REGULATORY ANALYSIS

DRAFT REGULATORY GUIDE DG-5079
CYBERSECURITY EVENT NOTIFICATIONS
(Proposed Revision 1 of Regulatory Guide 5.83)

1. Statement of the Problem

In 2015, the U.S. Nuclear Regulatory Commission (NRC) promulgated Title 10 of the *Code of Federal Regulations* 73.77, "Cyber security event notifications," and published its associated guidance, Regulatory Guide (RG) 5.83, "Cyber Security Event Notifications." The final rule established requirements regarding the types of cyberattacks that require notification to the NRC, different timeframes for making notifications, how licensees make notifications, and how licensees submit written security follow-up reports to the NRC.

The current version of RG 5.83 does not reflect the lessons learned from operating experience and interim cybersecurity milestone inspections, or recent insights gained from international and domestic cybersecurity attacks and new technologies. In addition, the NRC recently published Revision 1 of RG 5.71, "Cybersecurity Programs for Nuclear Power Reactors," which includes changes to the definitions in the glossary that are also used in RG 5.83. Finally, the Nuclear Energy Institute (NEI) has requested endorsement of NEI 15-09, "Cybersecurity Event Notifications," Revision 1 (Agencywide Documents Access and Management System (ADAMS) Accession Number ML22298A228) as an acceptable method to meet the requirements of 10 CFR 73.77.

2. Objective

This revision of the guide would update RG 5.83 to include lessons learned from operating experience since the original publication of the guide. Specifically, this revision would incorporate editorial changes to align the guide with the current revision of NUREG-1379, Revision 3, "NRC Editorial Style Guide"; approve NEI 15-09, Revision 1 for use as an acceptable method to meet the requirements of 10 CFR 73.77; add discussion regarding eight-hour notifications for incidents involving devices residing on the same network as a critical digital asset (CDA) or devices that support CDAs; add examples of malicious activity observed on a boundary device protecting a network containing CDAs; and revise the glossary to align with definitions in RG 5.71, Revision 1.

3. Alternative Approaches

The NRC staff considered the following alternative approaches:

1. Do not revise RG 5.83.
2. Withdraw RG 5.83 without issuing a revised RG.
3. Develop a revised RG 5.83 to address the current methods and procedures.

Alternative 1: Do not revise RG 5.83

Under this alternative, the NRC would not revise RG 5.83 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 act, 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 RG.

Alternative 2: Withdraw RG 5.83 without issuing a revised RG

Under this alternative, the NRC would withdraw this RG and would not issue a revised RG. Withdrawal of the guide would eliminate the important information already provided to commercial nuclear power plant licensees for complying with 10 CFR 73.77. It would also eliminate one of the only readily available descriptions of the methods the NRC staff considers acceptable for demonstrating compliance with 10 CFR 73.77. Licensees may, however, use methods other than those described in this guide to meet NRC regulations, if appropriately justified. Although this alternative would not involve significant resources, it would eliminate the public's accessibility to the most current NRC guidance available on cybersecurity event notification requirements.

Alternative 3: Develop a revised RG 5.83

Under this alternative, the NRC would develop and publish for comment DG-5079, a proposed revision of RG 5.83. This proposed 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 2015. By revising RG 5.83, the NRC would ensure that the guidance related to cybersecurity event notifications 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 revised RG. The impact to the public would be the voluntary costs associated with reviewing and providing comments to NRC during the public comment period. NRC staff, licensees, and other stakeholders would benefit from the enhanced clarity and effectiveness of using an updated guidance document as a technical basis for demonstrating compliance with regulatory requirements for reporting cybersecurity events to the NRC.

Conclusion

Based on this regulatory analysis, the NRC staff concludes that issuance of a revision of RG 5.83 is warranted. The staff concludes that the proposed action will enhance a licensee's access to and understanding of the most current information available regarding cybersecurity event notifications required by 10 CFR 73.77 since the guide's original issuance.