to Step 1.0
2.1 Consequence of concern prevented by remaining IROFS?
Y
Y
Y
N
5.0 Asset screens out – no cyber security controls required.
5.1 Maintain
5.2 Any modifications?
2.2 Consequence of concern prevented by uncredited alternate controls?
Y
N
N
6.0 Address cyber security controls.

Note: Detailed guidance for this diagram is in the early stages of development.

Appendix A – Application of Cyber Controls

Application of cyber controls

Use guidance based on consensus standard approach (NRC provided risk assessment based on facility type and 3S function)

Factors to consider when evaluating cyber controls:

- Utilize existing controls and program elements (e.g., training, configuration management program, physical security controls);
- Justify not applying certain controls;
- Apply certain controls to the entire network rather than individual digital assets on a network; and
- Use templates for similar digital assets (i.e., tailoring; guidance in NEI 13-10).