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

OFFICE OF THE
INSPECTOR GENERAL

March 19, 2021

MEMORANDUM TO: Margaret M. Doane
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF THE NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 (OIG-21-A-05)

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 2020. 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 2020*. 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. 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, 2019 through September 30, 2020, 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 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 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 2020

Report Summary

Objective

The objective was to evaluate the effectiveness of the information security policies, procedures, and practices of 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) 2020 Inspector General (IG) FISMA Reporting Metrics. In FY 2020, 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 2020 IG FISMA Reporting Metrics. While the NRC's information security program is effective, we did identify areas that need improvement.

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 adequately 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 sixteen 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
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
US-CERT	United States Computer Emergency Readiness Team

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 2020 IG FISMA Reporting Metrics. In FY 2020, 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 2020 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 2020 IG FISMA Reporting Metrics. The FY 2020 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 2020 IG FISMA Metric Domains[5]

Cybersecurity Framework Function	FY 2020 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
Respond	Incident Response
Recover	Contingency Planning

[5] OMB, DHS & CIGIE, *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, V4.0,* April 17, 2020

In FY 2020, 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 the FISMA 2014, based on the FY 2020 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; Configuration Management; Data Protection and Privacy; Security Training; and Contingency Planning[6] we determined that the NRC effectively established an information security program and

[6] We based our conclusions on our evaluation of the DHS FY 2020 IG FISMA reporting metrics; refer to the Appendix for additional information on scope and methodology.

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*	**Level 4**
PROTECT	**Level 4**
A. Configuration Management	Level 4
B. Identity and Access Management	Level 3
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.

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

- In FY 2020 we noted the following findings carried over from our FY 2019 assessment as the NRC had not yet remediated them;

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

a) The 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.

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

- Based on our FY 2020 assessment we noted the following findings;

a) The NRC was developing a process to capture and share lessons learned on the effectiveness of risk management processes and activities to update the program. Furthermore, the NRC did not perform an organization-wide assessment of security and privacy risks to serve as an input to its risk management policies, procedures, and strategy.

b) For one (1) of three (3) systems in scope for the assessment, one of the sub systems' system security plan noted that low risk POA&M items were no longer being tracked for one of the controls in the SSP identified as not being implemented during the FY 2020 cybersecurity assessment. However, according to NIST SP 800-53 Revision 4, the control is a priority one (1) moderate impact control.

c) The NRC has not formally established and implemented the use of qualitative and quantitative performance metrics to measure, report, and monitor the information security performance of contractor operated systems and services.

Recommendations:

1. Fully define the NRC's ISA across the enterprise, 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, if necessary, based on reviewing the ISA to identify risks from the supporting business functions and mission impacts.

c) If necessary, update 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 and implement a process to capture lessons learned and update risk management policies, procedures, and strategies.

e) Consistently assess the critically of POA&Ms to support why a POA&M is or is not of a high or moderate impact to the Confidentiality, Integrity and Availability (CIA) of the information system, data, and mission.

f) 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.

B. 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 the agency's efforts to more effectively manage, measure, and optimize the Configuration Management domain and overall information security program:

a) For two (2) of a sample of three (3) systems in scope for the FY 2020 assessment, the most recent system cybersecurity assessment report identified critical and high vulnerabilities that were not addressed timely in accordance with NRC policies and procedures.

Recommendation:

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

C. 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 considered to be not effective. The NRC should consider addressing the following weaknesses in the agency's efforts to more effectively manage, measure, and optimize the Identity and Access Management domain and overall information security program:

a) 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.

b) Four (4) of a sample of ten (10) individuals granted network access in FY 2020 had an approved security clearance waiver, however, a non-disclosure agreement was not completed prior to these individuals being granted access to NRC systems and sensitive information. Furthermore, the NRC does not require new contractors and employees to complete rules of behavior agreements prior to being granted access to NRC's network.

c) The NRC does not use automated tools to inventory and manage accounts and perform segregation of duties/least privilege[9] reviews. Furthermore, for one (1) of three (3) systems tested, several least privilege access controls were not implemented, and did not have a deviation approval. Although Plan of Action and Milestones were created to address these control failures, these POA&Ms had not been addressed over a year after they were created.

d) For two (2) of three (3) systems in scope for the assessment, we noted the following privileged user account activity discrepancies;

[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.
[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.

1. For two (2) sub systems of one (1) of the systems in scope, a plan of action was documented for one subsystem's failure to perform user access reviews; however, no plan of action was documented to address the other sub systems' failure to perform user access reviews.

2. One (1) system had one (1) sub system where log activity is captured but not periodically reviewed. Additionally, two sub systems of this same system, had plan of actions and milestones, documented to address failures to configure audit logging for a few devices in accordance with the NRC's configuration standard.

Recommendations:

4. 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 the NRC systems (findings noted in bullets 1, 3, and 4 above) by continuing efforts to implement these capabilities using the Splunk QAudit, Sailpoint, and Cyberark automated tools.

5. Update user system access control procedures to include the requirement for individuals to complete a non-disclosure agreement as part of the clearance waiver process prior to the individual being granted access to the NRC systems and information. Also, incorporate the requirement for contractors and employees to complete non-disclosure agreements as part of the agency's on-boarding procedures prior to these individuals being granted access to the NRC's systems and information.

D. Function 2D: 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 the agency's efforts to more effectively manage, measure, and optimize the Data Privacy and Protection domain and overall information security program:

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

Recommendation:

6. Continue efforts to identify individuals having additional responsibilities for PII or activities involving PII and develop role-based privacy training for them to be completed annually.

E. 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 the agency's efforts to more effectively manage, measure, and optimize the Security Training domain and overall information security program;

a) The NRC does not require employees and contractors to complete security awareness training or role-based training prior to system access and does not have enforcement mechanisms in place for employees who do not complete role based or annual security awareness training.

Recommendations:

7. 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.

8. 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.

F. 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 the agency's efforts to more effectively manage, measure, and optimize the Incident Response domain and overall information security program;

a) The NRC does not have metrics to measure the timely reporting of incidents to internal and external stakeholders. Thirty-nine events took place between one day to a few months of investigation before they were confirmed to be an incident that had no impact and that were not required to be reported to US-CERT. Furthermore, one incident reported to USCERT was in the investigation status for approximately16 hours before it was confirmed and reported to USCERT within one hour.

Recommendations:

9. 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.

G. Function 5: Recover - Contingency Planning

Despite the impact of the pandemic requiring 97% of NRC users to work remotely, the NRC's contingency and continuity plans allowed for no interruption to the agency's mission and system. As a result, despite the overall rating of level 3 consistently implemented, we determined that the NRC's contingency planning program is effective. However, we noted the following weaknesses that the NRC should consider in the agency's efforts to more effectively manage, measure, and optimize the Contingency Planning domain and overall information security program:

a) The NRC did not complete an organization level Business Impact Assessment (BIA). Furthermore, the NRC does not require that a BIA be completed to consider the cross utilization of security categorization and BIAs to identify potential conflicting information and anomalous conditions for systems categorized as low availability in accordance with NIST 800-60 Volume I, section 4.6.

b) The NRC has yet to 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.

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

Recommendations:

10. 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.

11. For low availability categorized systems complete an initial BIA and update the BIA whenever a major change occurs to the system or mission that it supports. Address any necessary updates to the system contingency plan based on the completion of or updates to the system level BIA.

12. 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.

13. Implement automated mechanisms to test system contingency plans, then update and implement procedures to coordinate contingency plan testing with ICT supply chain providers and implement an automated mechanism to test system contingency plans.

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 be consistent with the FISMA, 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 March 8, 2021. 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 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*