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

OFFICE OF THE
INSPECTOR GENERAL

April 29, 2020

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 THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019 (OIG-20-A-06)

The Office of the Inspector General (OIG) contracted SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the Nuclear Regulatory Commission's (NRC) Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019*.* Attached is SBG's report titled *Independent Evaluation of NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019*. The evaluation objective was to evaluate the effectiveness of the information security policies, procedures, and practices of the NRC. The findings and conclusions presented in this report are the responsibility of SBG. OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with the Council of Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

The report presents the results of the subject audit. Following the March 23, 2020, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

For the period October 1, 2018 through September 30, 2019, SBG found that while NRC established an effective agency-wide information security program and practices, SBG identified weaknesses that may have some impact on the agency's ability to adequately protect the NRC's systems and information.

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 follow-up 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 Terri Cooper, Team Leader, at (301) 415-5965.

Attachment: As stated

Independent Evaluation Report of NRC's Implementation of FISMA 2014 for Fiscal Year 2019

Report Summary

Objective

The objective was to evaluate the effectiveness of the information security policies, procedures, and practices of the U.S. Nuclear Regulatory Commission (NRC). To achieve this objective, we evaluated the effectiveness of NRC's information security policies, procedures, and practices on a representative subset of the Agency's information systems. We then determined whether NRC's overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA 2014), Department of Homeland Security (DHS), and other Federal regulations, standards, and guidance applicable during the evaluation period.

Background

NRC's Office of the Inspector General engaged SBG Technology Solutions, Inc. (SBG), to conduct an independent evaluation of NRC's overall information security program and practices to respond to the fiscal year (FY) 2019 Inspector General (IG) FISMA Reporting Metrics. In FY 2019, we evaluated the effectiveness of NRC's information security controls, including its policies, procedures, and practices on a representative subset of the Agency's information systems. For the evaluation, we used FISMA and other regulations, standards, and guidance referenced in the FY 2019 IG FISMA Reporting Metrics as the basis for our evaluation of NRC's overall information security program.

Findings

While the NRC security program is effective, we did identify areas that need improvement.

Recommendations

While NRC established an effective agency-wide information security program and practices, we identified weaknesses that may have some impact on the agency's ability to adequately protect the NRC's systems and information. To be consistent with FISMA, NRC should strengthen its information security risk management framework by implementing seven recommended remedial actions. NRC management generally agreed with the findings and recommendations of our independent evaluation.

TABLE OF CONTENTS

I. ABBREVIATIONS AND ACRONYMS

ATO	Authority to Operate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ISA	Information Security Architecture
IG	Inspector General
IM	Information Management
IR	Incident Response
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	Plan of Actions and Milestones
SBG	SBG Technology Solutions, Inc.
SP	Special Publication

II. BACKGROUND, OBJECTIVE, AND METHODOLOGY

Background

NRC's Office of the IG engaged SBG, to conduct an independent evaluation of NRC's overall information security program and practices in response to the FY 2019 IG FISMA Reporting Metrics. In FY 2019, we evaluated the effectiveness of NRC's information security controls, including its policies, procedures, and practices on a representative subset of the agency's information systems. We used FISMA[1] and other regulations, standards, and guidance referenced in the FY 2019 IG FISMA Reporting Metrics as the basis for our evaluation of NRC's overall information security program and practices. FISMA includes the following key requirements:

- Each agency must develop, document, and implement an agency-wide information security program.[2]
- Each agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.[3]
- The agency's IG, or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.[4]

Objective

Our objective was to evaluate the effectiveness of the information security policies, procedures, and practices of the NRC. To achieve this objective, we evaluated the effectiveness of NRC's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether NRC's overall information security program and practices were effective and consistent with the requirements of FISMA, DHS, and other federal regulations, standards, and guidance applicable during the evaluation period.

Methodology

The overall strategy of our evaluation considered National Institute of Standards and Technology (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 guidance from the Office of Management and Budget (OMB), and DHS. We conducted our independent evaluation in accordance with the Council of Inspectors General for Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. For each metric question, we tested through inquiry with management and inspection of management policies and procedures, including but not limited to, the Information Security Policy and Security Assessment and Authorization artifacts, such as

[1] *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014).
[2] 44 U.S.C. § 3554(b).
[3] 44 U.S.C. § 3554(a)(1)(A).
[4] 44 U.S.C. §§ 3555(a)(1) and (b)(1).

System Security Plans, Security Assessment Reports, Authority to Operate (ATO), and Plan of Actions and Milestones (POA&Ms).

Table 1: Testing Method and Descriptions

Testing Method	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; and witnessing the performance of controls.
Inspection	Inspected relevant records. This testing included reviewing documents, and system configurations and settings. In some cases, inspection testing involved tracing items to supporting documents, system documentation, or processes.

FISMA 2014 Reporting Metrics

The OMB, DHS, and CIGIE, in a collaborative effort and in consultation with the Federal Chief Information Officers Council, developed the FY 2019 IG FISMA Reporting Metrics. The FY 2019 metrics continue using the maturity model approach for all security domains and are fully aligned with the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) function areas.

Table 2 includes the DHS in-scope reporting metric domains for our evaluation.[5]

Table 2: Aligning the Cybersecurity Framework with the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Function	FY 2019 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring

[5] OMB, DHS & CIGIE, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, V1.3, April 1, 2019*.

Cybersecurity Framework Function	FY 2019 IG FISMA Metric Domains
Respond	Incident Response
Recover	Contingency Planning

In FY 2019, CIGIE, in partnership with OMB and DHS, continued refining these metrics. The metrics consisted of specific questions (performance metrics) for each metric domain and the descriptions of the five maturity levels for each metric. Table 3 includes DHS' general description of the five maturity levels.

Table 3: IG Assessment Maturity Levels

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

The DHS guidance states that ratings throughout the domains will be by a simple majority, where the most frequent level across the questions will serve as the domain rating. OMB strongly encourages IGs to use the domain ratings to inform the overall function ratings, and to use the five function ratings to inform the overall agency rating. The guidance further states that Level 4, *Managed and Measurable*, is considered to be an effective level of security at the domain, function, and overall security program level.

III. EVALUATION RESULTS

This report provides the results of SBG's independent evaluation of NRC's Information Technology (IT) security program and practices required by FISMA 2014, based on the FY 2019 IG FISMA Reporting Metrics that use the maturity model indicators. According to DHS criteria, Level 4, *Managed and Measurable*, is considered to be an effective level of security at the domain, function, and overall program level. Although we identified deficiencies related to Risk Management; Configuration Management; Data Protection and Privacy; Security Training; and Contingency Planning[6] we determined that NRC effectively established an information security program and security practices across the Agency, as required by FISMA, OMB policy and guidelines, and NIST standards and guidelines. Table 4 summarizes the overall assessed maturity levels for NRC's information security program.

Table 4: Assessed Maturity Levels for NRC's Information Security Program

FUNCTION / *Domain*	**Levels**
IDENTIFY *Risk Management*	**Level 4**
PROTECT	**Level 4**
A. *Configuration Management*	Level 4
B. *Identity and Access Management*	Level 3.67
C. *Data Protection and Privacy*	Level 3.6
D. *Security Training*	Level 3.67
DETECT *Information Security Continuous Monitoring*	**Level 4**
RESPOND *Incident Response*	**Level 4**
RECOVER *Contingency Planning*	**Level 4**
Overall Security Program Effectiveness	**Effective**

For the metric domains noted as being less than a level 4 above, we identified deficiencies that resulted in metric questions within that domain as being below a level 4. The subsequent section below provides a summary of these noted findings and our recommendations by domain for NRC to consider as NRC works to remediate them and mature the agency's information security program.

[6] We based our conclusions on our evaluation of the DHS FY 2019 IG FISMA reporting metrics; refer to the Appendix for additional information on scope and methodology.

Findings

In summary, we identified the following information security control weaknesses throughout our testing that were significant within the context of the objectives of our independent evaluation:[7]

A. Function Area: Identify – Risk Management

Overall, we determined NRC's Risk Management domain to be effective, however we noted the following weaknesses that NRC should consider in the agency's efforts to more effectively manage, measure, and optimize the Risk Management domain and overall information security program:

- NRC had not fully defined an Information Security Architecture (ISA) across the enterprise, business processes, and system levels necessary to maintain a disciplined and structured methodology for assessing and managing risk.

- NRC was in the process of re-evaluating the list of high value assets and developing procedures for considering risks from the supporting business functions and mission impacts necessary for prioritizing and guiding risk management decisions.

- NRC did not include supply chain risk or an organization-wide assessment of security and privacy risks in existing risk management procedures.

Recommendations

1. Fully define NRC's ISA across the enterprise and business processes and system levels.

2. Use the fully defined ISA to:

    a. Assess enterprise, business process, and information system level risks.

    b. Update the list of high value assets by considering risks from the supporting business functions and mission impacts.

    c. Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.

    d. Conduct an organization-wide security and privacy risk assessment.

    e. Conduct a supply chain risk assessment.

    f. Identify and update NRC risk management policies, procedures, and strategy.

[7] We provided agency management with findings and recommendations for weaknesses we noted during our independent evaluation.

B. Function 2A: Protect - Configuration Management

Overall, we determined NRC's Configuration Management domain to be effective. However, we noted the following weakness that NRC should consider in the agency's efforts to more effectively manage, measure, and optimize the Configuration Management domain and overall information security program:

- NRC has not yet implemented an automated application whitelisting tool to detect authorized software and block the risk of unauthorized software on its network.

Recommendation

3. Identify and implement a software whitelisting tool to detect authorized software and block the risk of unauthorized software on its network.

C. Function 2D: Protect – Data Privacy and Protection

Overall, we determined NRC's Data Privacy and Protection domain to be effective, however we noted the following weakness that NRC should consider in the agency's efforts to more effectively manage, measure, and optimize the Data Privacy and Protection domain and overall information security program:

- Although NRC performs role-based privacy training, NRC has not defined requirements for role-based privacy awareness training for those privileged users responsible for managing Personally Identifiable Information (PII).

Recommendations

4. Perform an assessment of role-based privacy training gaps.

5. Identify individuals having specialized role-based responsibilities for PII or activities involving PII, and develop role-based privacy training for them.

D. Function 5: Recover - Contingency Planning

Overall, we determined NRC's Contingency Planning domain to be effective, however we noted the following weaknesses that NRC should consider in the agency's efforts to more effectively manage, measure, and optimize the Contingency Planning domain and overall information security program:

- NRC has not integrated supply chain concerns into its contingency planning policies and procedures.

- NRC was in the process of updating contingency planning policies and procedures to include the consideration of system level business impact assessments to prioritize the agency and system level contingency, continuity, and/or recovery plans.

Recommendations

6. Based on NRC's supply chain risk assessment results, complete updates to the NRC's contingency planning policies and procedures to address supply chain risk.

7. Continue efforts to conduct agency and system level business impact assessments to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

IV. CONCLUSIONS

Although NRC established an effective agency-wide information security program and effective practices, we identified weaknesses that may have some impact on the agency's ability to adequately protect the NRC's systems and information. Some weaknesses we identified could negatively affect the confidentiality, integrity, and availability of the agency's systems and personally identifiable information. To be consistent with FISMA, NRC should strengthen its information security risk management framework by implementing the recommended remedial actions noted above in this report.

V. AGENCY COMMENTS

An exit briefing was held with the agency on March 23, 2020. Prior and subsequent to this meeting, NRC management reviewed a discussion draft and provided comments that have been incorporated into this report as appropriate. As a result, NRC management stated their general agreement with the findings and recommendations of this report and chose not to provide formal comments for inclusion in this report.

Appendix – Criteria

SBG focused the FISMA 2014 evaluation approach on Federal information security guidelines developed by NRC, NIST, and OMB. NIST SP 800 series 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 FY 2019 FISMA 2014 evaluation.

NRC

- MD 1.1, NRC Management Directives System, Volume 1: Management Directives, December 18, 2018, DT-18-18
- MD 2.3, Telecommunications, Volume 2: Information Technology, October 13, 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, April 18, 2019, DT-19-05
- MD 4.4, Enterprise Risk Management and Internal Control, Volume 4: Financial Management, December 14, 2017, DT-17-18
- MD 6.1, Resolution and Follow-up 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 FIPS and SPs

- FIPS-200, Minimum Security Requirements for Federal Information and Information Systems;

- FIPS- 201-2, Personal Identity Verification of Federal Employees and Contractors;

- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-30, Guide for Conducting Risk Assessments;

- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-35, Guide to Information Technology Security Services;

- NIST SP 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach;

- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View;

- NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies;

- NIST SP 800-44 Guidelines on Securing Public Web Servers;

- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems;

- 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 800-55 Revision 1, Performance Measurement Guide for Information Security;

- NIST SP 800-60 Volume I and II Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;

- NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide;

- NIST SP 800-70 Revision 3, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers;

- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops

- NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems;

- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations

- NIST SP 800-152, A Profile for U.S. Federal Cryptographic Key Management Systems;

- NIST SP 800-160, Systems Security Engineering;

- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations;

- NIST SP 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

- NIST SP 800-184 Guide for Cybersecurity Event Recovery

- NIST Interagency Report 8011 Volume I and II, Automation Support for Security Control Assessments.

- NIST Supplemental Guidance on Ongoing Authorization (See NIST 800-37).

- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018

OMB Policy Directives

- OMB Memorandum M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program
- OMB Memorandum M-17-25: Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- 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, FY 2008 Implementation of Trusted Internet Connections (TIC)