OFFICE OF THE INSPECTOR GENERAL

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

Audit of NRC's Network Security Operations Center

OIG-16-A-07
January 11, 2016

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

January 11, 2016

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

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

SUBJECT: AUDIT OF NRC'S NETWORK SECURITY OPERATIONS CENTER (OIG-16-A-07)

Attached is the Office of the Inspector General's (OIG) audit report titled *Audit of NRC's Network Security Operations Center*.

The report presents the results of the subject audit. Following the January 5, 2016, 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 recommendations 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 Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

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

OIG-16-A-07

January 11, 2016

Results in Brief

Why We Did This Review

The U.S. Nuclear Regulatory Commission's (NRC) Network Security Operations Center (SOC) is responsible for securing the agency's network infrastructure and monitoring the network for suspicious activity. The SOC accomplishes this through the use of automated security tools, analysis of network activity data, and participation in incident response efforts. The SOC is primarily staffed by contractors working under the Information Technology Infrastructure Support Services (ITISS) contract.

Robust SOC capabilities are particularly crucial given the sensitivity of the unclassified information processed on NRC's network, and the increasing volume of attacks carried out against Federal Government computer systems.

The audit objective was to determine whether NRC's network SOC meets operational requirements, and to assess the effectiveness of SOC coordination with other organizations that have a role in securing NRC's network.

Audit of NRC's Network Security Operations Center

What We Found

NRC's network SOC currently meets operational security requirements stipulated in the ITISS contract. However, the current contract is not optimized to meet NRC's needs, and opportunities exist to improve the SOC's range of capabilities and coordination with other NRC stakeholders.

Performance-based contracting is the preferred approach to Federal contracting. In this approach, the Government customer defines its needs in terms of the results it is seeking, in addition to metrics for measuring contractor performance, rather than describing the process that the contractor will use.

NRC staff described several areas in which the SOC does not meet agency needs, including proactive analysis and timely, detailed reports. This occurs because although the contract performance criteria are aligned with National Institute of Standards and Technology and NRC internal guidance, the contract does not clearly define SOC performance goals and metrics that can be used to determine whether agency needs are being met.

Additionally, SOC staff and NRC stakeholders expressed differing expectations of SOC roles and responsibilities. This occurs due to a lack of adequate definitions in agency policies and undifferentiated functional descriptions between different entities responsible for securing NRC's network.

What We Recommend

This report makes recommendations to improve SOC performance and capabilities through better definitions of contract requirements and improving clarity in organizational roles and responsibilities. Agency management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ITISS	Information Technology Infrastructure Support Services
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
SOC	Security Operations Center

I. BACKGROUND

The U.S. Nuclear Regulatory Commission's (NRC) network Security Operations Center (SOC) secures the agency's network infrastructure and monitors the network for suspicious activity. To support this mission, the SOC uses automated security tools, analyzes network activity data, and participates in incident response efforts. Robust SOC capabilities are particularly crucial given the sensitivity of unclassified information processed by NRC's network,[1] and the increasing volume of attacks carried out against Federal Government computer systems.[2]

NRC's SOC is staffed primarily by contractors working under the Information Technology Infrastructure Support Services (ITISS) contract. This contract provides NRC a broad range of network operations and support services that include security as well as desktop computing, printing, and mobile devices. The ITISS contract took effect in February 2011 and will expire in May 2017. Its ceiling is approximately $252.1 million. However, as of November 2015, NRC projects contract requirements may exceed the ceiling by approximately $10.6 million. NRC staff anticipate that the ITISS contract will reach the ceiling by December 2016, and are developing a solicitation for a new contract that would take effect when the contract expires.

NRC staff from the Office of the Chief Information Officer Operations Division oversee and work with SOC contractor staff. The SOC supports NRC's Information Security Directorate by providing information on network security incidents[3] and data required for Federal Information Security Modernization Act compliance reporting to the Office of Management and Budget. In addition, the SOC provides information to investigators from NRC's Office of the Inspector General.

[1] Classified and Safeguards Information processing is not permitted on NRC's main information technology infrastructure system.

[2] From Fiscal Year 2013 to Fiscal Year 2014, NRC experienced an 18-percent increase in computer security incidents reported to the Department of Homeland Security. This exceeds Federal Governmentwide trend data, which show an increase of approximately 9.7 percent during the same period. These incidents include unauthorized access; malicious code; social engineering; policy violations; and scans, probes, and other access attempts.

[3] The Information Security Directorate collects data on NRC network security incidents and reports it to the Department of Homeland Security's U.S. Computer Emergency Readiness Team.

II. OBJECTIVE

The audit objective was to determine whether NRC's network SOC meets its operational requirements, and to assess the effectiveness of SOC coordination with organizations that have a role in securing NRC's network. The report appendix describes the audit's scope and methodology.

III. FINDINGS

NRC's network SOC provides a range of capabilities to protect the agency against cybersecurity threats, and contractors who help run the SOC are meeting security operational requirements stipulated in NRC's primary information technology support contract. However, auditors found that SOC capabilities could be improved through better definition of contractual requirements. Additionally, auditors found that SOC coordination with other NRC stakeholders could benefit from a clearer definition of organizational roles and responsibilities.

A. Current Contract Limits Needed Capabilities

Federal internal control and procurement guidance emphasizes the importance of contracts delivering goods and services that meet agency needs. However, NRC's current ITISS contract does not provide some needed SOC capabilities. This occurs because the ITISS contract does not clearly define SOC performance objectives or functional requirements. As a result, NRC's SOC is not optimized to protect the agency's network in the current cyber threat environment.

What Is Required

Contracts Should Help Meet Agency Needs

Federal and NRC guidance asserts that contracts for goods and services should deliver what the agency needs. For example, the U.S. Government Accountability Office *Standards for Internal Control in the Federal Government*[4] states that clear communication of agency requirements is an important internal control responsibility of management relative to acquisitions contracts. Management may contract with a service organization to perform an organizational role. Nevertheless, management must communicate the expectations, responsibilities, and authorities for that role to the contractor, and enforce accountability.

Additionally, performance-based contracting is the preferred approach to Federal contracting. In performance-based contracting, the Government customer defines the results it is seeking, rather than the process the contractor will use. The Government customer also determines standards for measuring contractor performance. To define the desired results, an agency should analyze its needs. Requirements can then be broken down into clear functions and tasks. Staffing needs and performance metrics are, in turn, based on these requirements.

Lastly, NRC Management Directive 11.1, *NRC Acquisition of Supplies and Services*, states that acquisition of supplies and services to meet NRC's mission should be effective. This internal guidance reinforces the *Federal Acquisition Regulation*, which is intended to ensure that products or services will satisfy Government customers (principally end-users and line managers) in terms of cost, quality, and timeliness of the delivered product or service.

What We Found

ITISS Contract Does Not Deliver Some Needed SOC Capabilities

NRC staff described ways that the SOC does not meet agency needs.

[4] GAO-14-704G, *Standards for Internal Control in the Federal Government*, September 2014.

- NRC staff with an interest in SOC activities unanimously wished for proactive analysis and research into anomalies logged by network monitoring tools. However, the SOC has relatively few highly skilled SOC analysts. Further, these analysts are not solely dedicated to the SOC and can be assigned to other information technology support tasks instead of focusing on needed indepth analysis.

- NRC staff also identified the need for enhanced network monitoring.

- NRC staff stated reports from the SOC are not timely or lack detail needed by NRC stakeholders.

Recognizing these shortcomings, NRC staff has worked with the ITISS contractor to implement measures that enhance SOC activities within the contract terms. For example, the contractor has trained Network Operations Center staff to support monitoring of the SOC tools. NRC has acquired new technologies to assist the SOC in digesting the information produced by the automated tools. In addition, NRC staff report performing analysis to supplement contractor staff efforts.

Why This Occurred

ITISS Contract Does Not Clearly Define SOC Performance Objectives and Functional Requirements

Although performance-based contracting allows a contractor to determine the best way to meet performance goals, the NRC ITISS contract does not clearly define performance goals for the SOC. The ITISS contract addresses network security goals broadly with a stated purpose of "establish[ing] and maintain[ing] an effective security posture for NRC information and information systems." However, specific contractual service requirements are limited to managing a few mitigating controls such as anti-virus, anti-malware, and anti-spam across the network from personal computing devices to network infrastructure devices, servers, and systems. Further, although the contract states that the contractor

"shall staff and operate a facility to proactively monitor, avoid, report, mitigate, and respond to [information technology] security incidents," the

network security and monitoring activities are listed without describing performance expectations.

Because there are no performance goals for the SOC, the contract also contains no SOC-specific performance metrics. There is a single metric for the relevant section of the contract—i.e., a specific timeframe for updating security software on individual computers after they connect to the NRC network. The timeframe allows for measurable performance results, but the task is not necessarily a SOC activity. No metrics were included for monitoring tasks such as reviewing logs or evaluating events.

Additionally, NRC management did not perform a detailed analysis of SOC functions to develop service level agreements for the contract. One NRC staff member stated that this was "somewhat deliberate," because of the challenge of measuring prevention.[5] Another NRC staff member observed that clearly delineating duties and other requirements contributes to accountability, but this was not done to create the current contract structure.

Absent a definition of SOC functions and tasks, contract performance criteria are "aligned with" National Institute of Standards and Technology and NRC internal guidance. However, there are no expectations or "hooks" for NRC to ensure agency needs are met. For example,

- Contractor staffing levels for network operations security are provided in the contract as information about level of effort, but are not intended to form a requirement.

- The contractor is expected to provide reports of security monitoring, but the contract is vague regarding content, timing, or recipients of those reports.

[5] Compliance with security requirements and implementation of best practices does not guarantee an organization's ability to prevent network security compromises. Other approaches, such as measuring incident response times and denial of attempted intrusions, can be used to assess the effectiveness of an organization's network security program. Additionally, prioritizing network assets based on mission significance can help an organization develop risk-based security goals and performance measures.

- The contract states that procedures shall be updated "as necessary," but "necessary" is undefined and there is no requirement for periodic review to determine whether updates are necessary.

- The contract states the contractor shall "gather and analyze statistical security information" and "maximize the value of the information provided to the NRC by correlating related incidents." However, there is no specific description of who will do this analysis, how often, or what form the information will take.

Why This Is Important

SOC Not Optimized To Protect Agency Network

The SOC as shaped by the ITISS contract is not optimized to meet NRC's needs. NRC has limited influence over SOC capabilities at a time when the agency must adapt to both internal and external pressures in the SOC's current operating environment. A dynamic cyber threat environment demands a high-performing SOC. The sophistication and frequency of malicious activity targeting NRC has increased. These forces, combined with the need for NRC users to stay connected with stakeholders and partners through the Internet, makes effective information security a critical capability. Security strategies must be adjusted and enhanced over time to work against budget and personnel constraints and prevent capability gaps.

Moreover, NRC's Project Aim 2020 report has articulated the imperative for more efficient resource management across the agency.[6] According to this report, effectiveness, efficiency, and performance must improve for the agency to continue to succeed in the future. Given its key role in securing information systems, the SOC must be as effective as possible to

[6] Project Aim 2020 is an NRC initiative to improve agency efficiency, driven largely by the need to align agency structure and processes with numerous fact-of-life changes. NRC has grown significantly to enhance security and incident response, and to prepare for formerly projected growth in the use of nuclear power in the United States. The forecasted growth did not occur because of changes in the nuclear industry that resulted in fewer nuclear facilities and the early closure of existing plants. In addition, resources are likely to be constrained Governmentwide in the future.

support NRC's mission while also making best use of the limited resources available.

Recommendations

OIG recommends that the Executive Director for Operations

1. Revise information technology service contract requirements to include SOC-specific performance objectives.

2. Revise information technology service contract requirements to define SOC functional requirements.

B. SOC and Stakeholder Relationships Need Clearer Definition

Effective operations require clear roles and responsibilities within an organization. However, NRC stakeholders express differing expectations regarding SOC roles and responsibilities. This occurs because the SOC's role in supporting NRC stakeholders is not adequately defined in agency policy or in the contract. As a result, staff and contractor resources may not be used as efficiently as possible.

What Is Required

Organizational Roles and Responsibilities Should Be Defined

The U.S. Government Accountability Office *Standards for Internal Control in the Federal Government* states that management should develop an organizational structure with an understanding of overall responsibilities. These responsibilities should be assigned to discrete units that enable the organization to operate in an efficient and effective manner. Furthermore, management should consider how organizational units interact in order to fulfill their overall responsibilities.

In addition to this Government internal control guidance, private sector best practices for creating a SOC emphasize that an organization should define its SOC in terms of mission, charter, objectives, and responsibilities as a precondition for effective procedural guidance and staffing.

What We Found

Expectations of SOC Vary Among SOC Staff and Stakeholders

Auditors found that SOC staff and NRC stakeholders express differing expectations of SOC roles and responsibilities. For example, some stakeholders expect more detailed analysis from the SOC, and raised concerns about the timeliness of data provided for purposes such as quarterly Federal Information Security Modernization Act reporting. Conversely, SOC staff raised concerns about data requests and the level of support required by stakeholders who have access to the SOC's network analytic tools.[7] Additionally, stakeholders expect that roles could be better defined to clarify responsibilities such as, for example, who should notify affected users when an incident occurs.

Why This Occurred

SOC Roles and Responsibilities Lack Adequate Policy and Contractual Definition

Differing expectations of SOC roles and responsibilities reflect inadequate definition in agency policy and functional descriptions, and in the ITISS contract. For example, an organization within the Information Security Directorate that is responsible for network security monitoring shares a functional description with a counterpart organization in the Office of the Chief Information Officer that is responsible for managing the SOC. NRC created these two organizations in 2007 to differentiate computer security oversight from operations, yet failed at the time to differentiate the new organizations' respective roles and responsibilities. This lack of clarity is reflected in the current ITISS contract, which contains generic language regarding support for stakeholder information requests but does not provide detailed guidance on the nature and extent of support required.

[7] Some NRC stakeholders have access to SOC analytic tools and, in the past, have received training from SOC staff on how to use these tools. Nevertheless, some stakeholders lack the skills required to effectively use these tools and, consequently, rely on SOC staff to analyze network data for them.

Why This Is Important

Clear Organizational Roles and Responsibilities Support Efficiency

Without a clear definition of organizational roles and responsibilities, successful coordination of SOC activities with NRC stakeholders depends heavily on interpersonal relationships. Through positive rapport, staff can negotiate differing interpretations of unclear guidance. However, when relationships and communications fail, this can result in duplication of effort, redundant followup tasks, and extra meetings to discuss responsibilities and clarify expectations. Further, contractor staff who run the SOC need clear guidance on their stakeholder support obligations to prioritize work and make most effective use of limited resources.

Recommendations

OIG recommends that the Executive Director for Operations

3. Define in policy SOC functions and support obligations to NRC stakeholders, with emphasis on information reporting and technical support requirements.

4. Revise the information technology services contract to align with agency policy defining SOC functions and support obligations to NRC stakeholders.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Revise information technology service contract requirements to include SOC-specific performance objectives.

2. Revise information technology service contract requirements to define SOC functional requirements.

3. Define in policy SOC functions and support obligations to NRC stakeholders, with emphasis on information reporting and technical support requirements.

4. Revise the information technology services contract to align with agency policy defining SOC functions and support obligations to NRC stakeholders.

V. AGENCY COMMENTS

An exit conference was held with the agency on January 5, 2016. Prior to this meeting, after reviewing a discussion draft, agency management provided comments that have been incorporated into this report, as appropriate. As a result, 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 NRC's SOC meets its operational requirements, and to assess the effectiveness of SOC coordination with organizations that have a role in securing NRC's network.

Scope

This audit focused on SOC functions to determine whether SOC operational capabilities meet agency needs in support of network and information security. OIG conducted this performance audit from July 2015 to November 2015 at NRC headquarters (Rockville, MD). Internal controls related to the audit objectives were reviewed and analyzed. Throughout the audit, auditors were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

OIG reviewed relevant criteria for this audit, including National Institute of Standards and Technology Special Publication 800-series guidance on computer security; U.S. Computer Emergency Readiness Team guidance; industry best practices, such as MITRE Corporation, *Ten Strategies of a World-Class Security Operations Center*; the U.S. Government Accountability Office, *Standards for Internal Control in the Federal Government*; NRC Management Directive 11.1, *NRC Acquisition of Supplies and Services*; and the Office of Management and Budget, *Best Practices for Performance-Based Contracting*.

To understand how NRC manages network security activities, OIG reviewed additional internal documents. The ITISS contract Statement of Work, for example, presents NRC's expectations for the contractor running the SOC. Additionally, NRC guidance such as the Information Technology Infrastructure Security Plan, SOC operating procedures, and

Information Security Directorate standards provide context for SOC functions and activities.

OIG interviewed NRC staff and management to gain an understanding of roles and responsibilities as they relate to how the SOC functions and coordinates with other organizations responsible for NRC's network security. Auditors interviewed NRC staff from the Office of the Chief Information Officer and contractor staff in the SOC. OIG auditors also attended a briefing and demonstration in the SOC.

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.

The audit was conducted by Beth Serepca, Team Leader; Paul Rades, Audit Manager; Amy Hardin, Senior Auditor; Ebaide Esoimeme, Auditor, and Andy Pham, Student Analyst.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-270-2787

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.