DEFENSE NUCLEAR FACILITIES SAFETY BOARD
WASHINGTON, D.C. 20004-2901

OFFICE OF THE INSPECTOR GENERAL

March 31, 2020

MEMORANDUM TO: Glenn Sklar
General Manager

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

SUBJECT: INDEPENDENT EVALUATION OF DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2019 (DNFSB-20-A-05)

The Office of the Inspector General (OIG) contracted SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the Defense Nuclear Facilities Safety Board's (DNFSB) *Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019.* Attached is SBG's report titled *Independent Evaluation of DNFSB's Implementation of the Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year 2019*. The evaluation objective was to conduct an independent assessment of DNFSB's FISMA implementation for Fiscal Year 2019. 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 evaluation. Following the exit conference, DNFSB staff indicated that they had no formal comments for inclusion in this report.

SBG found that DNFSB's information security practices and programs were generally effective for the period October 1, 2018 through September 30, 2019. However, the evaluation identified areas that need improvement.

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

cc: R. Howard

Independent Evaluation Report of DNFSB'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 Defense Nuclear Facilities Safety Board (DNFSB). To achieve this objective, we evaluated the effectiveness of DNFSB's information security policies, procedures, and practices on the agency's General Support System (GSS) information system. We then determined whether DNFSB's overall information security program and practices were effective and consistent with the requirements of *Federal Information Security Modernization Act of 2014* (FISMA 2014), NIST Special Publications (SP's), Office of Management and Budget (OMB) and other federal regulations, standards, and guidance applicable during the evaluation period.

Background

The Office of the Inspector General engaged SBG Technology Solutions, Inc. (SBG), to conduct an independent evaluation of DNFSB'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 DNFSB's information security controls, including its policies, procedures, and practices on the agency's GSS. 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 DNFSB's overall information security program.

Findings

Although the Defense Nuclear Facilities Safety Board (DNFSB) established an Agency-wide information security program and practices that was 'Consistently Implemented' at a Cyber Scope overall rating of 'Level 3,' SBG identified weaknesses related to Risk Management, Identity and Access Management, Configuration Management, Incident Response, and Contingency Planning. The Cyber Scope overall rating of 'Effective' reflects DNFSB's strides since 2017 in organizing third-party Security Assessment Reviews (SAR) and Gap Analyses to determine outstanding risks to the system and organization.

Recommendations

While DNFSB established agency-wide information security program and practices, SBG identified weaknesses that may impact the agency's ability to adequately protect their systems and information. To be consistent with FISMA, DNFSB should strengthen its information security Risk Management Framework by implementing 11 recommended remedial actions.

TABLE OF CONTENTS

I. ABBREVIATIONS AND ACRONYMS

CCB	Change Control Board
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CM	Configuration Management
CP	Contingency Planning
DNFSB	Defense Nuclear Facilities Safety Board
DHS	Department of Homeland Security
DPP	Data Privacy and Protection
FY	Fiscal Year
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
ICAM	Identity, Credential, and Access Management
ICT	Information and Communication Technology
IDM	Identity and Access Management
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISA	Information Security Architecture
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
RM	Risk Management
SP	Special Publication
ST	Security Training

II. BACKGROUND, OBJECTIVE, AND METHODOLOGY

Background

The Office of the Inspector General engaged SBG, to conduct an independent evaluation of DNFSB'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 DNFSB's information security controls, including its policies, procedures, and practices on the agency's General Support System (GSS) information system. 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 DNFSB'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 Inspector General (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 DNFSB. To achieve this objective, we evaluated the effectiveness of DNFSB's information security policies, procedures, and practices on the GSS information system. We then determined whether DNFSB's overall information security program and practices were effective and consistent with the requirements of FISMA 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) SP 800-53A, Guide for Assessing Security Controls in Federal Information Systems and Organizations; NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations; and the FISMA 2014 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.

[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).

We tested each metric question through in-person inquiries with the DNFSB Chief Information Security Officer, Chief Information Officer, and Senior System Administrator of the GSS. We inspected documented management policies and procedures including - but not limited to - the DNFSB Information Security Policy and Security Operating Procedures (OP's). Other reviewed artifacts included: DNFSB GSS System Security Plan (dated 2016), Gap Analyses, Security Assessment Reports, Authorizations to Operate, and Plan of Actions and Milestones.

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, DHS, and CIGIE developed the FY 2019 IG FISMA Reporting Metrics in a collaborative effort - and in consultation with - the Federal Chief Information Officers Council. 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 the evaluation.[5]

[5] OMB, DHS & CIGIE, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, V1.0.1 (May 24, 2019). (https://www.dhs.gov/sites/default/files/publications/Final%20FY%202019%20IG%20FISMA%20Metrics%20v1.0.1.pdf).

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 (RM)
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)
Recover	Contingency Planning (CP)

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. Similar to FY 2018, IGs have the discretion to determine the

overall effectiveness rating and the rating for each of the Cybersecurity Framework functions (e.g., Protect, Detect) at the maturity level of their choosing. Using this approach, the IG may determine that a particular function area and/or the agency's information security program is effective at maturity level lower than Level 4. According to DHS's criteria, SBG determined that DNFSB did not adhere to the high Level-4 standards set forth to properly establish an information security program and security practices across the Agency, as required by FISMA, OMB policy and guidelines, and NIST standards and guidelines. This, however, was due mainly to the small size of the organization precluding the need for expensive monitoring resources necessary for proper Level 4 IS management. Overall, DNFSB's GSS is effective at Level 3.

III. EVALUATION RESULTS

This report provides the results of SBG's independent evaluation of DNFSB's IT security program and practices required by FISMA 2014, based on the FY 2019 IG FISMA Reporting Metrics that use the maturity model indicators.

Table 4 summarizes the overall assessed maturity levels for DNFSB's information security program.

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

FUNCTION / *Domain*	Levels
IDENTIFY *Risk Management*	**Level 3**
PROTECT	**Level 3**
A. Configuration Management (CM)	Level 3
B. Identity and Access Management (IDM)	Level 3
C. Data Protection and Privacy (DPP)	Level 3
D. Security Training (ST)	Level 3
DETECT *Information Security Continuous Monitoring (ISCM)*	**Level 3**
RESPOND *Incident Response (IR)*	**Level 3**
RECOVER *Contingency Planning (CP)*	**Level 3**

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 DNFSB to consider as DNFSB works to remediate them and mature the Agency's information security program.

Findings

Overall due to the small organizational structure, DNFSB can operate and communicate more efficiently and effectively compared to larger Federal agencies. DNFSB's key risk management personnel are intimately involved in all aspects of DNFSB's RM, CM, IDM, DPP, ISCM, IR, and CP programs and are aware of every important decision involving its information security program. However, DNFSB had only developed and implemented performance metrics to manage and measure the Security Training domain. To achieve **a level 4** more mature effective program, DNFSB should continue to develop metrics to measure and more effectively manage the performance of all domains of the Agency's information security program. **Furthermore, DNFSB was unable to provide the results of a risk assessment to support why a level 3 maturity achieves cost-effective security based on their mission, risks faced, and established risk appetite, and risk tolerance level.** 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

A. Function Area: Identify

We noted the following weaknesses that DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize DNFSB's Identify domain of the agency's information security program:

- DNFSB has not completed the agency's information security architecture (ISA) to provide a disciplined and structured methodology for managing risk, establishing risk appetite and tolerance levels including for risk from the organization's supply chain.

- DNFSB has not consistently implemented system specific contracting language (such as appropriate information security and privacy requirements and material disclosures, Federal Acquisition Regulation clauses, and clauses on protection, detection, and reporting of information) and SLAs to mitigate and monitor the risks related to contractor systems and services.

- Due to the small size of DNFSB, key stakeholders maintain a common understanding of risks across the organization, including risk control and remediation activities, dependencies, and risk scores/levels leading to the agency's decision to not identify and implement a technical solution for providing a centralized enterprise wide view of risk.

- DNFSB was in the process of implementing, but has not completed, a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time.

Recommendations:

1. Define an ISA in accordance with the Federal Enterprise Architecture Framework.
2. Use the fully defined ISA to:
    a. Assess enterprise, business process, and information system level risks.
    b. Formally define enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.
    c. Conduct an organization wide security and privacy risk assessment.
    d. Conduct a supply chain risk assessment.
3. Using the results of recommendations one (1) and two (2) above:
    a. Implement an automated solution to help maintain an up-to-date, complete, accurate, and readily available Agency-wide view of the security configurations for all its GSS components; Cybersecurity Team exports metrics and vulnerability reports and sends them to the CISO and CIO's Office monthly for review. Develop a centralized dashboard that Cybersecurity Team and the CISO can populate for real-time assessments of compliance and security policies.
    b. Collaborate with DNFSB Cybersecurity Team Support to establish performance metrics in service level agreements to measure, report on, and monitor the risks related to contractor systems and services being monitored by Cybersecurity Team.
    c. Establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program.
    d. Implement a centralized view of risk across the organization.
4. Finalize the implementation of a centralized automated solution for monitoring authorized and unauthorized software and hardware connected to the agency's network in near real time. Continue ongoing efforts to apply the Track-It!, ForeScout and KACE solutions.

B. Function Area: Protect

We noted the following weaknesses that DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize DNFSB's Protect domain of the agency's information security program:

- DNFSB did not consistently hold change control board (CCB) meetings necessary for reviewing and approving configuration changes to the DNFSB system in accordance with the agency's Configuration Management Plan.

- Due to the very small number of privileged users, accounts are monitored manually (at least) annually. No automated mechanisms exist (e.g. machine-based, or user-based enforcement) to support the management of privileged accounts, including for

the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate.

- DNFSB is consistently implementing its Identity, Credential, and Access Management (ICAM) strategy and is on track to meet milestones, however, DNFSB was still in the process of transitioning to its desired or "to-be" ICAM architecture.

Recommendations:

5. Management should re-enforce requirements for performing DNFSBs change control procedures in accordance with the agency's Configuration Management Plan by defining consequences for not following these procedures and conducting remedial training as necessary.
6. Implement procedures and define roles for reviewing configuration change activities to the DNFSB information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately.
7. Complete and document a risk-based justification for not implementing an automated solution (e.g. Splunk) to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network.
8. Continue efforts to meet milestones of the DNFSB ICAM Strategy necessary for fully transitioning to DNFSB's "to-be" ICAM architecture.

C. Function Area: Detect

We noted the following weakness that DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize DNFSB's Detect domain of the agency's information security program;

- DNFSB was in the process of refining existing procedures to utilize the results of security control assessments and monitoring to maintain ongoing authorizations of its information system.

Recommendation:

9. Complete current efforts to refine existing monitoring and assessment procedures to more effectively support ongoing authorization of the DNFSB system.

D. Function Area: Respond

We noted the following weakness that DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize DNFSB's Respond domain of the agency's information security program:

- Although DNFSB had an incident response plan in place, DNFSB did not fully develop containment strategies for all types of major incidents.

Recommendation:

10. Identify and fully define requirements for the incident response technologies DNFSB plans to utilize in the specified areas and how these technologies respond to detected threats (e.g. cross-site scripting, phishing attempts, etc.).

E. Function Area: Recover

We noted the following weaknesses that DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize DNFSB's Recover domain of the agency's information security program:

- DNFSB only has one information system in its inventory, and DNFSB has not invested in an automated mechanism to more thoroughly and effectively test the agency's information system contingency plan.

- DNFSB's contingency plan does not address Information and Communication Technology (ICT) supply chain concerns into its contingency planning policies and procedures.

Recommendation:

11. Based on the results of DNFSB's supply chain risk assessment included in the recommendation for the Identify function above, update DNFSB's contingency planning policies and procedures to address ICT supply chain risk.

IV. CONCLUSIONS

Although DNFSB established Agency-wide information security program and practices, we identified weaknesses that may have some impact on the Agency's ability to adequately protect DNFSB'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, we believe DNFSB should strengthen its information security risk management framework by implementing the above recommended remedial actions; performing a risk assessment to support why a level 3 maturity achieves cost-effective security based on their mission, risks faced, established risk appetite, and risk tolerance level.

V. AGENCY COMMENTS

An exit briefing was held with the agency on February 20, 2020. Prior to this meeting, DNFSB management reviewed a discussion draft and later provided comments that have been incorporated into this report as appropriate. As a result, DNFSB 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 DNFSB, NIST, and OMB. NIST SP 800 series provide guidelines that were considered essential to the development and implementation of DNFSB's information security program. The following is a listing of the criteria used in the performance of the FY 2019 FISMA 2014 evaluation.

DNFSB

- FISMA FY2019 PBC - OP-411.2-2 Identification and Authentication Operating Procedures.
- FISMA FY2019 PBC - DNFSB BOD 18-02 – Submission.
- FISMA FY2019 PBC - Draft OP 411.2-X Security Awareness and Training Operating Procedures.
- FISMA FY2019 PBC – BIA Cover Letter with Team.
- FISMA FY2019 PBC - DNFSB BIA of MEFs Validation May 2018.
- FISMA FY2019 PBC – D-312.1 Insider Threat Program Directive.
- FISMA FY2019 PBC - OP 412-1 Acceptable Use of DNFSB Information Technology Sep 2018.
- FISMA FY2019 PBC - Cybersecurity_Directive_March2018_Version One.
- FISMA FY2019 PBC - D-21.1 - Directives Program.
- FISMA FY2019 PBC - OP-21-1-1 - Directive and Supplementary Document Procedures.
- FISMA FY2019 PBC - Continuous Monitoring Policies and Procedures_finalv1-0.
- FISMA FY2019 PBC - OP-242-1-1-personal-property-final.
- FISMA FY2019 PBC - D-242-1-personal-property-directive-final.
- FISMA FY2019 PBC - D-260-2 Privacy Program Directive.
- FISMA FY2019 PBC - D-410.1 IT_Program_Revision_Three_Aug2018.

- FISMA FY2019 PBC - OP-411-2-1 - Attachment A Information Systems Risk Management Framework and Security Authorization Handbook.
- FISMA FY2019 PBC - OP-411-2-1 - Attachment A Information Systems Risk Management Framework.
- FISMA FY2019 PBC - OP-411-2-1 - Information System Security Program Certification and Accreditation.
- FISMA FY2019 PBC - DNFSB Directive Information Systems Security Program-411-2.

NIST Federal Information Processing Standards (FIPS) and SP

- 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 (ISCM) 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.