[7590-01-P]

NUCLEAR REGULATORY COMMISSION

Final Regulatory Guide: Issuance, Availability

[NRC-2010-0009]

AGENCY: Nuclear Regulatory Commission.

ACTION: Notice of Issuance and Availability of Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities."

FOR FURTHER INFORMATION CONTACT: Karl J. Sturzebecher, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, telephone: (301) 251-7494 or e-mail *Karl.Sturzebecher@nrc.gov*.

SUPPLEMENTARY INFORMATION:

I. Introduction

The U.S. Nuclear Regulatory Commission (NRC or Commission) is issuing a new guide in the agency's "Regulatory Guide" series. This series was developed to describe and make available to the public information such as methods that are acceptable to the NRC staff for implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in its review of applications for permits and licenses

RG 5.71, "Cyber Security Programs for Nuclear Facilities," was issued with a temporary identification as Draft Regulatory Guide, DG-5022. This regulatory guide provides guidance to applicants and licensees on satisfying the requirements of 10 CFR 73.54. The information contained within this guide represents the results of research conducted by the NRC Office of Nuclear Regulatory Research concerning cyber security program development and the collective

body of knowledge and experience that has been developed through all of the actions identified above. In addition, this guide embodies the findings by standards organizations and agencies, such as the International Society of Automation, the Institute of Electrical and Electronic Engineers, and the National Institute of Standard and Technology, as well as guidance from the U.S. Department of Homeland Security.

RG 5.71 provides a framework to aid in the identification of those digital assets that must be protected from cyber attacks. These identified digital assets are referred to as critical digital assets (CDAs). Licensees should address the potential cyber security risks of CDAs by applying the defensive architecture and the collection of security controls identified in this regulatory guide.

The RG 5.71 framework offers licensees and applicants the ability to address the specific needs of an existing or new system. The goal of this regulatory guide is to harmonize the well-known and well-understood set of security controls (based on NIST cyber security standards) that address potential cyber risks to CDAs to provide a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate these security controls into a site-specific cyber security program.

II. Further Information

The Agency released DG-5022, which contained safeguards information, directly to stakeholders, who provided comments on July 18, 2008, December 12, 2008, and January 14, 2009. The responses to stakeholder's comments are located in the NRC's Agencywide Documents Access and Management System under Accession Number ML090340185. Electronic copies of RG 5.71 are available through the NRC's public Web site under "Regulatory Guides" at *http://www.nrc.gov/reading-rm/doc-collections/*.

In addition, regulatory guides are available for inspection at the NRC's Public Document Room (PDR) located at 11555 Rockville Pike, Rockville, Maryland. The PDR's mailing address is USNRC PDR, Washington, DC 20555-0001. The PDR can also be reached by telephone at (301) 415-4737 or (800) 397-4205, by fax at (301) 415-3548, and by e-mail to pdr.resource@nrc.gov.

Regulatory guides are not copyrighted, and Commission approval is not required to reproduce them.

Dated at Rockville, Maryland, this 6 day of January, 2010.

For the Nuclear Regulatory Commission.

/RA/

Andrea D. Valentin, Chief,
Regulatory Guide Development Branch,
Division of Engineering,
Office of Nuclear Regulatory Research.