UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

July 12, 2019

MEMORANDUM TO: Shana Helton, Director
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

THRU: Anthony Bowers, Chief
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

FROM: Brad Bergemann, Cyber Assessment Team Lead **/RA/**
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

SUBJECT: POWER REACTOR CYBER SECURITY PROGRAM ASSESSMENT

This memorandum provides a publicly available Executive Summary of the Power Reactor Cyber Security Program Assessment conducted between January and May 2019. Additionally, there is an enclosure, "Assessment Sections" containing detailed licensee-specific assessment feedback that is not publicly available.

BACKGROUND:

In March 2009, the Nuclear Regulatory Commission (NRC) published Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of digital computer and communication systems and networks," also known as the cyber security rule. The newly issued cyber security rule required operating nuclear power reactor licensees and license applicants to submit a cyber security plan (CSP) that describes how licensees will implement security measures to protect digital computers, communication systems, and networks associated with safety-related, security, and emergency preparedness (SSEP) functions. Additionally, licensees and license applicants were required to submit a schedule to address full implementation of the (CSP). Recognizing that it would require a significant amount of effort to implement the new cyber security rule, licensees and the NRC agreed to a phased implementation of their cyber security programs as identified below:

- Interim implementation (referred to as Milestones 1-7) completed no later than December 2012; and

CONTACT: Brad Bergemann, NSIR/DPCP
(301) 287- 3797

- Full Implementation (referred to as Milestone 8) initially to be completed no later than 2014. However, most licensees were granted license amendments to change their full implementation date to no later than December 2017.

Interim implementation of the CSP established a foundation for the full implementation of the cyber security program. The phased approach allowed licensees to focus their efforts on protecting their most risk-significant digital assets (DAs) from immediate cyber threats while working towards full implementation of their cyber security programs.

As the NRC performed interim implementation inspections and licensees began working towards full implementation, the NRC and licensees observed that the quantity of DAs identified as critical[1] (critical digital assets (CDAs)) far exceeded the estimates developed at the time the cyber security rule was finalized.

In June 2014, the Nuclear Energy Institute (NEI) submitted a petition for rulemaking (PRM)-73-18, "Petition to amend 10 CFR 73.54, 'Protection of digital computer and communication systems and networks'" to bound the scope of the cyber security rule. The petition recommended that the scope of the cyber security rule be reduced to focus only on protecting digital computers, communication systems, and networks associated with Structures, Systems and Components (SSCs) that are necessary to prevent significant core damage and spent fuel sabotage or whose failure would cause a reactor scram.

In September 2017, the NRC staff informed the NEI that an assessment of the power reactor cyber security program would be conducted once the NRC completed one-third of the full implementation inspections. In addition, the NRC would use the feedback collected from the assessment to help inform the Petition Review Board recommendation on PRM-73-18.

In January 2019, the NRC initiated the assessment to collect feedback and lessons learned from stakeholders regarding the cyber security rule, associated guidance, licensee implementation, and NRC inspections (interim and full implementation). The feedback and lessons learned would be used to identify recommendations on approaches to improving the efficiency and effectiveness of the power reactor cyber security program. These recommendations could lead to follow-on actions such as rulemaking, new guidance development or guidance clarification, or other program changes.

ASSESSMENT PROCESS:

The assessment process involved engagements with representatives from a wide variety of nuclear power reactor licensees totaling approximately 44 sites. In addition, two public meetings and a closed meeting were conducted to discuss and collect feedback from stakeholders as well as engagements with the Federal Energy Regulatory Commission (FERC), NRC headquarters cyber security staff, and regional cyber security inspectors.

The feedback process utilized the development of stakeholder questionnaires regarding the cyber security program to include the cyber security rule, associated guidance, licensee implementation, and NRC inspections. The questions were provided to stakeholders in advance to develop responses and follow-on engagements were conducted to discuss their

[1] In accordance with Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" DAs identified as CDAs require protection against cyber attacks.

responses as well as elicit additional feedback and lessons learned. The questions varied slightly depending on the type of stakeholder engaged (NRC licensee versus NRC staff).

FEEDBACK SUMMARY:

Based on feedback collected from the assessment, the main area identified for improvement is the scoping of CDAs. Currently, the CDA scoping criteria and NRC regional cyber security inspections are focused on protecting CDAs from adverse impact[2]. Specifically, licensees stated that many of the CDAs being protected by their programs, if compromised by a cyber attack, would not result in radiological sabotage and would not pose a risk to public health and safety. However, based on the following factors many DAs were conservatively scoped by licensees as CDAs:

- Rule and guidance interpretations;
- Interim implementation inspections causing additional conservatism due to inspection results; and
- Broad definitions and terms (adverse impact, important-to-safety).

Additionally, licensees stated that the resulting high numbers of CDAs had a cascading effect on other areas of the cyber security program (i.e., review, application and documentation of security controls for each CDA) as well as other licensee programs (e.g., substantial increase in the critical group population required for unescorted access to CDAs).

Other common areas identified for improvement based on feedback collected from stakeholders includes:

- Adopting a more risk-informed, graded approach to the CDA scoping process as well as the protection of these CDAs;
- Providing an acceptable method to screen security controls versus address or justify security controls that are not needed or applicable based on certain factors (e.g., CDA system capability and complexity), and to reduce the amount of documentation;
- Providing additional criteria for alternate security controls and allow for the crediting of alternate means to maintain SSEP functions;
- Providing more credit for existing plant programs (i.e., Insider Mitigation, Physical Security, Configuration Management) and resolving discrepancies that may exist between physical and cyber security;
- Utilizing updated security controls and appropriate control sets for the technology being assessed (e.g., information technology and operational technology);
- Providing clarification for DAs that are important to the cyber security program but are not categorized as CDAs:
    - Portable media and mobile device (PMMD) program assets;
    - Calibration equipment; and

[2] Adverse impact: A direct deleterious effect on a CDA (e.g., loss or impairment of function, reduction in reliability, reduction in ability to detect, delay, assess or respond to malevolent activities, reduction of ability to call for or communicate with offsite assistance, and the reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). In the case where the direct or indirect compromise of a support system causes a safety, important-to-safety, security or emergency preparedness system or support system to actuate or “fail safe” and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds), this is not considered to be an adverse impact as it defined by 10 CFR 73.54(a).

  - Cyber security tools such as Security Information Event Managers, Intrusion Detection Systems and Password Managers.
- Updating the NRC policy to align with current North American Electric Reliability Corporation Critical Infrastructure Protection standards to address scoping of Balance of Plant (BOP) DAs; and
- Transforming the future cyber security inspection program with the use of key performance indicators to assess licensee cyber security program performance. Additionally, consider the observation of exercises involving cyber attacks and evaluate the performance of the licensees Cyber Security Incident Response capabilities consistent with existing programs (i.e., physical security and emergency preparedness).

NEXT STEPS:

Based on feedback collected from the assessment, the staff will develop an action plan to facilitate and prioritize recommended cyber security program changes. The staff recognizes that proposed program changes may affect multiple guidance documents and will take appropriate action to ensure that any changes made to these documents, or in the development of new guidance, are not in conflict with each other or the cyber security rule. Cyber security program guidance documents include:

- NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors;”
- NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule;”
- NEI 13-10, “Cyber Security Control Assessments;” and
- Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities.”

The NRC’s cyber security program with enhancements will remain flexible and adaptable to meet the continuously changing threat landscape and actively defend against high confidence targeted cyber attacks. The goal being to ensure SSEP functionality remains protected and to provide for public health and safety, and common defense and security.

DISCUSSION:

The feedback collected from the assessment was categorized based on areas identified for improvement and then prioritized based on significance. Each category provides specific details collected from the feedback that can be used to assist in the evaluation of improvements to the cyber security program. However, several categories overlap each other such that improvements within one area may also impact others. For example, revising the definition of ‘adverse impact’ would also impact the category ‘CDA scoping.’ The prioritized categories are:

1. CDA scoping;
2. Definitions and terms;
3. Existing plant programs;
4. Security controls;
5. Inspections;
6. Non-CDAs;
7. Critical group; and
8. FERC and BOP CDAs.

Enclosure:
Assessment Sections

POWER REACTOR CYBER SECURITY PROGRAM ASSESSMENT; DATED: JULY 12, 2019

DISTRIBUTION:
PUBLIC

ADAMS Accession No.: ML19175A210 *** (concurred via e-mail)**

OFC	DPCP/CSB	DPCP/CSB	DPCP/CSB
NAME	BBergemann	JBeardsley*	ABowers*
DATE	6/27/19	7/11/19	7/12/19

OFFICIAL RECORD COPY