PR-73
80FR53478

5

PUBLIC SUBMISSION

As of: 10/9/15 3:04 PM
Received: October 05, 2015
Status: Pending_Post
Tracking No. 1jz-8lin-6m02
Comments Due: October 05, 2015
Submission Type: Web

Docket: NRC-2015-0179
Cyber Security at Fuel Facilities

Comment On: NRC-2015-0179-0001
Cyber Security at Fuel Cycle Facilities; Draft Regulatory Basis

Document: NRC-2015-0179-DRAFT-0003
Comment on FR Doc # 2015-22051

Submitter Information

Name: Rick Medina
Address: United States,
Email: ricardo.medina@urenco.com

General Comment

NRC-2015-0179
URENCO USA Comments

Attachments

10-5-15 UUSA Comments on Part 73 Draft Regulatory Basis Document

Annette L. Vietti-Cook
Secretary of the Commission
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001
ATTN: Rulemakings and Adjudications Staff

Subject: Comments from URENCO USA on NRC Rulemaking for Cyber Security at Fuel Cycle Facilities Draft Regulatory Basis Document; Proposed Rule" (RIN 3150–AJ64; Docket ID NRC–2015–0179)

On September 4, 2015, the Nuclear Regulatory Commission published a "Draft Regulatory Basis for Fuel Cycle Cyber Security" (accession number ML15198A021) proposed rule to amend its regulations in 10 C.F.R. Part 73 governing Cyber Security for Fuel Cycle Facilities (FCF). As directed by Federal Register Notice 7590-01-P (ML15198A024), UUSA hereby submits comments on the proposed amendments.

The NRC has released a proposed rulemaking regulatory draft basis document with regard to the Cyber Security posture of network and computer systems that are associated with Safety, Security (physical and information), Emergency Preparedness (to include offsite communications), and Material Control and Accountability (SSEPMCA) functions. To UUSA this would have an impact on the way the business performs and applies security control mechanisms to various systems, specifically, the proposed rule would affect: systems utilized by Emergency Preparedness (EP) (both contracted and UUSA operated) in their operations center and at the training center in Eunice; SAP which is utilized for Material Control and Accountability; the security and access control systems; fire detection systems; and criticality alert systems. Some of these systems, specifically SAP and those utilized by EP, are a part of UUSA's privately owned business network. As such, the aforementioned systems would require the development of an Information Security Plan to be reviewed and approved by the Nuclear Regulatory Commission (NRC).

Background

In 2002 the Government passed what is known as the E-Government act. Title III of the law contains provisions known as the Federal Information Security Management Act (FISMA). The purpose of this law was to address and standardize the way in which the Federal Government agencies protect *information* within *Federal* information processing systems. FISMA directed all Government agencies to apply the framework provided by the National Institute of Standards and Technology (NIST) in the development and implementation of their networks and computer information systems. This was to allow for a standardized process, thus enabling efficiency and cost savings by allowing systems developed by one agency to easily be adopted and implemented by other agencies without having to re-accomplish the entire process from the start. The result however has been questioned by many throughout the security community. Security experts from the SANS Institute have described FISMA as simply replacing one paperwork drill for another and have criticized that the framework measures security planning and not actual information security. A former Government Accountability Office (GAO) chief

technologist, Keith Rhodes has cautioned that "implementation is everything. If security people view FISMA as just a checklist, nothing is going to get done."

Comments on Chapter 1

The Draft Regulatory Basis Document proposes to codify, in regulatory actions that must be taken to protect against Cyber Security threats. Please note that the systems in question (SSEPMCA systems) are privately owned (UUSA) and not a government organization, and as such, they are not Federal Information Systems. 800 series documents produced by NIST state the following in the "Authority" section in the beginning of the document directly after the title page:

> "This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST".

Within Chapter 1 the NRC defines a cyber-attack with a very broad definition:

> "the manifestation of physical, electronic, or digital threats against computers, communication systems, or networks that may: (1) originate from either inside or outside the licensee's facility, (2) utilize internal and/or external components, (3) involve physical, electronic, or digital threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to digital assets or systems."

This broad definition is not conducive to the protection of information or the system on which information is contained. We understand that this definition is consistent with Regulatory Guide 5.71 developed for power reactors; but with the lessons learned discussed in the NRC Public Meeting on September 23, 2015 and as stated in Section 3.3 of the draft regulatory basis document, this guidance is not appropriate to address the unique programs' associated risks specific to Fuel Cycle Facility licensees. Ultimately, this definition is the foundation of this proposed rule. Utilizing the definition above, one could come to the conclusion that an individual who simply turned the computer off at the end of the day, preventing it from receiving updates, is guilty of a cyber attack. Another example is an employee who watches an instructional video as part of training and the result is a degradation of network resources and bandwidth.

While certainly there are events which occur within network systems that may have a negative effect, not all events are attacks. An attack is targeted or directed in nature and is generally related to offensive nature and malicious intent. UUSA recommends this definition be revised to reflect the actual defined threat that the NRC intends to defend against and not encompass events that could possibly occur on a computer system.

Comments on Chapter 2

The draft rulemaking document suggests the implementation of controls provided by NIST Special Publication (SP) 800-53, Rev 4, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-53 Rev 4 is simply a catalog of controls

that can be applied to information systems. This document does not provide a holistic approach to the implementation of a process in which to apply those controls, nor does it define any roles, responsibilities, or expectations. The document that lays the actual framework for the implementation of the security controls is NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and NIST 800-39, *Managing Information Security Risk*

The problem with the approach of the draft regulatory basis document is that it points to NIST SP 800-53 Rev 4 but it does not provide a framework or process for its implementation. Within NIST 800-53 there are over 1600 individual points (when all controls, and control enhancements are thoroughly addressed) of interest that could be addressed within a Systems Security Plan. IT security is a process, not simply the application of controls and a documentation effort. There are roles and responsibilities that prevent conflicts of interest and establish the formal acceptance of risk. The systems the NRC is wanting to regulate with this proposal are business systems. This means that the Government is not the Authorizing Official as defined within the NIST Risk Management Framework. The operation of these systems is a business risk accepted and authorized by UUSA management.

The risk based decision to operate an IT system and the supporting processes is subjective; it is related to multiple factors ranging from risk appetite to financial considerations. We recommend having an objective basis in order to avoid differences in opinion on the subjective decision making factors currently written in the draft.

Comments on Chapter 3

The risk based approach to the application of security controls intends to address three areas of concern, known in the community as the security triad. These areas of concern are Confidentiality, Integrity, and Availability. Confidentiality concerns itself with the inability of data to be intercepted and read by unauthorized individuals. Integrity refers to the accuracy of data being interpreted by the user and ensuring that data is not modified in an unauthorized and potentially malicious manner. Availability is the system's ability to withstand attack or other service interruptions by incorporating failsafe, redundant design. With these three pillars of protection in mind it is can be said that the goal of a successful IT security program is providing the right data, to the right people, at the right time. Each of these areas of concern (Confidentiality, Integrity, Availability) is rated as either a High, Moderate, or Low level of concern. This final rating dictates the amount of controls that are recommended as applicable from NIST 800-53.

Chapter 3 of the draft document aims to address each of the SSEPMCA yet fails to adequately describe the level of concern for each system supporting it's respective SSEPMCA function. Most all functions contained in the sections of this chapter utilize general statements like the following:

> "If a compromise of one of these digital assets due to cyber-attack were to go undetected and unresolved, the digital asset could fail to perform its intended function."

This language implies that confidentiality and integrity is not a high level of concern and the focus seems to be on availability.

Considering that our classified systems have been rated at "Moderate, Low, Low" levels of concern for "Confidentiality, Integrity, and Availability" respectively, NIST 800-39, *Managing Information Security Risk,* recommends that a Risk Assessment be performed. This would also fall in compliance with NIST 800-30, *Guide for Conducting Risk Assessments.* This would provide an accurate categorization of the systems in question.

Comments on Chapter 4

Cyber vulnerabilities have not been established in this draft Regulatory Basis Document. The NRC has not shown in the draft nor in other documents that the industry has a problem. In fact, many of the systems identified have been scrutinized by the NRC and DOE, and to date no issue has been identified. Therefore, it is unclear as to why the NRC would regulate a business network that seems to be outside of the regulatory purview.

It is conventional for licensees to assume the risk for Confidentiality, Integrity, and Availability (NIST 800-53). The NIST standard leaves an interpretation that the NRC is going to assume the risk for areas which are part of a government business process. It seems as though the intention is not applicable for private business processes that has no impact on safety or security. This is strictly a business and primarily financial risk.

Comments on Chapter 8

Cost considerations for the proposed rulemaking as currently written, could be very broad due to the fact that many of the considerations would include the additional head count to security organizations from IT Security people to a IT Network Administrator. The man hours associated with a system that is NIST 800-53 compliant has a lot of parts that have to be verified on a regular basis. (Logs, Access, scanning of software and monitoring of systems). The cost of maintenance of the systems could also go up due to strict configuration management processes that would have to be in place to ensure compliance with NIST standards.

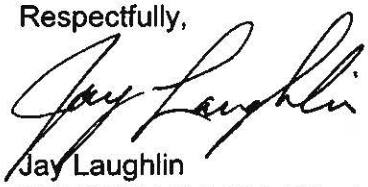
Summary

The Draft Regulatory Basis Document, Rulemaking for Cyber Security at Fuel Cycle Facilities, seems to be very broad and it does not seem appropriate for all fuel cycle facilities. The implementation of the risk based approach to fuel cycle facilities (NIST 800-53) would have a greater impact on the business systems than safety and security systems due to the majority of the licensees geographically not being in the same location. What has not been established is the basis for which the NRC will be regulating business related networks or systems that have no impact on safety or security. The implementation of a risk based approach involves a great deal with NRC providing threat and vulnerability information and how this will be established for each licensee. There still is a question to the fact that NRC has not provided information to an actual threat to these systems and how they relate to the safety of a plant and community.

With a risk based approach provided by NIST, which seems to be focused on continuous improvement and monitoring; how does the NRC intend to fit the Risk Management Framework into a performance based model of regulation? Performance based contract models generally employ the tracking of implementation times and percentages of completion in order to produce quantifiable data in which to grade performance. It is unclear whether the NRC intends to provide clear set of standards in order to better identify which assets within a network centric environment are not owned or operated by the Government.

UUSA appreciates the efforts of the NRC and the opportunity to comment on this important rulemaking. If you have any questions on these comments, please contact Amy Johnson, Licensing and Performance Assessment Manager, at 575-394-6203 or Amy.Johnson@URENCO.com.

Respectfully,



Jay Laughlin
URENCO USA Chief Nuclear Officer and Head of Operations