REGULATORY ANALYSIS

DRAFT REGULATORY GUIDE DG-5061
CYBER SECURITY PROGRAMS FOR NUCLEAR POWER REACTORS
(Proposed Revision 1 of Regulatory Guide 5.71, dated January 2010)

1. Statement of the Problem

The U.S. Nuclear Regulatory Commission (NRC) published Revision 0 of Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," in January of 2010, to provide licensees and applicants with agency-approved guidance for complying with Title 10 of the *Code of Federal Regulations* (10 CFR) Section 73.54, "Protection of digital computer and communication systems and networks."

On October 21, 2010, the Commission issued SRM-COMWCO-10-0001. In the SRM, the Commission determined as a matter of policy that the NRC's cyber security regulation (10 CFR 73.54) should be interpreted to include structures, systems, and components (SSCs) in the Balance of Plant (BOP) that have a nexus to radiological health and safety at NRC-licensed nuclear power plants. The Commission clarified the scope of the rule to include digital assets previously covered by cyber security regulations of the Federal Energy Regulatory Commission. In response to this SRM, licensees updated their cyber security plans to incorporate BOP systems. However, the staff did not include guidance for the BOP systems in its original regulatory guidance.

In 2015, the NRC published the regulation 10 CFR 73.77, "Cyber Security Event Notifications," and its associated guidance, RG 5.83, "Cyber Security Event Notifications," that provides guidance on cyber security event notifications. This rule established requirements clarifying the types of cyber attacks that require notification of the NRC, the timeliness for making the notifications, how licensees make notifications, and how to submit follow-up written reports to the NRC.

The current version of Regulatory Guide (RG) 5.71 is outdated because it does not reflect the lessons learned from operating experience and interim cybersecurity milestone inspections; as well as additional insights gained through industry Frequently Asked Questions, documented cybersecurity attacks, new technologies, and new regulations.

2. Objective

This revision of the guide (Revision 1) would update RG 5.71 to include lessons learned from operating experience since the original publication of the guide. Specifically, this revision would clarify issues identified from interim cybersecurity milestone inspections, additional insights gained through Security Frequently Asked Questions (SFAQs) process, documented cybersecurity attacks, new technologies, and new regulations. This revision would also consider the changes in the most recent revision to the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53, "Recommended Security Controls for Federal Information Systems," upon which Revision 0 of RG 5.71 was based. In addition, this revision to RG 5.71 would clarify the scope to include guidance for SSCs in the BOP, and contain references to the NRC's guidance for cyber security event notifications.

3. Alternative Approaches

The NRC staff considered the following alternative approaches:

1. Do not revise Regulatory Guide 5.71.
2. Withdraw Regulatory Guide 5.71.
3. Revise Regulatory Guide 5.71 to address the current methods and procedures.

Alternative 1: Do not revise Regulatory Guide 5.71

Under this alternative, the NRC would not revise or issue additional guidance, and the current guidance would be retained. This alternative is considered the “no-action” alternative and provides a baseline condition from which any other alternatives will be assessed. If NRC does not take action, there would not be any changes in costs or benefit to the public or the NRC. However, the “no-action” alternative would not address identified concerns with the current version of the regulatory guide. The NRC would continue to review each application on a case-by-case basis.

Alternative 2: Withdraw Regulatory Guide 5.71

Under this alternative the NRC would withdraw this regulatory guide. Withdrawal of the guide would eliminate the important information already provided to commercial nuclear power plant licensees for complying with 10 CFR 73.54. It would also eliminate the only readily available description of the methods the NRC staff considers acceptable for demonstrating compliance with 10 CFR 73.54. Although this alternative would not involve significant resources, it would eliminate the public’s accessibility to the most current NRC guidance available. Licensees may use methods other than those described in this guide to meet the Commission’s regulations if the chosen measures satisfy the stated regulatory requirements.

Alternative 3: Revise Regulatory Guide 5.71

Under this alternative, the NRC would revise Regulatory Guide 5.71. This revision would incorporate the latest information available to the NRC in the form of supporting guidance, practices, and lessons learned from operating experience developed since 2009. By doing so, the NRC would ensure that the RG guidance available in this area is current, remains robust and accurately reflects the staff’s position.

The impact to the NRC would be the costs associated with preparing and issuing the regulatory guide revision. The impact to the public would be the voluntary costs associated with reviewing and providing comments to NRC during the public/stakeholder comment period. The value to NRC staff and NRC stakeholders would be the benefits associated with enhanced efficiency and effectiveness in using a common guidance document as the technical basis for license applications and other interactions between the NRC and its regulated entities.

Conclusion

Based on this regulatory analysis, the NRC staff concludes that revision of Regulatory Guide 5.71 is warranted. The staff concludes that the proposed action will enhance a licensee’s or applicant’s access to the most current information available since the guide’s original issuance.