MEMORANDUM

December 20, 2021

TO: Daniel H. Dorman
Executive Director for Operations

FROM: Eric Rivera **/RA/**
Acting Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021 (OIG-22-A-04)

The Office of the Inspector General (OIG) contracted with 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 2021. Attached is SBG's report titled Independent Evaluation of the NRC's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2021. The objective was to evaluate the effectiveness of the information security policies, procedures, and practices at the NRC. The findings and conclusions presented in this report are the responsibility of SBG. The 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 evaluation. Following the exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

For the period October 1, 2020 through September 30, 2021, SBG found that while the NRC established an effective agency-wide information security program and practices, there are weaknesses that may have some impact on the agency's ability to optimally protect the NRC's

systems and information.

Please provide information on actions taken or planned on each of the recommendations within 30 calendar days of the date of this report. 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 evaluation. 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 the NRC's Implementation of FISMA 2014 For Fiscal Year 2021

Report Summary

Objective

The objective was to evaluate the effectiveness of the information security policies, procedures, and practices at the Nuclear Regulatory Commission (NRC). To achieve this objective, we evaluated the effectiveness of the NRC's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether the 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

The NRC's Office of the Inspector General engaged SBG Technology Solutions, Inc. (SBG), to conduct an independent evaluation of the NRC's overall information security program and practices to respond to the fiscal year (FY) 2021 Inspector General (IG) FISMA Reporting Metrics. In FY 2021, we evaluated the effectiveness of the NRC's information security controls, including its policies, procedures, and practices on a representative subset of the agency's information systems.

Findings

The NRC's information security program was "Effective" according to DHS criteria specified in the FY 2021 IG FISMA Reporting Metrics. While effective, we did identify areas that need to be improved upon to optimize the NRC's information security program.

Recommendations

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

I. TABLE OF CONTENTS

I. ABBREVIATIONS AND ACRONYMS

ATO	Authority to Operate
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIA	Confidentiality Integrity Availability
CP	Contingency Planning
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ISCM	Information System Continuous Monitoring
ISA	Information Security Architecture
ICT	Information Communication Technology
IG	Inspector General
IAM	Identity and Access Management
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
RM	Risk Management
SBG	SBG Technology Solutions, Inc.
ST	Security Training
SCRM	Supply Chain Risk Management
SP	Special Publication
SCRM	Supply Chain Risk Management
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team
VDP	Vulnerability Disclosure Policy

II. BACKGROUND, OBJECTIVE, AND METHODOLOGY

Background

The NRC's Office of the Inspector General (OIG) engaged SBG to conduct an independent evaluation of the NRC's overall information security program and practices in response to the FY 2021 IG FISMA Reporting Metrics. In FY 2021, we evaluated the effectiveness of the NRC's information security controls, including its policies, procedures, and practices, on a representative subset of the agency's information systems. We used the FISMA[1] and other regulations, standards, and guidance referenced in the FY 2021 IG FISMA Reporting Metrics as the basis for our evaluation of the NRC's overall information security program and practices. The 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 effectiveness of the information security policies, procedures, and practices of the NRC. To achieve this objective, we evaluated the effectiveness of the NRC's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether the NRC's overall information security program and practices were effective and consistent with the requirements of the FISMA, DHS, and other federal regulations, standards, and guidance applicable during the evaluation period.

Methodology

The overall strategy of our evaluation considered the 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 the 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; 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, the DHS, and the CIGIE, in a collaborative effort and in consultation with the Federal Chief Information Officers Council, developed the FY 2021 IG FISMA Reporting Metrics. The FY 2021 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: Aligning the Cybersecurity Framework with the FY 2021 IG FISMA Metric Domains[5]

Cybersecurity Framework Function	FY 2021 IG FISMA Metric Domains
Identify	Risk Management (RM) Supply Chain Risk Management (SCRM)
Protect	Configuration Management (CM) Identity and Access Management (IDM) Data Protection and Privacy (DPP) Security Training (ST)
Detect	Information Security Continuous Monitoring (ISCM)
Respond	Incident Response (IR)

[5] OMB, DHS & CIGIE, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, V1.1,* May 12, 2021

Cybersecurity Framework Function	FY 2021 IG FISMA Metric Domains
Recover	Contingency Planning (CP)

With the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. As a result, the FY 2021 IG FISMA Reporting Metrics included a new domain on Supply Chain Risk Management (SCRM) within the Identify function. This domain focuses on the maturity of SCRM strategies, policies, procedures, plans, and processes.

In FY 2021, the CIGIE, in partnership with the OMB and the 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 the 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. The 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 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 the NRC's Information Technology (IT) security program and practices required by FISMA 2014, based on the FY 2021 IG FISMA Reporting Metrics that use the maturity model indicators. According to DHS criteria, Level 4, *Managed and Measurable*, is an effective level of security at the domain, function, and overall program level. Although we identified deficiencies related to Risk Management; Supply Chain Risk Management, Configuration Management; Data Protection and Privacy; Security Training; and Contingency Planning[6] we determined that the NRC effectively established an information security program and security practices across the agency, as required by the FISMA, OMB policy and guidelines, and NIST standards and guidelines. Table 4 summarizes the overall assessed maturity levels for the NRC's information security program.

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

FUNCTION / *Domain*	Levels
IDENTIFY *Risk Management* *Supply Chain Risk Management*	**Level 4** **Level 2**
PROTECT	**Level 4**
A. Configuration Management	Level 4
B. Identity and Access Management	Level 4
C. Data Protection and Privacy	Level 4
D. Security Training	Level 4
DETECT *Information Security Continuous Monitoring*	**Level 4**
RESPOND *Incident Response*	**Level 4**
RECOVER *Contingency Planning*	**Level 3**
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. Following is a summary of these noted findings and our recommendations by domain for the NRC to consider as the agency works to remediate them and mature their information security program.

[6] We based our conclusions on our evaluation of the DHS FY 2021 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 1A: Identify - Risk Management

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

- Based on our FY 2021 assessment we noted the following findings;

  1. The NRC had not yet implemented the capability to use data driven prioritization to support the risk-based allocation of resources to protect the NRC's identified Agency level High Value Assets (HVAs).

  2. The NRC had not yet updated the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.

  3. The NRC's Information Security Architecture (ISA) does not include procedures for assessing the impacts to the organization's ISA prior to introducing to new information systems or major information system changes into the Agency's environment.

  4. Two (2) out of three (3) systems in scope for the assessment did not close a sample of critical and high categorized Plans of Action & Milestones (POA&Ms) within the required 30-day period in accordance with NRC requirements. Specifically, one (1) out of one (1) sampled POA&M for the ISMP system and thirty-four (34) out of thirty-four (34) POA&Ms for the ITI system were not closed within 30 days.

  5. The NRC consistently utilizes other comparable mechanism to a cybersecurity risk register to ensure that information about risks are communicated in a timely and effective manner to appropriate internal and external stakeholders. However, the NRC did not use a cybersecurity risk register to aggregate security risks, normalize information across organizational units, or prioritize operational risk response activities.

Recommendations:

- In FY 2021 we noted the following recommendations:

  1. Reconcile mission priorities and cybersecurity requirements into profiles to inform the prioritization and tailoring of controls (e.g. HVA control overlays) to support the risk-based allocation of resources to protect the NRC's identified Agency level and/or National level HVAs.

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

2. Continue current Agency's efforts to update the Agency's cybersecurity risk register to (i) aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.

3. Update procedures to include assessing the impacts to the organization's ISA prior to introducing new information systems or major system changes into the Agency's environment.

4. Develop and implement procedures in the POA&M process to include mechanisms for prioritizing completion and incorporating this as part of documenting a justification and approval for delayed POA&Ms.

B. Function 1B: Identify - Supply Chain Risk Management

Overall, we determined the NRC's Supply Chain Risk Management domain to be not effective, however we noted the following weaknesses that the NRC should consider in their efforts to effectively manage, measure, and optimize the Supply Chain Risk Management domain and overall information security program:

- In FY 2021 we noted the following finding carried over from our FY 2020 assessment as the NRC had not yet remediated this;

  1. The NRC had developed a strategy to establish a supply chain risk management program but has not yet fully implemented this strategy.

- Based on our FY 2021 assessment we noted the following findings;

  2. The NRC does not have policies and procedures in place for prioritization of externally provided systems or a risk-based process for evaluating cyber supply chain risks associated with third party providers.

  3. Procedures were developed and documented however, counterfeit components for the NRC supply chain are performed on an ad hoc basis and are not consistently monitored.

  4. Role-based training is not required and has not yet been developed for individuals with supply chain risk management responsibilities.

Recommendations:

- In FY 2020 we noted the following recommendation which carried over to our FY 2021 assessment:

  5. Assess the NRC supply chain risk and fully define performance metrics in service level agreements and procedures to measure, report on, and monitor the risks related to contractor systems and services.

- In FY 2021 we noted the following recommendations:

6. Document and implement policies and procedures for prioritizing externally provided systems and services or a risk-based process for evaluating cyber supply chain risks associated with third party providers.

7. Implement processes for continuous monitoring and scanning of counterfeit components to include configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

8. Develop and implement role-based training with those who hold supply chain risk management roles and responsibilities to detect counterfeit system components.

C. Function 2A: Protect - Configuration Management

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

- Based on our FY 2021 assessment we noted the following finding;

1. For one (1) (ITI) of a sample of three (3) systems in scope for the FY 2021 assessment, the most recent system cybersecurity assessment reports for the system identified critical and high vulnerabilities that were not addressed timely in accordance with NRC policies and procedures.

Recommendation:

- In FY 2020 we noted the following recommendation which carried over to our FY 2021 assessment:

9. Continue to monitor the remediation of critical and high vulnerabilities and identify a means to assign and track progress of timely remediation of vulnerabilities.

D. Function 2B: Protect - Identity and Access Management

The NRC's Identity and Access Management domain was determined to be a level 3 maturity level which according to DHS is not effective. NRC should consider addressing the following weaknesses in the agency's efforts to manage, measure, and optimize the Identity and Access Management domain and overall information security program more effectively:

- Based on our FY 2021 assessment we noted the following findings;

1. The NRC has consistently implemented strong authentication mechanisms for privileged and non- privileged users[8] of the NRC's facilities and networks, including for remote access, in accordance with federal targets. However, not all privileged and non-privileged users utilize strong mechanisms to authenticate to all NRC systems.

[8] Privileged users are users with administrative or elevated access to a system while non-privileged users are users without administrative or elevated access to a system.

2. The NRC does not currently require non-disclosure forms to be completed for all users prior to being granted access. The NRC currently requires non-disclosure forms (Standard Form 312) only for users with Q or L clearances who have physical access to the NRC facility, though the Personnel Security Branch intends to perform the SF-312 briefing for all applicable users once pandemic restrictions on physical access are lifted. NRC also does not require users to complete rules of behavior until after they have received system access.

3. The NRC did not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege[9] reviews. Furthermore, there were deficiencies in either the design or the operating effectiveness of account management and identification and authentication controls for one (1) of three (3) FISMA systems (ITI CDM and ICAM) that were in-scope for the FY 21 Inspector General FISMA assessment. Although Plans of Action and Milestones (POA&Ms) were created to address these control failures, these POA&Ms had not been closed out over a year after they were created.

Recommendations:

- In FY 2020 we noted the following recommendations which carried over to our FY 2021 assessment:

10. Centralize system privileged and non-privileged user access review, audit log activity monitoring, and management of Personal Identity Verification (PIV) or Identity Assurance Level (IAL) 3/Authenticator Assurance Level (AAL) 3 credential access to all NRC systems (findings noted in bullets a, and c, above) by continuing efforts to implement these capabilities using automated tools.

11. Update user system access control procedures to include the requirement for individuals to complete a non-disclosure and rules of behavior agreements prior to the individual being granted access to NRC systems and information.

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

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

- Based on our FY 2021 assessment we noted the following finding;

1. The NRC did not have an external assessment of its privacy program performed in FY 2021.

Recommendation:

- In FY 2021 we noted the following recommendation:

[9] Least privilege is the practice of limiting access rights for applications, systems, process, and devices to only those permissions required to perform authorized activities.

12. Conduct an independent review or assessment of the NRC privacy program and use the results of these reviews to periodically update the privacy program.

F. Function 2D: Protect - Security Training

Overall, we determined the NRC's Security Training domain to be effective, however we noted the following weakness that the NRC should consider in its efforts to effectively manage, measure, and optimize the Security Training domain and overall information security program;

- In FY 2021 we noted the following finding carried over from our FY 2020 assessment as the NRC had not yet remediated this;

  1. The NRC did not have enforcement mechanisms in place for employees who do not complete role based or annual security awareness training.

- Based on our FY 2021 assessment we noted the following findings;

  2. Although new contractors are required according to the NRC's policies to complete security awareness training within one week of being granted access to the NRC systems and information, the NRC does not have the capability to track and enforce this training completion within the one-week timeframe.

  3. Although the NRC requires employees and contractors to complete role-based training prior to assuming their role, they do not have a system in place to monitor and enforce the completion of this requirement.

Recommendations:

- In FY 2020 we noted the following recommendations which carried over to our FY 2021 assessment:

  13. Implement the technical capability to restrict access or not allow access to the NRC's systems until new NRC employees and contractors have completed security awareness training and role-based training as applicable or implement the technical capability to capture NRC employees and contractor's initial login date so that the required cybersecurity awareness and role-based training can be accurately tracked and managed by the current process in place.

  14. Implement the technical capability to restrict NRC network access for employees who do not complete annual security awareness training and, if applicable, their assigned role-based security training.

G. Function 3: Detect – Information Security Continuous Monitoring

Overall, we determined the NRC's Detect – ICSM domain to be effective. For the Fiscal Year 2021, there were no findings or recommendations for this domain.

H. Function 4: Respond - Incident Response

Overall, we determined the NRC's Incident Response domain to be effective, however we noted the following weaknesses that the NRC should consider in its efforts to effectively manage, measure, and optimize the Incident Response domain and overall information security program;

- In FY 2021 we noted the following finding carried over from our FY 2020 assessment as the NRC had not yet remediated it;

    1. The NRC does not have metrics to measure the timely reporting of incidents to internal and external stakeholders or for how long an event is in the investigative status before its determined to be or not be a reportable incident.

Recommendation:

- In FY 2021 we noted the following recommendation:

    15. Implement metrics to measure and reduce the time it takes to investigate an event and declare it as a reportable or non-reportable incident to US-CERT.

I. Function 5: Recover - Contingency Planning

Overall, we determined the NRC's Contingency Planning domain to be effective, however in FY 2021 we noted the following findings carried over from our FY 2020 assessment as the NRC had not yet remediated them;

1. The NRC did not complete an organization level Business Impact Assessment (BIA) to incorporate the results into the enterprise risk management program or enterprise risk register.

2. The NRC did not fully integrate metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans as appropriate to deliver persistent situational awareness across the organization. Appropriate related information from plans such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency would improve contingency plan effectiveness.

3. The NRC does not employ automated mechanisms to test system contingency plans or coordinate plan testing with Information Communication Technology (ICT) supply chain providers or other external stakeholders.

Recommendations:

- In FY 2020 we noted the following recommendations which carried over to our FY 2021 assessment:

    16. Conduct an organizational level BIA to determine contingency planning requirements and priorities, including for mission essential functions/high value assets, and update contingency planning policies and procedures accordingly.

17. Integrate metrics for measuring the effectiveness of information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation, and occupant emergency plans, as appropriate, to deliver persistent situational awareness across the organization.

18. Update and implement procedures to coordinate contingency plan testing with ICT supply chain providers.

IV. CONCLUSIONS

Although the NRC established an effective agency-wide information security program and effective practices, we identified a few weaknesses that may have some impact on the agency's ability to adequately protect NRC 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 optimize the NRC's information security program, the 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 December 15, 2021. Prior to this meeting, the NRC management reviewed a discussion draft and provided comments that have been incorporated into this report as appropriate. As a result, the 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 the NRC, the NIST, and the OMB. NIST SP 800 series provide guidelines that were considered essential to the development and implementation of the NRC's security programs. The following is a listing of the criteria used in the performance of the FY 2020 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, March 10, 2020, DT-20-05
- 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, October 1, 2020, DT-20-11

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-20-04, Fiscal Year 2019-2020 *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-14-03, FY 2014 *Enhancing the Security of Federal Information and Information Systems*
- OMB Memorandum M-15-14, *Management and Oversight of Federal Information Technology.*
- OMB Memorandum M-16-17, OBM Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*
- OMB Memorandum M-16-04, FY 2016 *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*
- OMB Memorandum M-17-12*: Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB Memorandum M-17-25: *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- OMB Memorandum M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*
- OMB Memorandum M-19-17*, Enabling Mission Delivery Through Improved Identity, Credential, and Access Management*
- OMB Memorandum M-20-04, Fiscal Year 2019-2020 *Guidance on Federal Information Security and Privacy Management Requirements*