OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018

OIG-19-A-08

April 2, 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

April 2, 2019

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF FISMA 2014 FOR FISCAL YEAR 2018 (OIG-19-A-08)

The Office of the Inspector General (OIG) contracted RMA Associates, LLC to conduct an independent evaluation of NRC's Implementation of the *Federal Information Security Modernization Act of 2014*. Attached is OIG's evaluation report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2018*. The objective of this evaluation was to conduct an independent assessment of the NRC's FISMA implementation for Fiscal Year 2018.

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

OIG found that the NRC's information security program and practices were generally effective for the period October 1, 2017, through September 30, 2018. However, the evaluation identified areas that need improvement. Specifically, improvements can be made in the following areas (1) management of non-standard software, (2) efforts to remove unsupported software vulnerabilities, and (3) mitigating high-risk vulnerabilities on NRC networks.

Please provide information on actions taken or planned on each of the recommendation(s) within 30 calendar 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 evaluation. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Eric Rivera, Team Leader, at (301) 415-7032.

Attachment: As stated

Office of the Inspector General

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

OIG-19-A-08
April 2, 2019

Results in Brief

Why We Did This Review

On December 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (FISMA 2014), reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor.

FISMA 2014 requires organizations to adopt a risk-based, life-cycle approach to improving information security that includes annual security program reviews and independent evaluations.

The objective of this evaluation was to conduct an independent assessment of the NRC's FISMA implementation for Fiscal Year 2018.

Independent Evaluation of NRC's Implementation of FISMA 2014 for FY 2018

What We Found

OIG found that the NRC's information security program and practices were generally effective for the period October 1, 2017, through September 30, 2018. However, the evaluation identified information technology security program areas that need improvement. Specifically, improvements can be made in the following areas (1) management of non-standard use software, (2) efforts to remove unsupported software vulnerabilities, and (3) mitigating high-risk vulnerabilities on NRC networks.

What We Recommend

This evaluation presents six recommendations to improve NRC's implementation of FISMA to strengthen information technology security. Management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ATO	Authority to Operate
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CRDB	Cybersecurity Risk Dashboard
CVSS	Common Vulnerability Scoring System
ERM	Enterprise Risk Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity Credential and Access Management
IDS	Intrusion Detection System
IG	Inspector General
IM	Information Management
IR	Incident Response
ISCM	Information Security Continuous Monitoring
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plans of Actions and Milestones
RMA	RMA Associates, LLC
SP	Special Publication
TIC	Trusted Internet Connection

I. INTRODUCTION

RMA Associates, LLC (RMA) performed this engagement in accordance with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation.

II. SUMMARY EVALUATION RESULTS

Consistent with applicable *Federal Information Security Modernization Act of 2014 (FISMA 2014)* requirements, the Office of Management and Budget (OMB) policy and guidance, and the National Institute of Standards and Technology (NIST) standards and guidelines, the U.S. Nuclear Regulatory Commission's (NRC) information security program and practices were established. We found the NRC's information security program and practices were generally effective for the period October 1, 2017, through September 30, 2018.

III. BACKGROUND

Federal Information Security Modernization Act of 2014

On December 18, 2014, the President signed the Federal Information Security Modernization Act of 2014 (FISMA 2014), reforming the Federal Information Security Management Act of 2002 (FISMA). FISMA 2014 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of the effectiveness of the information security policies, procedures, and practices of the agency. FISMA 2014 requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. Office of Management and Budget (OMB) memorandum M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements, dated October 16, 2017, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

FISMA 2014, along with the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* (known as the *Clinger-Cohen Act*), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, OMB, through Circular No. A-130, "Managing Federal Information as a Strategic Resource," requires executive agencies within the Federal government to

- Plan for information security;
- Ensure appropriate officials are assigned information security responsibility;
- Periodically review the security controls in their information systems; and
- Authorize system processing prior to operations and periodically after that.

These management responsibilities presume responsible agency officials understand the risks and other factors that could adversely affect their missions. Moreover, these officials must understand the current status of their security programs and security controls, planned or in place, to protect their information and systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information.

FISMA 2014 requires organizations to adopt a risk-based, life-cycle approach to improving information security that includes annual security program reviews and independent evaluations. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal systems. NIST also developed an integrated Risk Management Framework that effectively brings together all FISMA 2014-related security standards and guidance to promote the development of comprehensive and balanced information security programs by agencies.

FISMA 2014 states that NIST identifies security requirements for information security for government agencies and its contractors, including

- Security assessments conducted as part of an information system security authorization or re-authorization process; and
- Continuous monitoring activities, to include testing and evaluating the information system as part of the ongoing system development life cycle process (provided the testing and evaluation results are current and relevant to the determination of security control effectiveness).

FISMA 2014 Reporting Metrics

RMA evaluated the effectiveness of the information security program and practices on a maturity model spectrum, in which the foundation levels ensure the development of sound policies and procedures. The FISMA 2014 Reporting Metrics classify information security program and practices into five maturity model levels: Ad Hoc, Defined, Consistently

Implemented, Managed and Measurable, and Optimized. Within the context of the maturity model, Level 4, Managed and Measurable, represents an effective level of security.

Table 1: Maturity Level Description

Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies were not formalized; activities were performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies were formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies were consistently implemented, but quantitative and qualitative effectiveness measures were lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies were collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies were fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

This report reflects the results of our testing of NRC's information security program and practices. The FISMA 2014 Reporting Metrics were aligned with the five Cybersecurity Framework security function areas (key performance areas) as follows

- **Identify: Risk Management** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify function are foundational for effective use of the Cybersecurity Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

- **Protect: Configuration Management, Identity and Access Management, Data Protection and Privacy[1], and Security Training**

[1] The data protection and privacy domain was added to the annual Inspector General FISMA 2014 reporting metrics in 2018 as part of the Protect function. This domain includes metrics for assessing the effectiveness of the agency's privacy program, security controls to protect personally identifiable information, enhanced network defenses, responses to data breaches, and privacy awareness training.

– Develop and implement appropriate safeguards to ensure the delivery of critical services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

- **Detect: Information Security Continuous Monitoring** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables the timely discovery of cybersecurity events.

- **Respond: Incident Response** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond function supports the ability to contain the impact of a potential cybersecurity incident.

- **Recover: Contingency Planning** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

IV. OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this evaluation was to conduct an independent assessment of the NRC's FISMA implementation for FY 2018.

Scope

RMA conducted this evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation. The evaluation was designed to determine whether the NRC implemented security controls for selected information systems in support of FISMA 2014. Our evaluation was conducted between August 16, 2018 and November 30, 2018. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators considered the possibility of fraud, waste, and/or abuse in the program.

Methodology

The overall strategy of our evaluation considered *NIST Special Publication (SP) 800-53A, Guide for Assessing Security Controls in Federal Information Systems and Organizations, NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations,* and the FISMA 2014[2] guidance from CIGIE, OMB, and Department of Homeland Security. Our testing procedures were developed from NIST SP 800-53A[3].

RMA conducted interviews with NRC officials and reviewed legal and regulatory requirements stipulated in FISMA 2014. We also examined documents supporting the information security program and practices. Where appropriate, we compared documents, such as NRC's information

[2] OMB, DHS, and CIGIE developed the FISMA 2014 Reporting Metrics in consultation with the Federal Chief Information Officers Council. The 8 FISMA 2014 Metric Domains were aligned with the 5 functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover as defined in the NIST Framework for Improving Critical Infrastructure Cybersecurity.

[3] SP 800-53A provides (i) guidelines for building effective security assessment plans and privacy assessment plans; and (ii) a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in information systems and organizations supporting the executive agencies of the Federal government.

technology (IT) policies and procedures, to requirements stipulated in NIST SP. Also, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

V. CRITERIA

RMA focused our FISMA 2014 evaluation approach on Federal information security guidelines developed by NRC, NIST, and OMB. NIST SPs provide guidelines that were considered essential to the development and implementation of NRC's security programs. The following is a listing of the criteria used in the performance of the fiscal year (FY) 2018 FISMA 2014 evaluation.

NRC

- MD 1.1, *NRC Management Directives System, Volume 1: Management Directives, March 25, 2016, DT-17-100*
- MD 2.3, *Telecommunications, Volume 2: Information Technology, October 12, 2011, DT-17-101*
- MD 2.6, *Information Technology Infrastructure, Volume 2: Information Technology, March 7, 2005, DT-05-04*
- MD 2.7, *Personal Use of Information Technology, Volume 2: Information Technology, July 28, 2006, DT-06-15*
- MD 2.8, *Integrated Information Technology/Information Management (IT/IM) Governance Framework, Volume 2: Information Technology, February 24, 2016, DT-17-102*
- MD 3.2, *Privacy Act, Volume 3: Information Management, July 10, 2014, DT-17-104*
- MD 3.16, *NRC Announcement Program, Volume 3: Information Management, June 2, 2016, DT-17-113*
- MD 4.4, *Enterprise Risk Management and Internal Control, Volume 4: Financial Management, December 14, 2017, DT-17-18*
- MD 6.1, *Resolution and Followup of Audit Recommendations, Volume 6: Internal Management, July 3, 2014, DT-17-137*
- MD 6.2, *Continuity of Operations Program, Volume 6: Internal Management, February 20, 2013, DT-17-138*
- MD 10.37, *Position Evaluation and Benchmarks, Volume 10: Personnel Management, Part 2: Position Evaluation and Management, Pay Administration, and Leave, September 23, 2016, DT-17-193*
- MD 10.77, *Employee Development and Training, Volume 10: Personnel Management, Part 3: Performance Appraisals, Awards, and Training, January 4, 2016, DT-17-205*

- MD 10.166, *Telework, Volume 10: Personnel Management, Part 7: General Personnel Management Provisions, July 13, 2017, DT-17-219*
- MD 11.1, *NRC Acquisition of Supplies and Services, Volume 11: Procurement, May 9, 2014, DT-17-220*
- MD 12.0, *Glossary of Security Terms, Volume 12: Security, July 1, 2014, DT-17-224*
- MD 12.1, *NRC Facility Security Program, Volume 12: Security, September 28, 2016, DT-17-225*
- MD 12.3, *NRC Personnel Security Program, Volume 12: Security, October 8, 2013, DT-17-227*
- MD 12.4, *NRC Communications Security (COMSEC) Program, Volume 12: Security, April 8, 2016*
- MD 12.5, *NRC Cybersecurity Program, Volume 12: Security, November 2, 2017, DT-17-16*

NIST Federal Information Processing Standards (FIPS) and SP

- FIPS Publication 199*, Standards for Security Categorization of Federal Information, and Information Systems*
- FIPS Publication 200*, Minimum Security Requirements for Federal Information, and Information Systems*
- FIPS Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
- NIST SP 800-40, *Guide to Enterprise Patch Management Technologies*
- NIST SP 800-50, *Building an Information Technology Security Awareness, and Training Program*
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
- NIST SP 800-60, *Guide for Mapping Types of Information, and Information Systems to Security Categories*
- NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*
- NIST SP 800-63, *Digital Identity Guidelines*
- NIST SP 800-83, *Guide to Malware Prevention and Handling*
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems, and Organizations*
- NIST SP 800-181, *NICE Cybersecurity Workforce Framework*

OMB Policy Directives

- OMB Memorandum M-18-02, *Fiscal Year* (*FY) 2017-2018 Guidance on Federal-Information Security and Privacy Management Requirements*
- OMB Memorandum M-17-09, *FY 2017 Management of Federal High-Value Assets*
- OMB Memorandum M-16-04, *FY 2016 Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*
- OMB Memorandum M-14-03, *FY 2014 Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-08-05, *Fiscal Year 2008 Implementation of Trusted Internet Connections (TIC)*
- OMB Memorandum M-04-25, *Fiscal Year 2004 Reporting Instructions for the Federal Information Security Management Act*
- OMB Circular A-130*, Managing Information as a Strategic Resource*

VI. EVALUATION RESULTS

Evaluation Summary

This report constitutes our independent evaluation of NRC's IT security program and practices required by FISMA 2014, based on the *FY 2018 Inspector General (IG) FISMA Reporting Metrics* that use the maturity model indicators. IGs assess the effectiveness of information security programs on a maturity model spectrum in which the foundation levels ensure agencies develop sound policies and procedures and the advanced levels capture the extent to which agencies institutionalize those policies and procedures. This evaluation reflects the NRC's information security program's status based on the completion of FY 2018 FISMA 2014 testing.

NRC relies extensively on IT resources to accomplish its mission. The IT systems and resources strengthen management and monitoring of licensing and regulations of the Nation's civilian use of radioactive materials. Improving the overall management and security of IT resources and stakeholder information must be a top priority for NRC. While technology enables and enhances the ability to share information instantaneously among stakeholders through computers and networks, it also makes an organization's networks and IT resources vulnerable to malicious activity and exploitation by internal and external sources.

What We Found

The overall FY 2018 FISMA 2014 maturity score for NRC's security program is Managed and Measurable. The NRC maturity score for FY 2017 was also Managed and Measurable. However, NRC continues to take positive steps for improving its security posture. We noted some improvements in the component scoring. Under the Identify function area's Risk Management domain, NRC enhanced its Plans of Action and Milestones (POA&Ms) process, thereby increasing its maturity rating from Managed and Measurable to Optimized. Also, under the Protect function area's Configuration Management domain, NRC increased its flaw remediation processes maturity level from Defined to Consistently Implemented.

We identified three opportunities for improvement in the following areas

- Management of non-standard use software.
- Removing unsupported software vulnerabilities.
- Mitigating high-risk vulnerabilities on NRC's networks.

NRC must continue to be ahead of the constantly changing security threats. Senior management must be vigilant to maintain a secure and sustainable security posture and must consistently implement policies based on changing security risks.

What We Reviewed

Within each metric domain, we reviewed IT controls, policies and procedures, and current processes to determine whether they operated as intended and as specified by the FY 2018 IG FISMA 2014 Metrics. In assessing the adequacy of compliance or effectiveness of implemented security controls, RMA did not rely only on a review of NRC's policies and procedures or management's assertions regarding the implementation of control. Such evidence does not by itself constitute sufficient, appropriate evidence demonstrating the effectiveness of an implemented security control. We inspected evidence to determine whether each security control was satisfied. If evidence other than policies and procedures was not available, we evaluated whether the lack of sufficient, appropriate evidence was due to security control deficiencies or other program weaknesses and whether the lack of sufficient, relevant evidence may be the basis for evaluation findings.

Our tests included interviews with appropriate management, supervisory, and staff personnel; inspection of NRC's documents and records; and observation of NRC's activities and operations.

Table 2: Testing Method and Test Descriptions

Testing Method	Test Descriptions
Interview	Interviewed relevant personnel with the knowledge and experience of the performance and application of the related security control activity. This testing included collecting information via in-person meetings, telephone calls, or e-mails.
Observation	Observed relevant processes or procedures during fieldwork. Observation included walkthroughs; witnessing the performance of controls; or evidence of control performance with appropriate personnel, systems, or locations relevant to the performance of security control policies and procedures.
Inspection	Inspected relevant records. This testing included reviewing documents, system configurations and settings, or the existence of attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing items to supporting documents, system documentation, or processes.

Function 1: Identify – Risk Management

Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization. This includes senior leaders providing the strategic vision and top-level goals and objectives for the organization, mid-level leaders planning and managing projects, and individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization.

We determined NRC's Risk Management program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were operating effectively. The first step in risk management process is to account for all of an organization's software and hardware assets. NRC maintained an organization-wide hardware inventory system that controlled and accounted for all of NRC's network devices. NRC used appliances and software tools to collect information of all network-attached devices including software, version numbers, and quantities. NRC employed Management Directive (MD) 4.4, *Enterprise Risk Management (ERM) and Internal Control* and Directive Handbook, *Enterprise Risk Management and Internal Control*, which provided the foundation of NRC's ERM governance and communication structure. NRC has integrated ERM to address the full spectrum of the agency's risk portfolio across all its organizational and business activities. MD 4.4 incorporated ERM into the comprehensive performance management and internal control frameworks to facilitate the improvement of NRC's mission delivery, reduction of costs, and focus on corrective actions of its key enterprise risks. NRC monitored its risk profiles through dynamic reporting mechanisms, such as its Cybersecurity Risk Dashboard (CRDB) and Cybersecurity Daily Reports, to gain a fully integrated, prioritized, enterprise-wide view of its organizational risks.

Although we found NRC's Risk Management program effective, we noted an area of improvement for NRC's management of non-standard software.

A. NRC's Efforts to Monitor and Remove Unauthorized Non-Standard Software can be Improved

NRC policies prohibit the use of non-standard software[4] on NRC's devices. NRC MD 2.7, *Personal Use of Information Technology Handbook 2.7*, defines "personal use" and provides guidance on the use of agency information technology for personal reasons. MD 2.7 describes personal use as the following:

- An employee's activity conducted for purposes other than accomplishing official or otherwise authorized action. NRC employees are expressly prohibited from using agency information technology to maintain or support a personal, private business.

- The policy established herein allows NRC employees to use agency information technology for personal reasons when such use involves minimal or no additional expense to the Government, is performed on the employee's non-work time, does not interfere with NRC's mission or operation, does not violate the Standards of Ethical Conduct for Employees of the Executive Branch regulations, and is not otherwise prohibited by law.

Although non-standard software is not permitted, NRC allowed personnel to request the use of non-standard software by completing a request form. The software should be inspected for security flaws and approved by the Information System Security Officer before installation.

We found 57 instances of non-standard software on the NRC's network. However, this software was not supported by evidence of approval or inspected for security flaws. Some of the non-standard software included income tax preparation software; recording and video editing software; file management for scanners; and an Outlook add-on for sorting emails. The prior year editions of tax preparation software may be obsolete and not used.

[4] Non-standard software is software not included with the standard image and set of applications.

After the non-standard software was initially installed, vulnerabilities may appear in the software. For example, we found unpatched versions of approved smart phone management software that contained high-risk vulnerabilities. NRC did not monitor non-standard software to determine whether the software was still in use and whether the software contained known vulnerabilities.

Without properly inspected and approved non-standard software on NRC's network, there is an increased likelihood of information security breaches due to unpatched vulnerabilities and malicious codes.

Recommendations

We recommend the Executive Director for Operations

1) Develop and implement a process to remove all non-standard software that has not been approved by an authorized agency official.

2) Implement a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network.

3) Monitor the approved installed software on NRC's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found.

4) Develop and establish processes and procedures to govern the installation of non-standard software, including processes and procedures on determining impact to agency operations or cybersecurity.

Function 2A: Protect – Configuration Management

Configuration Management comprises a collection of activities focused on establishing and maintaining the integrity of software and hardware systems, through control of the processes for installing, initializing, changing, and monitoring the configurations of those systems.

Configuration management controls security features for all hardware, software, and firmware components of an information system and systematically controls changes to that configuration during the system's life cycle. At an organization-wide level, management develops security policies that establish the organization's configuration management process and may determine the configuration settings for the organization. Policy enforcement applications can be used to help administrators define and perform centralized monitoring and enforcement of an organization's security policies. An organization should have configuration management controls to ensure only authorized changes are made to such critical components. At a business process application level, all applications and changes to those applications should go through a formal, documented systems development process that identifies all modifications to the baseline configuration. Also, procedures should ensure no unauthorized software is installed.

We determined NRC's Configuration Management program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were operating effectively.

NRC's policies defined roles and responsibilities at the organizational level for stakeholders involved in information system configuration management. These defined roles were communicated across the organization. NRC developed an organization-wide configuration management plan which included the monitoring system components. NRC monitored system configurations of devices connected to NRC's networks through the use of CRDB dashboards. The dashboards showing configuration information from FISMA systems are updated weekly. NRC's CRDB contained a configuration section displaying a configuration and Continuous Diagnostics and Mitigation (CDM) metrics. NRC executed automated software tools to scan network devices on a routine cycle. NRC reviewed Cybersecurity Daily Reports that included a configuration management section that displayed the top ten (10) remediations and vulnerability scans. NRC's Change Control Board met weekly to review and approve change requests. NRC consistently implemented its Trusted Internet Connection (TIC) approved connections and critical capabilities that it managed internally with TIC 3.0 in its initial process. Additionally, NRC monitored, analyzed, and reported on the qualitative and quantitative

performance measures used to gauge the effectiveness of its configuration management policies and procedures.

Although we found NRC's Configuration Management program effective, we noted two areas of improvement:

B. NRC's Efforts for Removing Unsupported Software Vulnerabilities can be Improved.

OMB Circular No. A-130, *Managing Federal Information as a Strategic Resource*, Appendix I establishes minimum requirements for Federal information programs and assigns Federal agency responsibilities for the security of information and information systems. The Circular explicitly prohibits Federal agencies from the use of unsupported information systems and system components and requires agencies to ensure systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement.

We reviewed NRC's software listing and found 64 instances of unsupported software. Unsupported systems and programs that were no longer fully maintained by the software vendors expose NRC to vulnerabilities that cannot be fully mitigated. Unsupported software allows NRC systems to remain exposed to known vulnerabilities for an extended period of time as the vendor for the known security weaknesses does not update the unsupported software.

NRC relied on endpoint protection[5] to its workstations and felt the end-point protection was sufficient.

Recommendation

We recommend the Executive Director for Operations

5) Implement a process to remove unsupported software from NRC networks.

[5] Endpoint protection is a software approach which helps to identify and manage the users' computers access over a corporate network. This allows the network administrator to restrict certain web site access to specific users in order to maintain and comply with the organization's policies and standards.

C. NRC's Mitigation of High-Risk Vulnerabilities on its Networks can be Improved.

The NIST SP 800-53*, Security and Privacy Controls for Federal Information Systems and Organizations*, Rev 4, Security Control: SI-2, Flaw Remediation, states an organization must "identify information systems affected by announced software flaws, including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hotfixes, and anti-virus signatures."

We reviewed the NRC software list and found 13 high-risk vulnerabilities. We relied on a common and standardized vulnerability scoring system, Common Vulnerability Scoring System (CVSS) Version 3, to rate the severity of vulnerabilities. Using the CVSS Version 3, RMA affixed risk and assessed the implications of the identified risks within the environment. A CVSS score is generated using a combination of factors, such as how complex the attack would be to exploit the vulnerability, whether additional information would be needed to exploit the vulnerability and proximity of the attacker to the target host. High-risk vulnerabilities are software weaknesses that an attacker can exploit and gain direct access to the vulnerability on the target with negligible access impediments or authentication barriers. Known exploits require little skill to perform and may negatively impact the information system's confidentiality, integrity, and availability.

An external attacker would have to traverse NRC's border-firewalls and Intrusion Detection System (IDS) to exploit the vulnerabilities. However, the border-firewalls and IDS would not protect NRC from an insider threat from a rogue employee or contractor. Insiders account for more than 28 percent[6] of all intrusions.

Recommendation

We recommend the Executive Director for Operations

6) Implement a process to mitigate known high-risk vulnerabilities.

[6] Verizon 2018 Data Breach Investigations Report
https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

Function 2B: Protect – Identity and Access Management

Identity and Access Management (ICAM) is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in an IT system. For most systems, identification and authentication are the first line of defense. Identification and authentication are technical measures that prevent unauthorized individuals or processes from entering a system. Identification and authentication are critical building blocks of information security since it is the basis for most types of access control and for establishing user accountability. Access control often requires the system be able to identify and differentiate between users. For example, access control is usually based on least privilege, which refers to granting users only those accesses required to perform their duties. User accountability requires linking activities on a system to specific individuals and, therefore, requires the system to identify users. Systems recognize individuals based on the authentication data the systems receive.

We determined NRC's ICAM program was consistent with the Managed and Measurable level of the maturity model, where security controls were operating effectively. NRC's ICAM program supported the agency's regulatory mission by enabling licensees, stakeholders, and the public to electronically submit documents and data securely. NRC integrated its ICAM strategy and activities with its enterprise architecture and the Federal Identity, Credential, and Access Management segment architecture. NRC's ICAM program provided credential enrollment, issuance, maintenance, and transaction validation services to external and internal users of agency applications. NRC ensured access agreements for individuals were completed prior to access being granted to systems and were consistently maintained. ICAM supported the agency's facility security program through issuance and maintenance of NRC Personal Identity Verification cards which provide a standardized credential for personnel identification, building access, and network access for employees and contractors. The Personal Identity Verification card authenticates the individual and authorizes entry into an area relative to the access rights of the individual. ICAM supported the agency's information security program by ensuring only persons with approval from Personnel Security were given credentials for access to networked information. NRC used a fully automated account provision process for its non-privileged user accounts and integrated personal security system and

badging system. NRC required all privileged user accounts be approved by the Change Control Board, and extensive project role-based access control settings were configured for privileged user accounts for separation of permissions. ICAM credentials were used agency-wide by applications requiring strong user authentication, digital signature, and user-to-user encryption to meet agency security requirements.

Function 2C: Protect – Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and disclosure to protect personal privacy and proprietary information. Individual trust in the privacy and security of PII is a foundation of trust in government. PII can range from an individual's name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability. Organizations must identify and protect PII located within an organization's environment, assign PII impact levels, and select safeguards.

We determined NRC's Data Protection and Privacy program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were operating effectively. NRC is committed to Data Protection and Privacy. NRC established and maintained a privacy program to provide development and maintenance of privacy controls. The program includes a dedicated staff headed by a Senior Agency Official for Privacy. Further, the privacy personnel worked with IT staff and other stakeholders as needed for security of sensitive data. NRC implemented annual privacy training and has a privacy breach response plan in place.

NRC performed biannual exercises in FY 2018 to test the effectiveness of its data exfiltration PII out of NRC's networks. NRC performed tests in the Second Quarter and Fourth Quarter of FY 2018, using those test results and lessons learned from prior tests to improve privacy controls. NRC routinely monitored inbound and outbound network traffic to ensure security controls were in place for protecting PII. Additionally, NRC

measured the effectiveness of its privacy awareness training program by performing targeted phishing exercises for those with responsibility for protecting PII and obtaining feedback on the content of the training. Furthermore, NRC used dashboards to display the completion of its privacy training and to display privacy risk incidents. NRC made updates to its program based on statutes and regulations; mission, programs, and business process considerations; information system requirements; and results from monitoring and auditing. NRC monitored completion of its privacy training on its Human Capital Dashboard, which was updated weekly.

Function 2D: Protect – Security Training

A successful IT security program consists of 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program. Security awareness and training should be focused on the organization's entire user population. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program.

An awareness and training program is crucial as it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise.

We determined NRC's Security Training program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were operating effectively. NRC defined and appropriately communicated the roles and responsibilities of all the stakeholders involved in its Security Training program. NRC issued its "NRC Cybersecurity Training and Awareness Review and Action Plan," which assessed its security training and awareness program in order to identify areas of improvement and create a plan to improve. Although NRC's overall security training completion was 94.5%, which fell short of the 96%

target, NRC's role-based security training completion exceeded the target goal at 97%. NRC's MD 12.5 requires extra training annually for those with cybersecurity roles, such as system owners, senior executives, administrators, IT managers, and system architects. The specialized training was tailored to the specific needs of each role and position. NRC also continuously monitored compliance of its training program through its CRDB, which can identify compliance by office and have the capability to drill down to each personnel through the Office of the Chief Human Capital Officer. In addition to tracking the overall compliance of its security training program, point-of-contacts assigned for every office met regularly with Information System Security Officers to continuously document all aspects related to security training. NRC performed quarterly targeted phishing exercises to measure the effectiveness of its Security Training program. Results from phishing campaigns were also incorporated into the CRDB.

Furthermore, NRC hosted *HACK2018: Security from the Doorstep to the Desktop* which aimed to increase users' awareness of potential threats stemming from their activities and behavior at work and at home. The HACK event was open to all NRC staff, contractors, and guests and featured external speakers who are experts in the field of cybersecurity. All training materials are available and accessible through NRC's iLearn.

Function 3: Detect – Information Security Continuous Monitoring

Information Security Continuous Monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An ISCM program is established to collect information in accordance with pre-established metrics, using information readily available in part through implemented security controls. Organization officials gather and analyze the data regularly and as often as needed to manage risks appropriate for each organizational tier. This process involves the entire organization, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual systems in support of the organization's core missions and business processes. Subsequently, determinations are made from an organizational perspective on whether to conduct mitigation activities or to reject, transfer, or accept the risk.

We determined NRC's ISCM program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were operating effectively. NRC updated its CRDB to include authorization to operate (ATO) Continuous Monitoring Status Report, business impact analysis, and contingency plan updates for each of NRC's FISMA systems. The CRDB included a drill down function that contained additional detailed information. NRC maintained two (2) separate categories of programmatic POA&Ms, one to address recommendations for the Inspector General and another for issues/findings that cannot be resolved by a single System Owner and for each FISMA system. All NRC FISMA systems were under an ongoing continuous ATO except for Agency-wide Documents Access and Management System, which was still under the periodic ATO. CDM Phase 2 was completed, and CDM Phase 3 is currently in the process of being implemented. CDM dashboard is scheduled to be operational in FY 2019.

Function 4: Respond – Incident Response

Computer security incident response has become an important component of IT programs. Cybersecurity-related attacks have become not only more numerous and diverse, but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is, therefore, necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential. Establishing clear procedures for prioritizing the handling of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. It is also vital to build relationships and establish suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement).

We determined NRC's Incident Response (IR) program was consistent with the Managed and Measurable level of the maturity model, which the FY 2018 IG FISMA Metrics categorized as the maturity level wherein security controls were operating effectively. NRC defined and appropriately communicated the roles and responsibilities of all the stakeholders involved in its IR program. NRC conducted quarterly phishing exercises and utilized lessons learned to continually improve its phishing exercises and IR program. All incidents were tracked and monitored through NRC's incident response database and qualitative and quantitative performance metrics were consistently collected, monitored, and analyzed to measure the effectiveness of its IR activities. Additionally, the CRDB allowed drill down capabilities to incidents and were updated on a monthly basis. NRC utilized firewalls and integrated intrusion prevention system/intrusion detection system (IPS/IDS) were strategically placed internally at the headquarters and each regional office. All logs from protection tools were sent to NRC's security information and event management tool and were monitored by its Security Operations Center. NRC scanned its network every 72 hours and continuously monitored and updated its POA&Ms to track the remediation of identified vulnerabilities. Biannual IR testing was conducted in Second Quarter and Fourth Quarter of FY 2018. NRC used IR exercise after-action reports and lessons learned to continually improve its IR testing and its IR program.

Function 5: Recover – Contingency Planning

Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. Contingency planning generally includes one or more of the following approaches to restore disrupted services

- Restoring information systems using alternate equipment;
- Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
- Recovering information systems operations at an alternate location (usually acceptable for only long-term disruptions or those physically impacting the facility); and
- Implementing appropriate contingency planning controls based on the information system's security impact level.

We determined NRC's Contingency Planning program was consistent with the Consistently Implemented level of the maturity model, which the FY 2018 IG FISMA 2014 Metrics categorized as the maturity level wherein security controls were less than effective. However, our testing found no exceptions and the controls were operating as intended. We concluded the NRC's controls in place were effective.

NRC defined roles and responsibilities at the organizational level for stakeholders involved in Contingency Planning. These defined roles were communicated across the organization. NRC consistently implemented its defined Information System Contingency Plan policies, procedures, and strategies. NRC incorporated the results of NRC and system-level business impact analysis into strategy and planned development efforts consistently. Processes for information system contingency plan testing and exercises were consistently implemented. Information System Contingency Plan testing and exercises were integrated with an evaluation of related plans, such as their incident response plan, Continuity of Operations Plan, and Business Continuity Plan. NRC also employed automated mechanisms to more thoroughly and effectively test system contingency plans through risk management dashboards.

VII. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

1. Develop and implement a process to remove all non-standard software that has not been approved by an authorized agency official.

2. Implement a process to manage non-standard software to ensure the software is properly approved and inspected for security weaknesses before the software is installed on NRC's network.

3. Monitor the approved installed software on NRC's network to determine whether it is still in use, periodically inspect the software for known vulnerabilities, and mitigate any vulnerabilities found.

4. Develop and establish processes and procedures to govern the installation of non-standard software, including processes and procedures on determining impact to agency operations or cybersecurity.

5. Implement a process to remove unsupported software from NRC networks.

6. Implement a process to mitigate known high-risk vulnerabilities.

VIII. AGENCY COMMENTS

An exit conference was held with the agency on December 13, 2018, at which time agency management provided comments on a discussion draft; these comments have been incorporated, as appropriate, into this report. As a result, agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

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.