OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Audit of NRC's Cyber Security Inspections at Nuclear Power Plants

OIG-19-A-13
June 4, 2019

All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

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

OFFICE OF THE
INSPECTOR GENERAL

June 4, 2019

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

FROM: Dr. Brett M. Baker ***/RA/***
Assistant Inspector General for Audits

SUBJECT: AUDIT OF NRC'S CYBER SECURITY INSPECTIONS AT NUCLEAR POWER PLANTS (OIG-19-A-13)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Cyber Security Inspections at Nuclear Power Plants*.

The report presents the results of the subject audit. Following the May 30, 2019, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendation(s) within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Paul Rades, Team Leader, at (301) 415-6228.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-19-A-13
June 4, 2019

Results in Brief

Why We Did This Review

Under the Cyber Security Rule at 10 Code of Federal Regulations 73.54, the Nuclear Regulatory Commission (NRC) requires that licensees operating a nuclear power plant provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. The Cyber Security Rule required licensees to submit for NRC review and approval a Cyber Security Plan with a proposed implementation schedule.

NRC is conducting cyber security inspections through 2020 to verify that licensees have fully developed cyber security programs conforming to the Cyber Security Rule and licensing basis commitments such as the approved Cyber Security Plan.

The audit objective was to determine whether the cyber security inspection program provides reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness.

Audit of NRC's Cyber Security Inspections at Nuclear Power Plants

What We Found

NRC's cyber security inspections generally provide reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness.

However, although NRC trains current staff as cyber security inspectors, the inspection program faces future staffing challenges because demographic and resource constraints work against optimal staffing. Challenges in maintaining cyber security expertise among the inspectors could hinder NRC's ability to manage cyber security risk.

Additionally, the current cyber security inspection program is risk-informed but not yet fully performance based. The cyber security inspection program has not identified performance measures because of technical and regulatory challenges in program implementation, and there are challenges in predicting the level of effort required to conduct inspections. Identifying appropriate performance measures will permit NRC's cyber security inspection program to become more efficient and reliable without diminishing the level of assurance.

What We Recommend

This report makes two recommendations to address future inspection staffing challenges and suitable performance measures for the cyber security inspection program. Agency management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
ICS	Industrial Control System
NIST	National Institute of Standards and Technology
SP	Special Publication

I. BACKGROUND

NRC's Cyber Security Rule and Rule Implementation

In 2009, NRC published the Cyber Security Rule in 10 Code of Federal Regulations 73.54, requiring that licensees operating a nuclear power plant provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks.[1] The Cyber Security Rule required licensees to submit for NRC review and approval a Cyber Security Plan with a proposed implementation schedule.[2]

Milestone 1 Through 7 Inspections

NRC executed its cyber security inspection program in phases. In the first phase, NRC worked with industry to develop seven interim milestones for licensee Cyber Security Plan implementation, known as Milestones 1 through 7. Through the milestones, a licensee would deploy the planned defensive strategy consisting of a defensive architecture and security controls, supported by important program elements. Each milestone focused on a subset of systems and requirements to address specific technical and organizational controls required by the Cyber Security Plan. For example, Milestone 2 required identification of Critical Digital Assets.[3] Milestone 6 required applying security controls[4] to the most important Critical Digital Assets.

[1] The Cyber Security Rule formalized the requirement established by the 2007 NRC update of the "Design Basis Threat Rule" to add cyber attack as a threat licensees must be able to protect against to prevent radiological sabotage.

[2] The deadline for Cyber Security Plan and implementation schedule submission was November 23, 2009. Although the Cyber Security Rule was effective in 2009, there was no mandated effective date for implementation of licensees' cyber security programs.

[3] Critical Digital Assets are digital components of critical systems, such as plant systems or communication systems, which perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.

[4] Security controls are the safeguards and countermeasures prescribed for information systems as defined in National Institute of Standards and Technology Special Publication 800-53, Revision, 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

The defensive architecture protects Critical Digital Assets that have similar risk significance from other devices, systems, or equipment by establishing the logical and physical boundaries to control the data transfer between boundaries. The boundaries denote levels entailing security control requirements rather than networks of devices. Defensive levels with the highest cyber security risk significance are separated from other levels by one-way deterministic devices that limit data flow to one direction.

NRC conducted inspections during the interim milestones,[5] with the goal of preparing licensees for the final and current verification phase, Milestone 8. Inspections of Milestones 1 through 7 focused on a limited set of controls tailored to address significant threats to specific systems, structures and components. Under Milestone 8, by the end of 2017, NRC expected licensees to have fully developed cyber security programs conforming to the Cyber Security Rule and licensing basis commitments such as the approved Cyber Security Plan.

Milestone 8 Inspections

The Milestone 8 inspections began in 2017 and are scheduled to end in 2020. These inspections[6] review the full scope of a licensee's cyber security program, beyond the targeted requirements inspected during Milestones 1 through 7. NRC inspection teams spend two separate weeks onsite for each cyber security inspection, in addition to time spent offsite conducting information requests, inspection planning, document review, and inspection report preparation. As of March 31, 2019, NRC had conducted Milestone 8 inspections at 24 of 57 nuclear power plant licensees subject to NRC's cyber security regulations.

The Cyber Security Branch in NRC's Office of Nuclear Security and Incident Response leads activities related to oversight of cyber security programs. Division of Reactor Safety staff based at each of NRC's four

[5] In 2014, OIG conducted an audit of NRC's interim milestone oversight, and published OIG-A-14-15, *Audit of NRC's Cyber Security Inspection Program for Nuclear Power Plants*. The report made no recommendations.

[6] The Milestone 8 inspections are conducted based on a provisional inspection procedure, *Inspection Procedure 71130.10P, Cyber Security*.

regions conduct the inspections. The inspection teams consist of four people: two inspectors, and two contractors who serve as technical cyber security advisors. NRC inspectors have backgrounds in engineering and typically conduct engineering and fire protection inspections, in addition to cyber security inspections.[7]

NRC's Assessment of the Cyber Security Oversight Program

In early 2019, NRC staff began an assessment of the agency's cyber security oversight program for nuclear power plant licensees to prepare for the next phase. Based on input from NRC staff, licensees, other regulators, and industry organizations,[8] staff are evaluating the effectiveness of Milestone 8 cyber security inspections and developing potential options for modifying the program in the future. NRC staff expect to complete this assessment in mid-2019.

II. OBJECTIVE

The audit objective was to determine whether the cyber security inspection program provides reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety,[9] security, and emergency preparedness. The report appendix contains information on the audit scope and methodology.

[7] Inspectors conducting the cyber security inspections follow a qualification program and take introductory and advanced cyber security training.

[8] Regulators include the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation. Industry organizations include Nuclear Energy Institute, Institute for Nuclear Power Operations, and Nuclear Information Technology Strategy Leadership.

[9] Safety-related structures, systems and components are relied upon to remain functional during and following design basis events, such as to ensure safe shutdown. Systems that perform important-to-safety functions should include those that are required to maintain diversity and defense-in-depth for safety functions.

III. FINDINGS

NRC's cyber security inspections generally provide reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness. However, opportunities exist to improve NRC's cyber security inspection program by (1) creating strategies to support recruitment, training, and retention of personnel for a future inspection program, and (2) making the inspection program more performance based.

A. NRC Can Strengthen Its Future Inspection Program By Developing Strategies To Support Recruitment, Training, And Retention Of Personnel

NRC should determine potential gaps in critical skills and competencies to address emerging needs and workload fluctuations. NRC trains current staff as cyber security inspectors, but the inspection program faces future staffing challenges, because demographic and resource constraints work against optimal staffing. If this is not addressed, challenges in maintaining cyber security expertise among the inspectors could hinder NRC's ability to manage cyber security risk.

What Is Required

NRC Should Determine Potential Gaps in Critical Skills and Competencies to Address Emerging Needs and Workload Fluctuations

The Government Accountability Office's *Key Principles for Effective Strategic Workforce Planning* and NRC's Strategic Workforce Planning initiative both include strategies that enable NRC to determine potential gaps in critical skills and competencies to address emerging needs and workload fluctuations.

A key principle of workforce planning is to determine the critical skills and competencies needed now and in the future to achieve programmatic goals. Workforce planning should also consider strategies to address gaps in number, deployment, and alignment of human capital to enable and sustain critical skills and competencies. Similarly, NRC's Strategic Workforce Planning initiative seeks to create strategies that enable NRC to recruit, retain, and develop the workforce required to address emerging needs and workload fluctuations.

What We Found

NRC Trains Current Staff as Cyber Security Inspectors But Inspection Program Faces Future Staffing Challenges

NRC is training current staff as cyber security inspectors, but the inspection program faces future staffing challenges. Inspectors have taken introductory and advanced cyber security training, however, regional staff are concerned about training a sufficient number of inspectors to meet future workload requirements. For example, cyber security inspectors do not focus exclusively on cyber security, but also perform inspections in areas such as fire protection at nuclear power plants. Additionally, staff are uncertain about the extent to which NRC will rely on contractors for program support, if at all. This support is critical to the program in its current state because NRC lacks full time staff who have comparable technical expertise that can be leveraged to assist inspection teams.

Why This Occurred

Demographic and Resource Constraints Work Against Optimal Staffing

At NRC there are demographic and resource constraints working against optimal staffing. First, some staff with cyber security experience are approaching retirement age and hiring processes can be slow. As shown in Table 1, currently an average of 26 percent of staff in the regional

Divisions of Reactor Safety[10] are eligible to retire, somewhat higher than the agency average. Further, projected retirement eligibilities for regional staff in the Divisions of Reactor Safety will increase to 32 percent by the end of fiscal year (FY) 2020, illustrating a continuing trend.

Table 1: Retirement Eligibility of NRC Staff

Retirement Eligibility of NRC Staff		
	Now[11]	End FY2020[12]
Regional Divisions of Reactor Safety (combined)	26%	32%
Agencywide	24%	30%

Source: NRC provided data, as of March 2, 2019

Additionally, agencywide, attrition levels of all types far outpace hiring. This is compounded as Governmentwide, Federal agencies face difficulties in recruiting and retaining qualified cyber security staff.

Further, since inspectors perform other, non-cyber security inspections, maintaining cyber security expertise can be difficult. More specifically, performing other non-cyber security inspections means that inspectors have less time on the job to ensure they are receiving cyber security experience. After completing introductory and advanced training, inspectors may enroll in graduate study programs or seek other outside training, both of which can be expensive and time consuming.

[10]Each NRC regional office has a Division of Reactor Safety. All regional staff in the Division of Reactor Safety are combined.

[11] As of March 2, 2019, there are 224 people in the combined regional Divisions of Reactor Safety, 59 of whom are currently eligible to retire. Agencywide, there are 3,003 employees on board, 724 of whom are currently eligible to retire.

[12] By the end of FY2020, 12 more people will be eligible to retire in the Divisions of Reactor Safety, and agencywide, 168 more people will be eligible to retire.

Why This Is Important

Challenges in Maintaining Cyber Security Expertise Among Inspectors Could Hinder NRC's Ability To Manage Cyber Security Risk

NRC relies on qualified, well trained personnel to perform its oversight mission effectively. If staffing levels and skillsets do not align with cyber security inspection workload requirements, NRC's ability to adapt to a dynamic threat environment and detect problems with licensees' cyber security programs could be compromised.

Recommendation

OIG recommends that the Executive Director for Operations

1. Concurrent with developing any changes to the cyber security inspection program, use the Strategic Workforce Planning initiative to identify critical skill gap and closure strategies for future cyber security inspection staffing, such as:

    a) Hiring flexibilities,
    b) Internal rotations,
    c) Competency modeling,
    d) Availability of outside training and continuous training,
    e) Appropriate numbers and roles of staff.

B. The Cyber Security Inspection Program Needs Changes to Become Fully Performance Based

The current cyber security inspection program is risk-informed but not yet fully performance based, although NRC oversight activities should be risk-informed and performance based. The cyber security inspection program has not identified performance measures because of technical and regulatory challenges in program implementation. The broad scope inspection, while effective, cannot be sustained beyond the current commitment.

What Is Required

NRC's Reactor Oversight Process Is Risk-Informed and Performance Based

NRC oversight activities should be risk-informed and performance based. The Reactor Oversight Process[13] uses licensee-reported formal performance indicators[14] that provide objective indications of key attributes of licensee performance. Performance indicators have risk-informed thresholds and support performance assessment between inspections. A risk-informed approach incorporates an assessment of safety significance or relative risk. Less formal performance measures, such as site-specific assessments or analyses, are also risk-informed, and can support the conduct of performance based[15] inspections.

The National Institute of Standards and Technology (NIST) recommends attributes of potential performance measures for cyber security, emphasizing that performance measures development should use a risk-informed approach to identify a small number of high-priority measures. NIST Special Publication (SP) 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*,[16] points out that the impacts on an ICS, such as in critical infrastructure, cannot be adequately determined by focusing only on the digital aspects of the system, and non-digital mechanisms must be incorporated into the impact assessment process.

NIST SP 800-82 discusses how to determine that the system controls perform as intended and measure performance against a set of predefined and appropriate metrics. Performance areas that can be gauged include vulnerability assessment and patching, equipment changes, equipment

[13] The Reactor Oversight process is described in key policy and guidance documents Management Directive 8.13, *Reactor Oversight Process*, and Inspection Manual Chapter 0308, *Reactor Oversight Process Basis Document*.

[14] NRC defines performance indicator as a quantitative measure of a particular attribute of licensee performance that shows how well a plant is performing when measured against established thresholds.

[15] A performance based oversight approach focuses on desired, measurable outcomes or results, rather than prescriptive processes, techniques, or procedures.

[16] NIST Special Publication 800-82, Revision 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015.

configurations, and antivirus software management. Because typical tools for assessing performance in traditional information technology networks can be too intrusive for ICS, NIST SP 800-82 recommends testing in a laboratory[17] or replicated environment[18] or passively collecting[19] vulnerability information. Using both methods provides a more complete picture of performance while reducing ICS operational risks.

What We Found

Cyber Security Inspections Are Not Yet Fully Performance Based

The current cyber security inspection program is risk-informed but not yet fully performance based. Current cyber security inspections are largely programmatic and compliance based. The principal focus of the inspection procedure is verifying that the key cyber security program elements have been established and are working together effectively in a viable program.

NRC Activities

The current provisional inspection procedure, IP 71130.10P, *Cyber Security*, is compliance oriented, emphasizing selection of samples of a certain size and composition from licensee-identified critical systems and critical digital assets, and reviewing the configured security controls. The primary consideration in sample selection is plant safety, and inspectors use both quantitative and qualitative risk information to identify what is safety significant. Inspectors review the controls on sampled systems and assets through activities such as walkdowns and physical inspections, interviews with cognizant staff, and reviews of control assessments.

NRC inspectors also verify that the licensee's defensive architecture establishes cyber security defensive levels. Defensive levels are

[17] For example, components of ICS like redundant servers or independent test systems can be tested in lab conditions.

[18] Replicated, virtualized, or simulated environments help to accommodate testing of ICS.

[19] For example, a passive tool can provide real-time diagnostic security information by continuously monitoring activity in an ICS network and sending alerts of any abnormal activity.

separated by security boundary devices, and inspectors verify the effectiveness of boundary implementation. For example, one approach used by industry is to place a one-way deterministic device in one defensive level, with a monitoring device placed immediately after in the next lowest defensive level to confirm data flow restriction. NRC inspectors examine the configurations of security boundary devices and may review logs or log scan results. Inspectors do not routinely perform log reviews for all boundary devices.

The use of risk-informed samples is supplemented by programmatic reviews of many areas, including training, supply chain management, documentation of assessments, table top incident response drills, and monitoring. These verify that the licensee's full implementation of the planned cyber security program meets NRC regulatory requirements.

Licensee Activities

Licensee cyber security programs include areas with potential for identifying performance measures as described in NIST SP 800-82. For example, through activities such as program self-assessments and audits, licensees understand how aspects of their programs work together. Technical activities include use of laboratory testing for configuring new equipment, testing vendor patches for their specific environments, and other maintenance activities. In addition, licensees have deployed tools, such as security information and event management devices, for real-time monitoring of boundary devices, logs, antivirus, patch management, and other security mechanisms. These practices and tools can provide evidence of program performance.

Why This Occurred

Technical and Regulatory Challenges Impeded Use of Cyber Security Performance Measures

The cyber security inspection program has not identified performance measures because of technical and regulatory challenges. The interim inspection milestones reflected an understanding by both NRC staff and industry of potential challenges in full implementation of new cyber

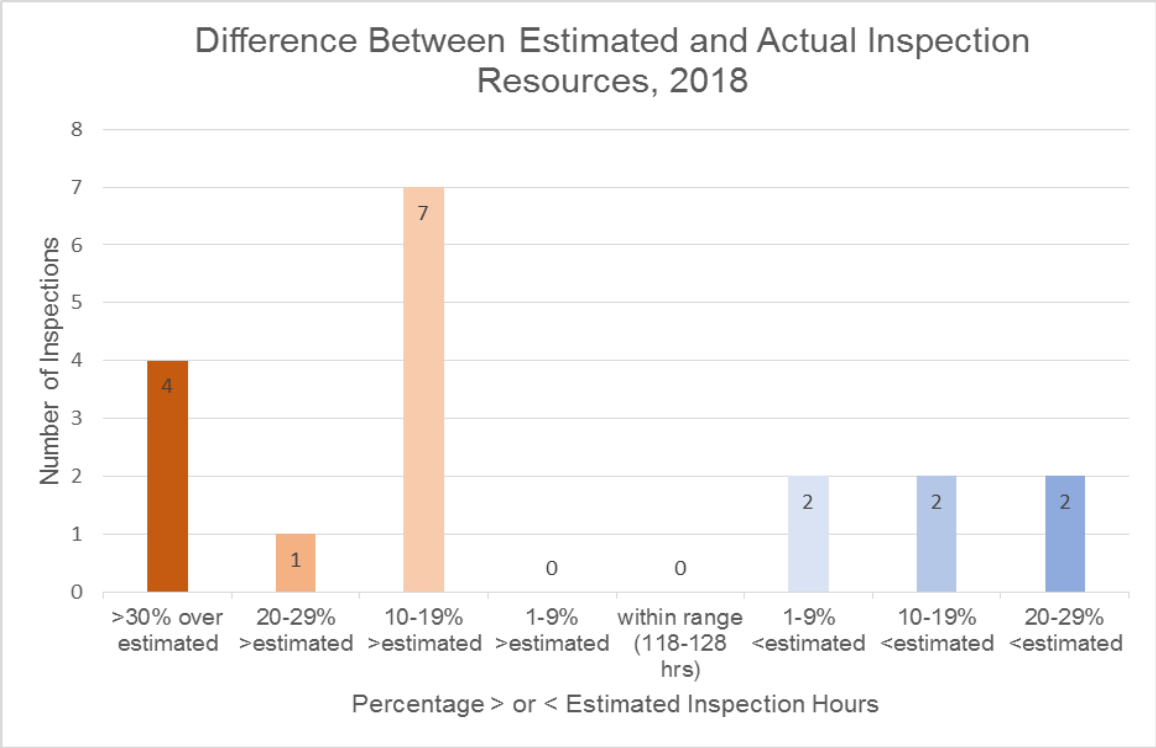
security programs. For example, ICS in nuclear power plants mix legacy and modern control devices. Licensees report that their control systems continue to require additional considerations for cyber defense because they directly control continuous processes and operational risk is higher than security risk. Both NRC staff and industry representatives describe how technical complexities of implementing the milestones prompted significant effort on guidance development and revisions during the last decade. In turn, NRC incorporated lessons learned from the interim milestones into the current inspection program, but could not alter the program until verifying that licensees had completely met the new cyber security regulatory requirement.

Why This Is Important

While Effective, Cyber Security Inspections Need Changes

The broad scope inspection, while effective, cannot be sustained beyond the current commitment. The current inspection program is resource intensive for both the licensees and the agency, and requires a wide range of hours to complete, depending on conditions at each facility inspected. The inspection procedure identifies an estimated range of hours in which the current inspection should be completed. As shown in Chart 1 below, of 18 inspections completed during calendar year 2018, none were completed within the estimated range. Further, two-thirds ran more than the estimate, and 4 out of 18 were more than 30 percent greater than the estimate.

Chart 1: Difference Between Estimated and Actual Inspection Resources, 2018



Source: OIG, from RPS data

The inspection procedure requires a deep dive into a licensee's program, and inspection resource requirements vary depending upon site characteristics, licensees' documentation, and the level of licensee preparation for inspections. This presents challenges for NRC in predicting the level of effort required to conduct inspections. Licensees are also impacted because they commit significant resources to support NRC inspection teams while the teams are onsite, and must plan accordingly.

NRC strives for its regulatory activities to be both efficient and predictable. Where several effective alternatives are available, the option which minimizes the use of resources should be adopted. Once established, regulation should be perceived to be reliable and not unjustifiably in a state of transition. Identifying appropriate performance measures will permit NRC's cyber security inspection program to become more efficient and reliable without diminishing the level of assurance.

Recommendation

OIG recommends that the Executive Director for Operations

2. Use the results of operating experience and discussions with industry to develop and implement suitable cyber security performance measure(s) (e.g., testing, analysis of logs, etc.) by which licensees can demonstrate sustained program effectiveness.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Concurrent with developing any changes to the cyber security inspection program, use the Strategic Workforce Planning initiative to identify critical skill gap and closure strategies for future cyber security inspection staffing, such as:

    a. Hiring flexibilities,
    b. Internal rotations,
    c. Competency modeling,
    d. Availability of outside training and continuous training,
    e. Appropriate numbers and roles of staff.

2. Use the results of operating experience and discussions with industry to develop and implement suitable cyber security performance measure(s) (e.g., testing, analysis of logs, etc.) by which licensees can demonstrate sustained program effectiveness.

V. AGENCY COMMENTS

An exit conference was held with the agency on May 30, 2019. Prior to the meeting, after reviewing a discussion draft, agency management had no comments on the report. At the meeting, agency management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

Appendix

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether the cyber security inspection program provides reasonable assurance that nuclear power plant licensees adequately protect digital computers, communication systems, and networks associated with safety, important-to-safety, security, and emergency preparedness.

Scope

The audit focused on NRC's cyber security inspections at nuclear power plants. OIG conducted this performance audit from August 2018 to March 2019 at NRC headquarters (Rockville, MD). We visited three nuclear power facilities in Athens, AL; Berwick, PA; and Killona, LA. During that time, internal controls related to the audit objectives were reviewed and analyzed.

Methodology

To accomplish the audit objective, OIG reviewed relevant regulations and guidance including

- Title 10 Code of Federal Regulations, Part 73, Section 73.54, "Protection of Digital Computer and Communication Systems and Networks."
- NRC Regulatory Guide: 5.71, *Cyber Security Programs for Nuclear Facilities*, dated January 2010.
- Management Directive and Handbook 8.13, *Reactor Oversight Process*, dated January 16, 2018.
- Executive Director of Operations, *Enhancing Strategic Workforce Planning*, Memorandum dated January 19, 2017, ADAMS Accession Number ML17005A256.
- Inspection Manual Chapter 1245, Appendix C-14, *Cyber Security Inspector Technical Proficiency Training and Qualification Journal*, dated August 3, 2015.
- Inspection Manual Chapter 0308, *Reactor Oversight Process Basis Document*, dated January 1, 2018.
- Inspection Procedure 71130.10P, *Cyber Security*, dated May 15, 2017.

- Government Accountability Office 04-39, Human Capital: *Key Principles for Effective Strategic Workforce Planning*, dated December 2003.
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated January 22, 2016.
- NIST SP 800-82 Revision 2, *Guide to Industrial Control System (ICS) Security*, dated May 2015.
- NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security*, dated July 2008.
- Nuclear Energy Institute 08-09 Revision 6, *Cyber Security Plan for Nuclear Power Reactors*, dated April 2010.

OIG also reviewed inspection data and agency hiring and attrition data.

OIG conducted interviews of NRC staff, management, and industry representatives to gain an understanding of inspector qualifications and the performance of the cyber security inspection program. Auditors interviewed staff from the Office of Nuclear Security and Incident Response and all NRC Regions, licensee representatives, and representatives from the Nuclear Energy Institute.

OIG auditors also observed the work of inspection teams from NRC Regions I, II, and IV on their cyber security inspections at Browns Ferry Nuclear Power Plant, Susquehanna Steam Electric Station, and Waterford 3 Nuclear Generating Station in October and November 2018. In addition, OIG observed Security Issues Forums and public meetings related to the cyber security inspections.

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, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Throughout the audit, auditors considered the possibility of fraud, waste, and abuse in the program.

The audit was conducted by Paul Rades, Team Leader; Amy Hardin, Audit Manager; Tim Wilson, Senior Analyst; Magdala Boyer, Management Analyst; and Mathew Soares, Management Analyst.

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, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TTY/TDD: 7-1-1, or 1-800-201-7165

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.