# U.S. CYBER SECURITY EXPERIENCES

James Beardsley
Division of Physical and Cyber Security
NRC Office of Nuclear Security and Incident Response
Rockville, United States

**Abstract # 383**

The increasing advancement of digital technology and the large amount of digital equipment in nuclear power plants have created new cyber threats to the nuclear power industry. In the U.S., nuclear power plants have implemented measures to address ever increasing cyber threats since the September 11, 2001 terrorist attacks. The NRC published a cyber security rule for power reactor licensees (10 CFR 73.54) in 2009.

The power reactor licensees implemented the cyber security rule at their facilities (cyber security program) in two steps. The first step had seven milestones, referred to as “interim milestones”. The licensees implemented security measures that would address significant threat vectors so that nuclear power plants were protected. The licensees completed the implementation of these security measures by 2012. The NRC inspected licensees’ implementation of the interim milestones between 2013 and 2015. The second step involves full implementation of the cyber security program. In general, licensees fully implemented the cyber security program at their facilities by 2017. The NRC began inspecting licensees’ full implementation program in July 2017 and this inspection is scheduled to be completed in 2020. The NRC performs a two-week onsite inspection. As of December 2018, the NRC completed the inspections of 20 sites.

The NRC has gained valuable insights on implementing cyber security programs at commercial nuclear power plants in the United States. This paper provides an overview of the challenges faced in implementing a cyber security oversight program for nuclear power plants, as well as the lessons learned from its implementation. In addition, this paper will also discuss those controls that are effective in minimizing the cyber attack surfaces for the commercial nuclear power plants in the U.S.

## 1. INTRODUCTION

The NRC has gained valuable insights in the ten years since the NRC established the cyber security rule for commercial nuclear power plants in the United States. This paper provides an overview of the operating experience and lessons learned from implementation of cyber security oversight at U.S. commercial nuclear power plants.

The cyber security threat environment continues to be very dynamic, which presents a number of challenges to the US nuclear power licensees. Over the course of the cyber security program inspections, the industry and NRC have developed considerable operating experience and a greater understanding of cyber security protections. As a result, the NRC is focusing efforts to improve the guidance for program implementation and oversight. This transformative process will continue to leverage risk insights while ensuring that industry digital assets are adequately protected.

## 2. 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. This 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.

In 2010, the NRC published Regulatory Guide (RG) 5.71 “Cyber Security Programs for Nuclear Facilities.” The RG identified a structure for program implementation and a construct for digital asset protection based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, “Recommended Security Controls for Federal Information Systems.” The RG included a template for a licensee to use in development of their cyber security plans. The RG introduced the concept of a layered approach to digital asset protection and the use of a one-way deterministic device to protect SSEP CDAs. The RG also identified the basic elements required to implement cyber security program. Those elements included the following steps:

- Establish a multi-disciplinary team to assess the program requirements and identify the digital assets that should be protected.
- Evaluate all digital assets and identify those systems and assets that should be protected, critical systems (CSs) and critical digital assets (CDAs).
- Implement a defensive architecture
- Apply security controls to the identified CDAs

Following the release of RG 5.71, industry developed NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” to provide additional guidance on cyber security program implementation and a slightly modified template for the licensee’s CSP. All operating power reactors licensees adopted the NEI 08-09 template for their CSP. By the end of 2010, all the operating reactor licensees submitted their CSPs to the NRC and had them approved as license conditions.

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:

- Interim implementation (referred to as Milestones 1-7); completed in December 2012; and
- Full Implementation (referred to as Milestone 8); completed by most licensees 2017.

The interim implementation of the cyber security program established a foundation for the full implementation of the cyber security program. The phased approach allowed licensees to first focus their efforts on protecting their most significant digital assets (DAs) from immediate cyber threats while continuing development of their cyber security program full implementation.

As the licensee’s fully implemented their cyber programs, they identified a large number of CDAs, and that some might not need to have the full suite of cyber controls required by their CSPs. As a result, industry developed NEI 13-10 “Cyber Security Control Assessments,” which the NRC approved for use, to provide a risk-informed approach the assessment CDAs. NEI 13-10 provided a methodology for the licensees to evaluate the significance of a CDA. For those with a lower significance, the process identified a lesser set of controls required to secure the assets. As a result, a majority of the CDAs were classified as “indirect” and only required to have about 10% of the controls that a safety or security CDA was required to have implemented. This effort simplified the licensee’s cyber program implementation and facilitated their ability to focus on the more risk-significant CDAs.

Recognizing that there were significant differences between interim implementation and full implementation, the NRC and industry conducted a series of table top exercises in 2016 and early 2017 to evaluate areas of the full implementation that could present challenges for industry and the inspectors. As a result of that effort, industry developed additional program implementation guidance, approved for use by the NRC, to assist the licensee implementation and preparation for the upcoming inspections.

## 3. DISCUSSION

### 3.1 Inspection Program

To date the NRC has completed 70% of the full implementation inspections and plans to be 100% complete by the end of 2020. In mid 2017, the NRC started to inspect industry’s full cyber security implementation. The initial phase included two inspections in mid 2017. Following those inspections, the NRC and industry suspended inspections to evaluate lessons learned and ensure that the program implementation guidance and inspection processes were effective.

Over the course of the inspection program, NRC incorporated lessons from the early inspections to improve the efficiency and effectiveness of the inspection process. The most notable of the improvements was the development of guidance for the inspection request for information (RFI) process. During early inspections, the NRC and licensees experienced delays during the initial phases of the inspection because of poor communication. When the NRC requested licensee cyber security program material for inspection preparation and conduct, the licensees either did not fully understand the information being requested or did not have the information in a format that facilitated smooth inspections. As a result, the NRC engaged industry to clarify the type and format of information requested for inspection conduct.

An NRC-industry team developed a structured RFI process to address the issue. The process documented a phased approach for RFIs that allowed the inspectors and licensees to focus their efforts on specific information related to the inspections. The initial RFI (14 weeks prior to the inspection) included high level programmatic information and lists of CDAs. That information was used to select the specific CDA inspection sample and thus the second RFI (closer to the inspection date) was focused on the inspection samples. A third RFI was identified as well. This request made up the documents that the inspection team requested to be available once they arrived on site for the actual inspection. In addition to the phased RFI process, the RFI guidance also clarified the terminology that the requests would use to ensure that the inspectors and licensees were clear. This process has been successfully implemented and is considered a key element on the smooth implementation of the cyber security inspection process.

Over the course of the full implementation inspections, NRC and industry have compiled insights from lessons learned related to the licensee's cyber security full implementation and the conduct of the cyber oversight program. As a result, industry operating experience and, in some cases, new industry guidance have been developed to share the lessons and improve program effectiveness. Some of the areas identified for improvement over the first two years of the program include the following:

- The quality of CDA and CS assessments.
  - NRC inspectors noted challenges with the quality and fidelity of the licensee's CDA and CS assessments. This issue led to delays during inspection conduct because the licensees were challenged to explain their methodology for analyzing and protecting their CDAs and CSs. In many cases the assessments were either incomplete or lacked the fidelity to support the licensee's cyber security protections. As a result, licensees had to perform further research and develop new inspection artifacts to support the inspection process.
  - As NRC's inspections progressed through 2018 and into 2019, industry operating experienced helped licensees identify issues with their assessments prior to their inspections. The challenge of adequate CDA and CS assessments was identified as a programmatic challenge during the 2019 Cyber Security Program Assessment and is included in the post assessment improvements discussed later in this paper.
- Guidance on portable media & mobile device program
  - NRC's inspection program identified a number of issues with the licensee implementation of their portable media programs. In particular, the NRC noted that the controls implemented to secure the media scanning stations or kiosks may not be sufficient to ensure that the stations will perform their intended function.
  - After considerable discussion on the issue, industry developed a guidance document for the configuration of portable media transfer stations. At a public meeting conducted on March 7, 2019, (Agencywide Documents Access and Management System (ADAMS) Accession Number ML19175A210). ADAMS ML19093B029 reference to meeting summary, the NRC provided some comments on the document and stated that they would accept the guidance with the comments incorporated. Following that meeting, most of industry has implemented the recommended configuration changes.
- Guidance on periodicity for ongoing monitoring & assessment modifications.
  - The licensee's CSPs include a number of requirements that must be completed or changed at specified periodicities. As licensees implemented their cyber programs, they identified that many of the requirements were difficult to meet due to operational challenges. As a result, licensees proposed alternate implementations and each inspection team was forced to adjudicate the proposals.
  - To simplify the process for implementing alternate periodicities, industry and the NRC developed a matrix of the periodicities in the licensee's CSPs and identified an acceptable set of alternate approaches.
- Guidance on vulnerability management

- The licensee's CSP requires that they assess CDA vulnerabilities for all CDAs. The requirements assess CDAs vulnerabilities past and present, a potentially large number. During inspections the NRC staff noted that licensees were struggling to conduct adequate assessments.
- In order to address the large backlog of vulnerability assessments, the NRC and industry developed guidance on vulnerability prioritization. The guidance has been implemented throughout most of industry and has helped industry address their vulnerability assessment backlog.

## 3.2 Cyber Assessment and Follow-on Activities

In January 2019, the NRC initiated an assessment of the cyber oversight program 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 informed recommendations on approaches to improving the efficiency and effectiveness of the power reactor cyber security program. In July 2019, the NRC finalized the Cyber Assessment report (ADAMS Accession Number ML19175A210).

In August 2019, NRC staff was tasked to develop a Cyber Assessment Action Plan to consolidate and prioritizes short-term and long-term improvements to the power reactor cyber security program, (ADAMS Accession Number ML19175A210). The goal of the action plan was to identify enhancements to the cyber security program that promote regulatory efficiency and effectiveness, while continuing to provide for reasonable assurance of public health and safety and promote common defense and security. These recommendations have led to follow-on actions such guidance development or clarification, or other program changes.

In October 2019, the NRC completed Version 1.0 of the Cyber Assessment Action Plan. The plan documented the history of the cyber security program, the key issues identified in the 2019 cyber program assessment and other factors impacting the cyber security program's future. The plan identified five primary areas of effort for program improvement. Those areas are listed below. Each of the areas is documented in an addendum to the action plan including an implementation schedule. The addendums are maintained by the NRC as living documents, used to track progress for each effort.

## 3.3 Action Plan Elements

### *3.1.1 Program Definitions & Terms*

The glossaries industry and NRC cyber security guidance documents are inconsistent on the definitions of some terms. The NRC will monitor development of the guidance updates associated with the following action plan activities and ensure that definitions and terms are made consistent during their updates. The completion date for this activity is dependent on the update schedule for the guidance documents

### *3.1.2 Risk-Informing Critical Digital Asset Determination*

— Emergency Preparedness (EP): NRC staff and industry are evaluating the guidance related to CDA determination for EP digital assets. This effort is expected to be completed by February 2020.

— Balance of Plant (BoP): NRC staff and industry are working with staff from the Federal Energy Regulatory Commission (FERC) to evaluate the cyber security protections for nuclear power plants as compared to other power producing facilities. The effort includes the potential for updating guidance for BoP CDA determination. This effort is expected to be completed by May 2020.

— Security: NRC staff and industry are evaluating the guidance related to CDA determination for physical security digital assets. Industry may have been overly conservative evaluating security digital assets for inclusion in the cyber security program, and additional guidance may enhance that process. This effort is expected to be completed by June 2020.

— Safety-Related and Important-to-Safety: During the inspection program multiple issues associated with the classification of Safety-Related and Important-to-Safety digital assets. The effort will improve the guidance associated with that process. This effort is expected to be completed by May 2020.

### *3.1.3 Critical Digital Asset Assessment*

During the cyber security inspections, both industry and the NRC staff identified issues with the fidelity of the licensee's CDA assessments. The NRC staff and industry will work together to document the characteristics of a quality assessment. This effort is expected to be completed by March 2020.

### *3.1.4 Risk-Informing CDA Protection (Cyber Control Implementation)*

Each power reactor licensee committed to a cyber security plan that includes approximately 140 controls that have to be assessed and implemented to protect the CDAs. This effort would evaluate the security plan requirements at a generic level and potentially modify or delete requirements that are not necessary. This effort is expected to be completed by June 2020.

### *3.1.5 Cyber Inspection Oversight Program following Full Implementation*

The power reactor cyber security oversight program establishes a baseline for program implementation through the current, one-time, inspection procedure. The NRC intends to develop a revision to the inspection program that shifts focus from programmatic verification to a performance informed assessment of the licensee's cyber security program. The NRC is working with industry to evaluate the potential incorporating performance metrics into the inspection process. In addition, industry has proposed the implementation of a performance testing program to further inform the inspection process. This effort is expected to be completed by December 2020 to support implementation of the revised inspection procedure in 2021.

## 4. CONCLUSION

Over the past ten years the NRC and the industry have devoted considerable resources to establish the US power reactor cyber security program and ensure that licensees are adequately protected from the cyber threat. The program was fully implemented by most licensees and the implementation will be verified by NRC inspection by the end of 2020. Although the NRC staff has identified some issues with the industry implementation over the course of the inspection program, to date of all the findings have been of a very low safety significance.

The NRC staff conducted an assessment of the power reactor cyber security program in 2019. As a result of the assessment, the NRC staff and industry have identified areas that may be further risk-informed to increase the cyber security program's efficiency and effectiveness, and to ensure that licensee's cyber programs are focused on the areas that are most important for security. The majority of those efforts will be implemented through revised industry guidance. In conjunction with the program improvements, the NRC staff is developing a performance-informed inspection process to evaluate industry's continued cyber security implementation.