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

OFFICE OF THE
INSPECTOR GENERAL

March 25, 2021

MEMORANDUM TO: James Biggins
Acting General Manager

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

SUBJECT: INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2020 (DNFSB-21-A-04)

The Office of the Inspector General (OIG) contracted with 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 2020*.* Attached is SBG's report titled *Independent Evaluation of the DNFSB'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 DNFSB. The findings and conclusions presented in this report are the responsibility of the 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, DNFSB staff indicated that they had no formal comments for inclusion in this report.

SBG found that the DNFSB's information security practices and programs were generally effective for the period October 1, 2019 through September 30, 2020. 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

Independent Evaluation Report of the DNFSB's Implementation of the FISMA 2014 for Fiscal Year 2020

Report Summary

Objective

Our 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 the DNFSB's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether the DNFSB's overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), the Department of Homeland Security (DHS), 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 the DNFSB'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 DNFSB's information security controls, including its policies, procedures, and practices on a representative subset of the agency's information systems.

Findings

While the DNFSB established an effective agency-wide information security program and practices, we identified a weakness that may impact the agency's ability to adequately protect the DNFSB's systems and information. We identified weaknesses related to Risk Management, Identity and Access Management, Configuration Management, Incident Response, and Contingency Planning.

Recommendations

To be consistent with the FISMA, the DNFSB should strengthen its information security risk management framework by implementing fourteen recommended remedial actions. DNFSB management generally agreed with the findings and recommendations of our independent evaluation.

TABLE OF CONTENTS

I. Abbreviations and Acronyms

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
DRP	Disaster Recovery Plan
FY	Fiscal Year
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
ICT	Infrastructure Communications Strategy
IDM	Identity and Access Management
IG	Inspector General
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISA	Information Security Architecture
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Actions and Milestones
RM	Risk Management
SP	Special Publication
ST	Security Training

II. BACKGROUND, OBJECTIVE, and METHODOLOGY

Background

The Office of the Inspector General (OIG) engaged SBG Technology Solutions, Inc. (SBG) to conduct an independent evaluation of the DNFSB's overall information security program and practices to respond to the FY 2020 IG FISMA Reporting Metrics. In FY 2020, we evaluated the effectiveness of the DNFSB's information security controls, including its policies, procedures, and practices on the agency's General Support System (GSS) information system. 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 DNFSB'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 the effectiveness of the information security policies, procedures, and practices of the DNFSB. To achieve this objective, we evaluated the effectiveness of the DNFSB's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether the DNFSB's overall information security program and practices were effective and consistent with the requirements of the FISMA, the Department of Homeland Security (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) 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 the Department of Homeland Security. We conducted our independent evaluation in accordance with the Council of the Inspectors General on 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 (CISO), Chief Information Officer (CIO), and Senior Systems Administrators 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). Other reviewed artifacts included: The DNFSB GSS System Security Plan (dated 2016), Gap Analyses, Security Assessment Reports, Authorizations to Operate, and Plan of Actions and Milestones (POA&Ms).

Table 1: Testing Method and Descriptions

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

FISMA 2014 Reporting Metrics

The OMB, the DHS, and the CIGIE developed the FY 2020 IG FISMA Reporting Metrics in a collaborative effort - and in consultation with - the Federal Chief Information Officers Council. 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 includes the DHS in-scope reporting metric domains for the evaluation.[5]

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

Table 2: Aligning the Cybersecurity Framework with the FY 2020 IG FISMA Metric Domains

Cybersecurity Framework Function	FY 2020 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 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. 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 function area and/or the agency's information security program is effective at a maturity level lower than Level 4. According to DHS's criteria, SBG determined that the 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 the FISMA, OMB policy and guidelines, and NIST standards and guidelines.

III. EVALUATION RESULTS

This report provides the results of SBG Technology Solutions' independent evaluation of the DNFSB's 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 considered an effective level of security at the domain, function, and overall program level. **Error! Not a valid bookmark self-reference.** summarizes the overall assessed maturity levels for the DNFSB's information security program.

Table 4: Assessed Maturity Levels for the 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**
Overall Security Program Effectiveness	**Effective**

The subsequent section below provides a summary of our findings and our recommendations by domain for the DNFSB to consider as the agency works to remediate them and mature their information security program.

Findings

Although the DNFSB established an agency-wide information security program and practices, we identified weaknesses that may have some impact on the agency's ability to adequately protect the 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 the FISMA, we believe the DNFSB should strengthen its information security program by considering the following findings and recommendations:[6]

A. Function Area: Identify

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

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

  a) The DNFSB was in the process of implementing ForeScout, a centralized automated solution for monitoring authorized and unauthorized software and hardware (e.g. switches, routers, printers, mobile devices etc.) connected to the agency's network in near real time. For FY 2020, ForeScout is still not fully implemented across the GSS to centralize system inventory;

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

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

  d) Per management, due to the small size of the 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.

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

  a) The DNFSB did not consistently utilize POA&Ms to effectively mitigate security weaknesses. More specifically, we noted that the POA&Ms that were provided for testing were three (3) years old.

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

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; and,
   d) Conduct a supply chain risk assessment.

3. Using the results of recommendations in bullets one (1) and two (2) above:
   a) Collaborate with the DNFSB's Cybersecurity Team 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 IT Operations;
   b) Utilize guidance from the National Institute of Standards in Technology (NIST) Special Publication (SP) 800-55 (Rev. 1) – *Performance Measurement Guide for Information Security* to establish performance metrics to more effectively manage and optimize all domains of the DNFSB information security program;
   c) Implement a centralized view of risk across the organization; and,
   d) Implement formal procedures for prioritizing and tracking POA&M to remediate vulnerabilities.

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

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

  a) The DNFSB did not consistently document change control board (CCB) meetings or security impact assessments necessary for reviewing and approving configuration changes to the DNFSB's system in accordance with the agency's Configuration Management Plan; and,

  b) 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.

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

  a) Two (2) of a sample of five (5) users selected for testing did not complete nondisclosure agreements prior to system access;

  b) Not all the DNFSB's privileged system accounts are accessed via PIV or an IAL 3 credential;

  c) The DNFSB did not conduct the agency's annual breach response plan exercise; and,

  d) The DNFSB was in the process of developing role-based privacy training.

Recommendations:

5. Conduct remedial training to re-enforce requirements for documenting CCB's approvals and security impact assessments for changes to the DNFSB's system in accordance with the agency's Configuration Management Plan.

6. Implement procedures and define roles for reviewing configuration change activities to the DNFSB's information system production environment by those with privileged access to verify the activity was approved by the system CCB and executed appropriately.

7. Implement a technical capability to restrict new employees and contractors from being granted access to the DNFSB's systems and information until a non-disclosure agreement is signed and uploaded to a centralized tracking system.

8. Implement the technical capability to require PIV or Identification and Authentication Level of Assurance (IAL) 3 to all DFNSB privileged accounts.

9. Implement automated mechanisms (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.

10. Continue efforts to develop and implement role-based privacy training.

11. Conduct the agency's annual breach response plan exercise for FY 2021.

C. Function Area: Detect

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

a) The DNFSB has not documented standard operating procedures for the use of the agency's continuous monitoring tools or updated the continuous monitoring plan to include the use of new monitoring tools.

Recommendation:

12. Continue 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 carried over from our FY 2019 assessment that the DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize the DNFSB's Respond domain of the agency's information security program:

a) Although the DNFSB had an incident response plan in place, it does not fully define profiling techniques for identifying incidents or strategies for containing all types of major incidents.

Recommendation:

13. Update the DNFSB's incident response plan to include profiling techniques for identifying incidents and strategies to contain all types of major incidents.

E. Function Area: Recover

We noted the following weaknesses that carried over from our FY 2019 assessment that the DNFSB should consider in the agency's efforts to more effectively manage, measure, and optimize the DNFSB's Recover domain of the agency's information security program:

a) As per management, because the DNFSB only has one information system in its inventory, the DNFSB has not invested in an automated mechanism to more thoroughly and effectively test the agency's information system contingency plan and,

b) The DNFSB does not address Information and Communication Technology (ICT) supply chain concerns into its contingency planning policies and procedures.

Recommendation:

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

IV. CONCLUSION

Most of the IG FISMA metric and maturity level indicators for each metric are directed to large agencies with the resources and risk that would require that they meet level four (4) maturity to be effective. Having procured a third-party assessment of the agency information security program, the DNFSB is aware of the risk to the agency's information system and information. Due to the small nature of the agency and its population of network users, the DNFSB's key risk management personnel are intimately involved in all aspects of the DNFSB's information security program and are aware of every important decision involving risk to the agency's information system, information, and mission. This includes having implemented or developed plans to address this risk. As a result, although the DNFSB has not achieved a level 4 calculated maturity level, the DNFSB's information security program is overall effective.

V. AGENCY COMMENTS

An exit briefing was held with the agency on March 15, 2021. 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 Technology Solutions focused the FISMA 2014 evaluation approach on federal information security guidelines developed by the DNFSB, the NIST, and the OMB. NIST SP 800 series provide guidelines that were considered essential to the development and implementation of the DNFSB's information security program. The following is a listing of the criteria used in the performance of the FY 2020 FISMA 2014 evaluation:

DNFSB

- OP-411.2-2 *Identification and Authentication Operating Procedures*
- Draft OP 411.2-X *Security Awareness and Training Operating Procedures*
- D-312.1 *Insider Threat Program Directive*
- OP 412-1 *Acceptable Use of DNFSB Information Technology*
- Cybersecurity Directive, *Version One*
- D-21.1 *Directives Program*
- OP-21-1-1 *Directive and Supplementary Document Procedures*
- Continuous Monitoring Policies and Procedures, *Version One*
- OP-242-1 *Personal Property Directive*
- D-260-2 *Privacy Program Directive*
- D-410.1 IT Program, *Version Three*
- OP-411-2-1 *Information Systems Risk Management Framework and Security Authorization Handbook*
- OP-411-2-1 *Information System Security Program Certification and Accreditation*

NIST SP and Federal Information Processing Standards (FIPS)

- 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-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-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*

- 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*