Regulatory Efforts to Improve Cyber Security

James Wiggins, C. Erlanger, T. Harris

U.S. Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response
Washington D.C., United States

Abstract. The cyber threat has significantly increased over the last decade and continues to evolve. Improving the cyber security at nuclear facilities is critical in today's environment. The United States Nuclear Regulatory Commission is implementing a number of efforts in rulemaking, licensing and inspection to address and improve cyber security at regulated facilities. The United States Nuclear Regulatory Commission has been working multilaterally with the IAEA and bilaterally with our international partners to promote improvements in cyber security.

1. Introduction

The United States Nuclear Regulatory Commission (USNRC) is an independent regulatory agency created to enable the United States to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. The USNRC regulates commercial nuclear power plants and other uses of radioactive materials, such as in nuclear medicine and industrial practices, through rules, licensing, inspection and enforcement of these requirements. Over the last ten years, the USNRC has taken measurable steps through rulemaking, licensing and inspection to address and improve cyber security at USNRC regulated facilities. In addition, the USNRC interfaces with other federal and state agencies, such as the Department of Homeland Security, Federal Energy Regulatory Commission, National Institute of Standards and Technology (NIST), the Intelligence and Law Enforcement Communities, and other agencies on cyber security issues. The USNRC has also been working multilaterally with the IAEA and bilaterally with our international partners to promote improvements in cyber security.

2. Context

There are an increasing number of state and non-state malicious actors using cyber tools and techniques as part of their ongoing efforts to gather information as well as conduct criminal, espionage or terrorist related-activities. Such activities are increasingly targeting government networks, critical infrastructure and key resources of industries and facilities throughout the world. Cyber threat actors are wide ranging and include criminals and organized crime groups, hacktivists, terrorists and violent extremists as well as nation-states. Each of these cyber threat actors may have differing motivations for conducting cyber attacks ranging from identity theft to extortion; acts of civil disobedience to service disruption and physical damage to a machine; as well as technology transfer and information gathering.

Although the global cyber threat has been present for many years, the fact that operating nuclear power plants in the United States have predominately used analog industrial control systems makes these facilities more resistant to the cyber threat. However, with current USNRC licensees upgrading their systems to digital industrial control systems, as well as new nuclear power plant's being licensed that use primarily digital industrial control systems, it is imperative that the USNRC and its licensees are aware of this threat and take appropriate actions to mitigate cyber threats. Cyber attacks can adversely impact digital equipment and information systems that are associated with safety, security, or emergency preparedness

functions and can affect a nuclear power plant's ability to operate safely or effectively respond to events.

3. Regulatory Framework

The USNRC mission is to protect the public health and safety and promote America's common defense and security. We have two primary goals:

- Safety Goal: Ensure adequate protection of public health and safety and the environment, and
- Security Goal (including safeguards): Ensure adequate protection in the secure use and management of nuclear and radioactive materials.

Safety has always been a primary pillar of USNRC's regulatory programs. In the current threat environment, there has been a renewed focus on security including cyber security, and the USNRC has been proactive in requiring our licensees to protect against the cyber threat using a risk informed approach. Our regulatory framework is comprised of regulations, licensing activities, and oversight, which includes inspection and enforcement. Licensees develop security plans based on the regulations and implement a physical protection program which includes cyber security. USNRC inspects the licensee's facilities to verify compliance with our regulations and takes enforcement actions for non-compliance. We have taken measurable steps to improve cyber security in each of these areas.

4. Cyber Security Regulation and Licensing

The terrorist attacks on September 11, 2001, reaffirmed the need for collective vigilance, enhanced security, and improved emergency preparedness and incident response capabilities across the Nation's critical infrastructure. As a result, the USNRC conducted thorough evaluations of the Commission's security programs in a risk informed manner and took prompt actions to enhanced security at regulated facilities. The USNRC issued Orders containing enhanced security requirements between 2001 and 2003, which included a cyber security component for nuclear power plants and other high risk facilities. Acknowledging the cyber threat but not fully appreciating specific vulnerabilities at nuclear power plants, the cyber security requirements in these orders were general in nature. With this in mind and recognizing that rulemaking to codify the enhanced security requirements would take time, the USNRC published NUREG/CR-6847, "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants" [1] in October 2004. The USNRC also worked with industry to assess cyber risk at nuclear power plants; and in 2005, the USNRC endorsed the Nuclear Energy Institutes' NEI 04-04, "Cyber Security Program for Operating Reactors" [2].

USNRC's regulations are codified in the Code of Federal Regulation. USNRC security regulations are predominately performance based, that is they describe the outcome or what should be achieved, not necessarily how to accomplish the outcome. As part of the rulemaking process, proposed rules are published for stakeholder comments. The stakeholder comments and the draft final rule language are reviewed and approved by the Commission.

In 2006, USNRC published a proposed rule to amend the physical security of nuclear power plants in 10 CFR Part 73, "Physical Protection of Plants and Materials," [3]. The proposed rule included cyber security requirements as a subsection within the nuclear power plant physical security requirements. In 2009, the USNRC issued the final rule which included a specific section for cyber security, 10 CFR 73.54, "Protection of Digital Computer and

Communication Systems and Networks" [4]. Having a new stand-alone section rather than a subsection placed greater emphasis on the importance of cyber security and enabled cyber security requirements to be made applicable to other types of facilities and applications through future rulemakings. These new program based and performance based cyber security requirements are designed to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks up to and including the design basis threat as established by 10 CFR Section 73.1(a)(1)(v). These new cyber security requirements are a substantial improvement to the general requirements imposed by Orders.

As defined in the regulations, the cyber security program is a component of and is integrated into the overall physical security program. The cyber security regulation requires operating power reactor licensees and combined license applicants for new reactors to implement a cyber security program that provides high assurance that safety, important to safety, security, and emergency preparedness functions are protected from cyber attacks. The cyber security regulations were intentionally developed to be performance based to provide licensees flexibility to best determine how to protect critical digital assets and critical systems from cyber attacks. This performance based approach also accommodates advances in technology and changes to cyber threats and threat vectors without the need to change the regulations through rulemaking.

The cyber security regulations require the submission of a cyber security plan and implementation schedule to USNRC for review and approval. The cyber security plan describes how licensees will maintain the capability for timely detection and response to cyber attacks, mitigate the consequences of cyber attacks, correct exploited vulnerabilities and restore affected systems, networks and/or equipment affected by cyber attacks.

The USNRC issued guidance on an acceptable approach to meeting the regulation in Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" [5]. While the cyber security regulation is performance based, the Regulatory Guide is comprehensive and provides details on developing a robust cyber security program. An effective cyber security program cannot be static and must be maintained through continuous monitoring, program review, change control, and records retention. Because the cyber security program involves consideration of many plant programs and organizations, the cyber security assessment team, which manages and oversees the cyber security program, is composed of individuals with broad knowledge in the areas of information and digital systems technology; nuclear facility operations, engineering and safety; and plant security and emergency preparedness. The basic requirements of the cyber security program include:

- Identifying digital assets that must be protected (i.e., critical digital assets)
- Maintaining Defense-In-Depth protective strategies to ensure the capability to detect, respond to and recover from cyber attacks
- Applying of security controls to protected digital assets
- Mitigating the adverse affects of cyber attacks
- Ensuring functions of protected digital assets are not adversely impacted due to cyber attacks
- Training appropriate facility personnel on cyber security requirements
- Managing cyber risks
- Evaluating modifications to digital assets to ensure cyber security is maintained

Regulatory Guide 5.71 provides a template for a generic cyber security plan which licensees and applicants may use to comply with the licensing requirements of the cyber security

regulations. Regulatory Guide 5.71 also includes a suite of technical, operational and management security controls, which are to be assessed and implemented, as appropriate, for each critical digital asset. The assessment process allows for alternative countermeasures that provide the same or greater protections as the corresponding security control to be used to address specific attack vectors or vulnerabilities when a security control cannot be applied. One or more security controls may not need to be applied if an attack vector does not exist or is not applicable, or if implementing the security control would adversely impact safety, important to safety, security or emergency preparedness functions. Licensees perform effectiveness analyses and vulnerability assessments to verify that the cyber security program provides high assurance that critical digital assets are protected from cyber attacks and has closed any identified gaps. The security controls listed in Regulatory Guide 5.71 Appendices B and C were tailored to the unique nuclear power plant environment using the high baseline security controls in NIST 800-53, Rev. 3, "Recommended Security Controls for Federal Information Systems" [6] and NIST 800-82, "Guide to Industrial Control Systems Security" [7].

The cyber security plans required by the cyber security regulation were submitted for USNRC review and approval by November 23, 2009. The USNRC reviewed and approved all operating power reactor licensees' cyber security plans, and those plans were incorporated into each plant's licensing basis via license amendments.

In addition to submitting their cyber security plan, operating power reactor licensees were also required to submit a proposed implementation schedule for their cyber security programs. As a result of the amount of work and significant lead time required to fully implement all the provisions called for in their USNRC-approved cyber security plans, interim milestones were identified that stressed the completion of a set of prioritized activities by December 31, 2012. For these interim milestones, emphasis was placed on key threat vectors, or areas of compromise, having the right people trained on cyber security, making sure the assets that require protection are identified, achieving isolation where possible, and putting security controls and best practices in place to render a high degree of protection from cyber-based attacks until full cyber security program implementation can be achieved. Specifically, the seven interim milestones included:

- Establish the Cyber Security Assessment Team
- Identify Critical Systems and Critical Digital Assets
- Install a deterministic one-way device between certain levels in their plant architecture
- Implementation of a specific security control related to portable and mobile devices
- Implementation of observation and identification of obvious cyber related tampering to existing insider mitigation rounds
- Application of security controls to critical digital assets associated with target set equipment
- Commence ongoing monitoring and assessment activities for those security controls that have been implemented

Implementation of Milestone 8 (i.e., full implementation of the regulation and cyber security program) is a site specific date for each nuclear power plant.

The USNRC has also addressed cyber security interface issues relative to power generation under its statutory authority (i.e., at nuclear power plants) and to electricity distribution (i.e. the power grid). In January 2008, the Federal Energy Regulatory Commission issued Order

No. 706 that specified Critical Infrastructure Protection (CIP) Reliability Standards to safeguard critical cyber assets. This order, which is implemented by the North American Electric Reliability Corporation, exempted facilities regulated by the NRC from these requirements. Both the USNRC and the Federal Energy Regulatory Commission recognized the need to ensure that there was no gap or overlap between the Order 706 and 10 CFR 73.54. The USNRC and the North American Electric Reliability Corporation have a Memorandum of Understanding that coordinates their responsibilities for applying cyber security requirements to nuclear power plants and their surrounding infrastructure. The USNRC also has a Memorandum of Agreement with the Federal Energy Regulatory Commission to facilitate a continuing and cooperative relationship and to exchange experience, information, and data related to the reliability of the U.S. bulk electricity supply.

5. Regulatory Oversight

In the nuclear power plant arena starting in 1999, USNRC revised its Reactor Oversight Process [8] to establish a risk-informed baseline inspection program and to set documented risk-informed thresholds for licensee safety and security performance, below which increased USNRC interaction would be warranted. USNRC also established a significance determination process for inspection findings and integrated those with Performance Indicators in a timely manner to support overall assessment of licensee performance.

The regulatory framework for reactor oversight consists of three key strategic performance areas: reactor safety, radiation safety, and safeguards. Within each strategic performance area are seven cornerstones that reflect the essential safety aspects of facility operation. These seven cornerstones include: initiating events, mitigating systems, barrier integrity, emergency preparedness, public radiation safety, occupational radiation safety, and security. Satisfactory licensee performance in the cornerstones provides reasonable assurance of safe facility operation and that the USNRC's safety and security missions are being accomplished. Each cornerstone contains inspection procedures and performance indicators to ensure that their objectives are being met.

As discussed above, the cyber security program is a component of and is integrated into the overall physical security program. As such, cyber security has been added as a component of the security cornerstone.

Within the existing Reactor Oversight Process, the USNRC developed an oversight program for cyber security that includes cyber security inspector training, a cyber security inspection program, and a process for evaluating the significance of cyber security inspection findings. The cyber security inspection program included developing temporary instructions to be used in inspections for both the interim milestones and the full implementation of licensees' cyber security programs. This was accomplished collaboratively with stakeholders, including NRC staff and regional inspectors, members of industry, and representatives from the Department of Homeland Security, the Federal Energy Regulatory Commission, and the National Institute of Standards and Technology.

Starting in January 2013, USNRC began inspecting licensee's implementation of milestones 1-7. These inspections will continue thru next year. As licensees reach their full implementation dates, NRC inspectors will begin inspecting the full cyber security program and compliance with 10 CFR 73.54. As with any new requirement, NRC inspections have identified findings as licensees are implementing milestones 1-7. These observations will be

used along with other lessons learned in assessing whether changes are required to USNRC's cyber security framework.

To evaluate cyber security incidents reported by licensees and to coordinate with other governmental agencies, the USNRC established a Cyber Assessment Team in 2009. The Cyber Assessment Team is comprised of technical staff from several USNRC Offices, including Regional Office representation, and is administered by the Office of Nuclear Security and Incident Response. The Cyber Assessment Team's primary roles include:

- Assess and provide analysis of cyber security related issues and events received from industry, stakeholders and other government agencies to identify technical issues that may warrant NRC action
- Provide technical support to the Information Assessment Team during its response to events that may have cyber security implications

6. Cyber Security Roadmap

The USNRC's risk informed regulatory approach incorporates an assessment of safety and security 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. As discussed above, the USNRC used a risk informed approach to determine the need and priority for enhanced security measures in the Orders issued in the early 2000's and is following this approach in determining which facilities and which digital assets may require additional protection. As a continuation of USNRC's consideration of cyber risk at regulated facilities, staff developed Commission paper, SECY-12-0088 dated June 25, 2012 [9]. In addition to providing the status of the USNRC's implementation of cyber security requirements for power reactor licensees and combined operating license applicants, the paper communicated the staff's approach, or "roadmap", for evaluating the need for cyber security requirements for the following four categories of the USNRC licensees and facilities: (1) fuel cycle facilities; (2) non-power reactors; (3) independent spent fuel storage installations; and (4) byproduct materials licensees. The process being used for these evaluations consists of 1) establishing a working group and assessment materials, 2) conducting targeted site visits, 3) conducting USNRC assessments or industry self assessments, 4) working group assesses the results of the assessments and 5) USNRC staff determines the next steps. The USNRC staff has begun assessments for each of the categories of licensees, starting with fuel cycle facilities (i.e., the category of facilities being the next risk significant following nuclear power plants).

The implementation of this roadmap will ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all USNRC licensed facilities and identify if any program improvements are needed. Recent high-profile attacks such as Stuxnet, combined with a specific interest by US lawmakers to develop a framework for cyber security for all sectors of the nation's critical infrastructure, underscore the importance of evaluating cyber security requirements for all classes of USNRC licensees.

7. Conclusion

NRC has taken measurable steps to define, institutionalize, and improve the cyber security through improvements to our regulatory framework, development of specific regulations and guidance documents. The development of frameworks and mechanisms that promote and establish a robust cyber security program is critical in today's environment. Cyber threats and vulnerabilities are changing almost daily. As with any continuously learning organization, the

USNRC will evaluate and assess the effectiveness of our regulations and oversight programs. Existing nuclear plants are moving from analog systems to digital systems; and thus, the breath of the programs affected and the importance of providing high assurance of protection from a cyber attack are critical. As we gain experience and insights from the implementation of 10 CFR 73.54, the USNRC plans to revise its regulatory guidance and determine what additional guidance is needed. We will also evaluate and assess how we inspect the performance-based implementation of the regulations and determine if and what changes are prudent.

REFERENCES

[1] UNITED STATES NUCLEAR REGULATORY COMMISSION, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants, NUREG/CR-6847, NRC (2004).

[2] NUCLEAR ENERGY INSTITUTE, Cyber Security Program for Operating Reactors, NEI 04-04, NEI (2005).

[3] UNITED STATES NUCLEAR REGULATORY COMMISSION, Requirements for the Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage, 10 CFR Part 73 (2009).

[4] UNITED STATES NUCLEAR REGULATORY COMMISSION, Protection of Digital Computer and Communication Systems and Networks, 10 CFR 73.54 (2009).

[5] UNITED STATES, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC (2010).

[6] UNITED STATES NATIONAL INSTITUTE OF STATNDARS AND TECHNOLOGY, Recommended Security Controls for Federal Information Systems, NIST 800-53, Rev. 3, NIST (2009).

[7] UNITED STATES NATIONAL INSTITUTE OF STATNDARS AND TECHNOLOGY, Guide to Industrial Control Systems Security, NIST 800-82, NIST (2008).

[8] UNITED STATES NUCLEAR REGULATORY COMMISSION, Reactor Oversight Process (ROP) Basis Document, Inspection Manual Chapter 0308, NRC (2007).

[9] UNITED STATES NUCLEAR REGULATORY COMMISSION, The Nuclear Regulatory Commission Cyber Security Roadmap, SECY-12-0088, NRC (2012).