UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

May 7, 2014

MEMORANDUM TO: Mark A. Satorius
Executive Director for Operations

FROM: Stephen D. Dingbaum ***/RA/***
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S CYBER SECURITY INSPECTION PROGRAM FOR NUCLEAR POWER PLANTS (OIG-14-A-15)

The Office of the Inspector General (OIG) conducted this audit to determine the adequacy of the Nuclear Regulatory Commission's (NRC) cyber security inspection program for nuclear power plants. Through interviews with NRC staff, analysis, and direct observation, OIG auditors determined that NRC has adequate management controls in place for the cyber security inspection program. Therefore, OIG makes no recommendations.

BACKGROUND

NRC's Role in Power Plant Cyber Security Oversight

Cyber threats to NRC licensees are dynamic and multi-dimensional due to the continuously evolving capabilities of potential adversaries and emerging technologies. Potential adversaries run the gamut from nation-state actors to individuals. Recent threats against international nuclear facilities, such as Stuxnet and Duqu, are examples of malware specifically targeting control systems that operate industrial facilities, such as nuclear power plants.

The purpose of cyber security is to detect and then eliminate or mitigate vulnerabilities in digital systems that could be exploited either from outside or inside of a plant's protected area. Licensees operating a nuclear power plant are required to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks in accordance with 10 Code of Federal Regulations 73.54, which is also known as the "Cyber Security Rule."

In January 2013, NRC issued Temporary Instruction 2201/004 and began cyber security inspections of nuclear power plants in accordance with the Cyber Security Rule. The Cyber Security Rule required nuclear power plants licensed by NRC to submit a Cyber Security Plan with a proposed implementation schedule to the Commission for review and approval. However, the rule did not mandate an effective date for implementation of licensees' cyber security programs. As a result, NRC staff worked with the nuclear power industry to develop seven interim implementation milestones (i.e., Milestones 1-7) based on organizational and technical security controls to be used while licensees prepare for full implementation, which NRC and licensees commonly refer to as "Milestone 8." NRC expects licensees to implement their respective Milestone 8 cyber security programs beginning in late calendar year 2014 through the end of calendar year 2017. NRC's Milestone 8 inspections will occur on a rolling basis as licensees come into full compliance with their regulatory commitments.

The Cyber Security Directorate of the Office of Nuclear Security and Incident Response oversees activities related to the cyber security inspection of NRC licensees, which are managed at the regional level. Headquarters staff and security risk analysts provide support to inspectors based in NRC's four regional offices. Cyber security specialists under contract to NRC serve as technical advisors to the NRC teams and assist with some inspection tasks.

NRC Interim and Full Implementation Cyber Security Inspections

In January 2013, NRC issued Temporary Instruction 2201/004 and staff began cyber security inspections at nuclear power plants using Temporary Instruction guidance that was developed specifically for assessing licensees' interim cyber security programs according to Milestone 1-7 criteria. NRC inspection teams spend two separate weeks onsite at nuclear power plants for each cyber security inspection. During the first week, inspectors obtain and review documentation, and familiarize themselves with a plant's cyber security program, personnel, and layout. During the second week onsite, NRC

teams perform followup and verification tasks, and present conclusions of their work to licensees. In cases where inspection teams identify tentative findings, they present the findings to licensees during the second inspection week, and then submit the findings for review by NRC's Security Issues Forum.[1]

NRC has allocated 1.5 Full Time Equivalents each to Regions I, III, and IV for cyber security inspections; Region II has been allocated 2 Full Time Equivalents because of its additional responsibility for new reactor construction inspections. Region-based teams are supported by headquarters staff as well as NRC cyber security contractors. As of December 2013, NRC had conducted 21 cyber security inspections among all 4 regions. Each 2-week inspection for Milestones 1-7 requires approximately 64 hours.

NRC staff members have developed a new draft Temporary Instruction to be used in Milestone 8 pilot inspections, which are planned to begin in the spring of Calendar Year 2015.

OBJECTIVE

The audit objective was to determine the adequacy of NRC's cyber security inspection program for nuclear power plants.

RESULTS

The audit determined that NRC has adequate management controls in place for the cyber security inspection program.[2] Although OIG did not identify any findings or make any recommendations, this report describes specific challenges related to resource management and inspection guidance as NRC moves toward full implementation of its cyber security inspection program.

NRC Cyber Security Inspection Program Has Adequate Management Controls

The Cyber Security Rule took effect in 2009 and established regulatory requirements for the nuclear power industry. Subsequent to the rule, NRC:

- Developed, in consultation with industry, an interim inspection program based on technical milestones.

[1] NRC created the Security Issues Forum to provide a means for regional and headquarters staff to discuss security findings and to promote regulatory consistency. NRC is currently paneling all cyber security inspection findings through the Security Issues Forum to ensure proper handling and use of enforcement discretion before final disposition of findings.

[2] Management controls include organizational structure and delegation of authority, human capital management, program monitoring, and communication with internal and external stakeholders.

- Created a preliminary inspector training program for headquarters- and region-based staff.

- Performed pilot inspections at nuclear power plants and used those inspections to test and develop interim inspection guidance.

- Created a Cyber Security Directorate within the Office of Nuclear Security and Incident Response to consolidate program management in a single organization at NRC.

- Issued multiple supplementary guidance documents for use by NRC staff and licensees.

- Engaged industry stakeholders through conferences and staff meetings.

Resource Management and Guidance Challenges as the Program Moves Into Full Implementation

Resource Challenges

Milestone 8 will expand the current scope of cyber security inspections and create resource management challenges for NRC. Currently, NRC's inspection scope is limited to critical digital components and systems[3] associated with target set equipment.[4] Milestone 8 inspections will expand inspection scope to cover *all* critical digital components and systems with a safety, security, and emergency preparedness function. In addition, NRC will begin inspecting "balance of plant" equipment,[5] which traditionally falls under Federal Energy Regulatory Commission jurisdiction. Although NRC provided initial cyber security training to inspectors in 2012, establishment of a formalized cyber security inspection training program has been delayed, due in part to

[3] NRC guidance refers to "critical digital assets," which are defined as digital assets that must be protected against cyber attacks in accordance with 10 Code of Federal Regulations 73.54.

[4] A target set is defined as a minimum combination of equipment or operator actions that, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in radiological sabotage. Specifically, this entails significant core damage or a loss of coolant and exposure of spent fuel, barring extraordinary actions by plant operators.

[5] "Balance of plant" refers to the interface between a power plant and the electrical grid, such as electrical distribution equipment leading out to a plant's first inter-tie with the offsite distribution system.

funding issues.[6] In addition, NRC staff cited recruitment and retention as challenges, with several inspectors having retired or become eligible for retirement in 2013. NRC managers must balance these issues with inspection requirements for other programs, particularly at NRC regional offices, where inspectors also work in other oversight programs like fire protection and physical security. Recruiting, retaining, and training adequate numbers of inspectors with appropriate skills, and determining the appropriate level of contractor support for inspections, is important to ensuring that NRC inspection teams are adequately staffed to conduct Milestone 8 inspections thoroughly and consistently in accordance with NRC standards.

Guidance Challenges

NRC faces challenges as it develops guidance for use by inspectors as well as licensees. In particular, sampling guidance for inspectors will become especially important with the expanded scope of Milestone 8 inspections. Sound sampling methodology can help inspectors perform thorough inspections and reduce reliance on professional judgment in sample selection. For instance, some staff told auditors that they did not understand the basis for the current sampling methodology, while others said that sample selection depends considerably on professional judgment and time available to perform inspection work. NRC is working to address this issue, in part through endorsement of industry-developed guidance for "consequence based analysis" of critical digital assets. Further, regulatory guidance that clearly articulates NRC's regulatory position is important to prevent misinterpretation by licensees of regulatory standards.

During early Milestone 1-7 inspections, some licensee performance problems were reportedly attributable to lack of alignment between industry and NRC guidance, as well as misinterpretation by licensees of key technical definitions. Licensees bear considerable implementation costs, and want assurance that their cyber security investments help them satisfy regulatory commitments. Creating inspection guidance is an iterative process, and using lessons learned from pilot inspections is critical to developing guidance that helps inspectors do their work effectively while facilitating licensee compliance with NRC regulations. NRC can thus enhance the transparency of Milestone 8 inspections and foster regulatory stability by issuing clear guidance that incorporates lessons learned from prior inspections.

[6] NRC's Technical Training Center plans to begin a training needs assessment in October 2014, and will develop a training program for NRC inspectors based on results of this assessment. The new cyber security inspection training program is projected to be ready by summer 2015.

CONCLUSION

OIG conducted this audit to determine the adequacy of NRC's cyber security inspection program for nuclear power plants. Through interviews with NRC staff, analysis, and direct observation, OIG auditors determined that NRC has adequate management controls in place for the cyber security inspection program. Therefore, OIG makes no recommendations.

AGENCY COMMENTS

An exit conference was held with the agency on April 25, 2014. Prior to this meeting, a discussion draft was distributed to the agency for comment. Agency staff had no formal comments for inclusion in this report.

SCOPE AND METHODOLOGY

To address the audit objective, auditors reviewed and analyzed pertinent law, regulations, authoritative guidance, NRC policies and procedures, inspection reports, and prior relevant NRC OIG reports. Guidance reviewed included the following:

- Government Accountability Office Standards for Internal Control in the Federal Government.
- Title 10 Code of Federal Regulations, Part 73, Section 73.54.
- Management Directive 11.1, *NRC Acquisition of Supplies and Services*.
- Inspection Manual Chapter 1245, *Qualification Program For Operating Reactor Programs.*
- Temporary Instruction 2201/004, *Inspection of Implementation of Interim Cyber Security Milestones 1-7.*
- Regulatory Guide 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.*
- Regulatory Guide 5.71, *Cyber Security Programs for Nuclear Facilities*.
- NRC Security Frequently Asked Questions for Milestones 1-7.

- National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

- Nuclear Energy Institute 08-09, *Cyber Security Plan for Nuclear Power Reactors*.

OIG auditors interviewed managers, inspectors, and other program staff from NRC headquarters and all four NRC regional offices, both in person and by telephone, to gain an understanding about the qualifications of the inspectors and management staff for cyber security inspections. OIG interviewed NRC staff responsible for inspection training to assess the agency's progress in formalizing the cyber security inspection training program. OIG interviewed industry representatives and licensee personnel to gather external perspectives on program performance and NRC management's receptivity to industry concerns. OIG also reviewed NRC contract documentation for cyber security technical support. During this audit, OIG observed cyber security inspections at two nuclear power plants: Quad Cities Nuclear Power Station in Cordova, IL, and Vogtle Electric Generating Plant in Waynesboro, GA. Prior to starting this audit, OIG attended cyber security inspection training provided to NRC staff at Idaho National Laboratory and observed cyber security inspections at Calvert Cliffs Nuclear Power Plant in Lusby, MD, and at Oconee Nuclear Station in Oconee County, SC.

OIG conducted this performance audit from October 2013 through March 2014 at NRC headquarters in Rockville, MD, and at licensee facilities. Internal controls related to the audit objective were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility or existence of fraud, waste, or abuse in the program. We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Ziad Buhaissi, Senior Auditor; and Neil Doherty, Senior Analyst.