MEMORANDUM

December 21, 2021

TO: Joel C. Spangenberg
Executive Director of Operations

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

SUBJECT: INDEPENDENT EVALUATION OF THE DNFSB'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2021 (DNFSB-22-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 2021. 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 2021*. The 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 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. On December 13, 2021, prior to the December 16, 2021, exit conference, the agency staff indicated that they had formal comments for inclusion in this report. These comments and the SBG's response to the comments are included as report appendices.

For the period October 1, 2020 through September 30, 2021, SBG found that while the DNFSB 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 DNFSB's system and information.

Please provide information on actions taken or planned on each of the recommendations within 30 calendar days of the date of this report. Actions taken or planned are subject to OIG follow-up as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions, please call me at (301) 415-5915 or Terri Cooper, Team Leader at (301) 415-5965.

Attachment: As stated

Independent Evaluation of the DNFSB's Implementation of FISMA 2014 For Fiscal Year 2021

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) 2021 Inspector General (IG) FISMA Reporting Metrics. In FY 2021, 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. For the evaluation, we used the FISMA and other federal regulations, standards, and guidance.

Findings

While the DNFSB established an effective agency-wide information security program and practices, we identified weaknesses 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 the twenty-four recommended remedial actions. The DNFSB management provided formal comments to our independent evaluation (See Appendix A of the report).

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	Group Support System
ICT	Information Communications Technology
IAM	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
SCRM	Supply Chain Risk Management
SP	Special Publication
ST	Security Training
VDP	Vulnerability Disclosure Policy

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 2021 IG FISMA Reporting Metrics. In FY 2021, we evaluated the effectiveness of the DNFSB's information security controls, including its policies, procedures, and practices on the agency's Group Support System (GSS) information system. We used the FISMA[1] and other regulations, standards, and guidance referenced in the FY 2021 IG FISMA Reporting Metrics as the basis for our evaluation of the 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*

[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).

Information Systems and Organizations, and the FISMA 2014 guidance from the Office of Management and Budget (OMB), and 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.

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 2: 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 tools, 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 2021 IG FISMA Reporting Metrics in a collaborative effort - and in consultation with - the Federal Chief Information Officers Council. The FY 2021 metrics continue using the maturity model approach for all security domains and are fully aligned with the NIST Framework for Improving Critical Infrastructure Cybersecurity

(Cybersecurity Framework) function areas. Table includes the DHS in-scope reporting metric domains for the evaluation.[5]

Table 2: Aligning the Cybersecurity Framework with the FY 2021 IG FISMA Metric Domains

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

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

In FY 2021, the CIGIE, in partnership with the OMB and the DHS, continued refining these metrics. The metrics consisted of specific questions (performance metrics) for each metric domain and the descriptions of the five maturity levels for each metric. Table includes the DHS' general description of the five maturity levels.

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

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 maturity level lower than Level 4. According to the DHS's criteria, the 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 the SBG Technology Solutions independent evaluation of the DNFSB's IT security program and practices required by FISMA 2014, based on the FY 2021 IG FISMA Reporting Metrics that use the maturity model indicators. According to DHS criteria, Level 4, *Managed and Measurable*, is 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* *Supply Chain Risk Management*	**Level 2** **Level 1**
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 2**
RESPOND *Incident Response (IR)*	**Level 2**
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 finding and recommendations:[6]

A. Function 1A: Identify – Risk Management

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

- In FY 2021 we noted the following findings carried over from our FY 2020 assessment as the DNFSB had not yet remediated them:

    1. The DNFSB defined its information security architecture and how this architecture is integrated with the enterprise architecture in the Board General Support System, System Characterization Document. However, this document had not been updated since August 2015 despite a number of changes having been made to the Agency's information security and enterprise architectures.

    2. The DNFSB did not consistently utilize POA&Ms to effectively mitigate security weaknesses. More specifically, POA&Ms could not be provided for the FY2021 testing period.

    3. The DNFSB has defined the roles and responsibilities of internal and external stakeholders involved in the risk management processes in the Agency's Risk Management Framework document. However, the Risk Management Framework document has not been updated since July 2016 and did not reflect the roles and responsibilities in the Agency's current environment.

    4. The DNFSB developed and is consistently implementing its plan to onboard to the Department of Homeland Security Continuous Diagnostics and Mitigation (DHS CDM) dashboard where continuous vulnerability scanning results and other security risk will be viewed and used for internal and external reporting. However, this plan

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

does not yet address dashboard solution for monitoring risk control and remediation activities, dependences, and risk scores/levels.

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

    5. A Risk Assessment Report could not be provided for the FY2021 testing period. It was noted that the DNFSB is currently undergoing a re-validation of their Authorization to Operate (ATO).

Recommendations:

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

    1. Update the ISA and use the updated ISA to:

        a. Assess enterprise, business process, and information system level risks;
        b. Update enterprise, business process, and information system level risk tolerance and appetite levels necessary for prioritizing and guiding risk management decisions.

    2. Using the results of recommendations one above:

        a. Utilizing 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 manage and optimize all domains of the DNFSB information security program more effectively;
        b. Implement a centralized view of risk across the organization;
        c. Implement formal procedures for prioritizing and tracking POA&Ms to remediate vulnerabilities.

- In FY 2021 we noted the following recommendations:

    3. Update the Risk Management Framework to reflect the current roles, responsibilities, policies, and procedures of the current DNFSB environment, to include:

        a. Defining a frequency for conducting Risk Assessments to periodically assess agency risks to integrate results of the assessment to improve upon mission and business processes.

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

We noted the following weakness that the DNFSB should consider in their efforts to effectively manage, measure, and optimize the Supply Chain Risk Management domain and overall information security program:

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

    1. The DNFSB has not developed a Supply Chain Risk Management strategy or policies and procedures to manage supply chain risks.

Recommendations:

- In FY 2021 we noted the following recommendation:

    4. Define a Supply Chain Risk Management strategy to drive the development and implementation of policies and procedures for:

        a. How supply chain risks are to be managed across the agency;
        b. How monitoring of external providers compliance with defined cybersecurity and supply chain requirements;
        c. How counterfeit components are prevented from entering the DNFSB supply chain.

C. Function 2A: Protect – Configuration Management

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

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

    1. The DNFSB Configuration management plan has not been integrated with its risk management and continuous monitoring programs and does not utilize lessons learned to make improvements to this plan.

    2. The DNFSB did not consistently consider security impacts prior to change implementation.

Recommendations:

- In FY 2021 we noted the following recommendations:

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

    6. Integrate the Configuration management plan with risk management and continuous monitoring programs and utilize lessons learned to make improvements to this plan.

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

We noted the following weaknesses that the DNFSB should consider in its efforts to manage, measure, and optimize the DNFSB's Identity and Access Management domain of the agency's information security program:

- In FY 2021 we noted the following findings carried over from our FY 2020 assessment as the DNFSB had not yet remediated them:

    1. The DNFSB does not employ 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.

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

    2. The DNFSB had not fully implemented a data loss prevention tool to limit unauthorized data transfer or exfiltration across the agency's Microsoft Office 365 environment.

    3. The DNFSB has not developed milestones that describe how the agency will align with all aspects of Federal initiatives, including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.

Recommendations:

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

7. 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.

- In FY 2021 we noted the following recommendations:

8. Continue efforts to implement data loss prevention functionality for the Microsoft Office 365 environment.

9. Update agency strategic planning documents to include clear milestones for implementing strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program.

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

We noted the following weaknesses that the DNFSB should consider in its efforts to manage, measure, and optimize the DNFSB's Data Privacy and Protection domain of the agency's information security program:

- In FY 2021 we noted the following findings carried over from our FY 2020 assessment as the DNFSB had not yet remediated them:

1. The DNFSB did not implement role-based training for individuals with significant privacy or data protection related responsibilities.

2. The DNFSB did not conduct a tabletop or functional exercise of its data breach response plan.

Recommendations:

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

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

11. Continue efforts to develop and implement role-based privacy training for users with significant privacy or data protection related duties.

F. Function 2D: Protect – Security Training

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

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

    1. The DNFSB did not have formally documented requirements and procedures for the completion of role-based training or enforcement methods in place for individuals who do not complete role-based training.

Recommendation:

- In FY 2021 we noted the following recommendation:

    12. Formally document requirements and procedures for the completion of role-based training and enforcement methods in place for individuals who do not complete role-based training.

G. Function 3: Detect – Information Security Continuous Monitoring

We noted the following weakness that the DNFSB should consider in its efforts to effectively manage, measure, and optimize the DNFSB's Information System Continuous Monitoring domain of the agency's information security program;

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

    1. The DNFSB did 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.

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

    2. The DNFSB ISCM policies & procedures were out of date and did not clearly define what needs to be monitored or how; existing procedures focus almost exclusively on monitoring the internal network and do not address external systems like Office 365;

    3. The DNFSB did not consistently implement its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the

organizational security posture, as well as each system's contribution to said security posture;

4. The DNFSB had not defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.

Recommendations:

- In FY 2021 we noted the following recommendations:

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

14. Update the DNFSB ISCM policies and procedures clearly defining what needs to be monitored at the system and organization level.

15. Define standard operating procedures for the use of the agency's continuous monitoring tools or update the continuous monitoring plan to include the use of new monitoring tools.

16. Defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program.

H. Function 4: Respond – Incident Response

We noted the following weakness that carried over from our FY 2020 assessment that the DNFSB should consider in its efforts to effectively manage, measure, and optimize the DNFSB's Incident Response domain of the agency's information security program:

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

1. The DNFSB did not define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents;

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

2. The DNFSB did not test its Incident response plan in FY21.

3. The DNFSB did not update its incident response plan to reflect the USCERT incident reporting guidelines.

4. The DNFSB did not have adequate resources to manage its incident response activities.

5. The incident response tools in place were not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

Recommendations:

- In FY 2021 we noted the following recommendations:

17. Define handling procedures for specific types of incidents, processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed for prioritizing incidents.

18. Consistently test the Incident response plan annually.

19. Update the Agency's incident response plan to reflect the USCERT incident reporting guidelines.

20. Allocate and train staff with significant incident response responsibilities.

21. Configure all incident response tools in place to be interoperable, can collect and retain relevant and meaningful data that is consistent with the incident response policy, plans and procedures.

I. Function 5: Recover – Contingency Planning

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

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

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

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

    2. The DNFSB did not measure the effectiveness of its contingency planning activities using performance metrics or dashboards;

    3. The DNFSB did not perform a business impact assessment within at least every two years or incorporate the results of such an assessment into its strategy and mitigation planning activities;

    4. The DNFSB did not implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.

Recommendations:

- In FY 2021 we noted the following recommendations:

    22. Develop and track metrics related to the performance of contingency planning and recovery related activities.

    23. Conduct a business impact assessment within every two years to assess mission essential functions and incorporate the results into strategy and mitigation planning activities.

    24. Implement role-based training for individuals with significant contingency planning and disaster recovery related responsibilities.

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. Due to the small organizational structure, The DNFSB can operate and communicate more efficiently and effectively compared to larger Federal agencies. 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. The DNFSB should continue to formalize its information security program by fully developing documenting standard operating procedures for security controls in place to manage the risk to The DNFSB's information system, information, and missions. 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 December 16, 2021. Prior to this meeting, the DNFSB management reviewed a discussion draft and provided comments that have been incorporated into this report as appropriate.

On December 13, 2021, the DNFSB provided formal comments to the draft report that stated its disagreement with the findings and recommendations.

Appendix A contains a copy of the agency's formal comments. Appendix B contains the OIG response to agency's formal comments.

Appendix – Criteria

SBG Technology Solutions focused the FY 2021 IG FISMA 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 2021 IG FISMA 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;*
- The Board General Support System, System Characterization Document;
- 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 Interagency Report 8286, *Integrating Cybersecurity and Enterprise Risk Management.*
- NIST Interagency Report 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework.*
- *NIST Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.
- Other Federal guidance and standards cited in the DHS annual FISMA IG reporting Metrics.

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-20-32, Improving Vulnerability Identification, Management and Remediation.
- OMB Memorandum M-21-02, Fiscal Year 2020-2021 *Guidance on Federal Information Security and Privacy Management Requirements.*
- OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.
- OMB Circular No. A-130, *Managing Information as a Strategic Resource***.**

Appendix A

AGENCY FORMAL COMMENTS

DEFENSE NUCLEAR FACILITIES SAFETY BOARD
Washington, DC 20004-2901

December 13, 2021

DNFSB COMMENTS IN RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL 2021 AUDIT OF IMPLEMENTATION OF FISMA

The Office of the Inspector General (OIG) through a contractor conducted an audit of the Defense Nuclear Facilities Safety Board's (DNFSB) implementation of the cybersecurity requirements in the Federal Information Security Modernization Act of 2014 (FISMA). This audit is a welcome independent review of the cybersecurity posture of the DNFSB, and is an important tool to assist the agency in improving and sustaining cybersecurity in its information systems. The effectiveness of the information security policies, procedures, and practices is a high priority of the DNFSB. While we are glad that the audit found our program overall effective, we agree with the majority of OIG findings and recommendations for improving weaknesses and hardening our program against potential threats.

The DNFSB, as a very small agency does not have a complex information technology system compared to larger agencies, nor does DNFSB have substantial holdings of sensitive information to protect. However, as noted by the OIG in its audit report, the DNFSB must still comply with the extensive requirements of FISMA, Department of Homeland Security, and other federal regulations, many of which do not correlate to the small size and simplicity of the DNFSB IT system. DNFSB will continue to ensure that it implements the requirements in an effective manner for its IT system.

For the 2021 FISMA audit the OIG took a hard look at the DNFSB FISMA program. This review corresponded with new office management, turnover in the Chief Information Officer position, turnover in the Chief Information Security Officer position, and poor attention to cyber security risks in prior years. While the OIG recognized that the agency has made progress on many repeat findings from the prior year, the timing of the audit did not provide an opportunity to fully close out prior findings resulting in a repeat of many prior year findings. As the OIG notes, these issues need to be resolved through corrective actions. In the current report, the OIG only failed to accurately capture the status of compliance with requirements for a few items. The OIG finds in the report that "DNFSB did not have formally documented requirements and procedures for the completion of role-based training or enforcement methods in place for individuals who do not complete role-based training." This finding is referring to IT personnel with privileged access to the IT system. Unfortunately, despite being provided with evidence that the agency complied with the FISMA standards by ensuring that all privileged account holders completed the required annual training, the OIG incorrectly considered informal internal deadlines to be the FISMA requirement rather than the actual completion of the annual training. Further, the OIG disregarded evidence that if the personnel had not completed the required training, their privileged account access would have been suspended. Thus, the finding and recommended corrective action for this issue are invalid.

With respect to incident response, the DNFSB faced several situations of potential breaches through which it exercised its processes for responding to breaches. While the agency, due to its size and the limited holdings of its IT system does not regularly experience direct security incidents, the IT and security teams routinely follow government-wide situations to ensure that our agency is prepared for internal incidents. For example, the DNFSB staff closely tracked several external cyber attacks such as SolarWinds. In each instance, the staff examined the information concerning the attack, determined applicability and potential impact to DNFSB systems, and although they determined that no breach or vulnerability existed, considered how to further harden our system against such attacks. Further, during FY 2021, the DNFSB specifically engaged in continuity of operations exercises with substantial IT system injects designed to test our ability to respond to and overcome system failures and cyber security attacks. Overall, these efforts meet the objectives of FISMA and other requirements, but did not demonstrate to the OIG's satisfaction that the FISMA audit metrics were met by the agency. The undue reliance on audit metrics rather than performance objectives does not adequately assess the true preparedness of the DNFSB system or team.

The DNFSB team will continue to work toward an effective, optimized IT system and cyber security posture that hardens the system against attack, prepares for incidents, and continues to implement new controls and technologies. We look forward to continued engagement with the OIG to close out the findings and recommendations from the FY 2021 FISMA audit.

James Biggins
General Manager

JAMES BIGGINS

Digitally signed by JAMES BIGGINS
Date: 2021.12.13 19:24:25 -05'00'

Appendix B

THE OIG RESPONSE TO AGENCY FORMAL COMMENTS

December 16, 2021

Subject: Response letter to the Defense Nuclear Safety Board (DNFSB) Information Security Programand Practices for Fiscal Year 2021 Feedback

Reference a: DNFSB letter of 13 December Regarding Subject Independent Evaluation

1. In response to reference a, SBG Technology Solutions Incorporated (SBG) conducted an independent evaluation of DNFSB's information security program and practices (the program) to determine whether they were effective and consistent with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), as defined by the Department of Homeland Security (DHS) for the period October 1, 2020, through September 30, 2021 (the "independent evaluation objective"). The applicable criteria are set forth in FISMA and Office of Management and Budget (OMB) policy and guidelines, and National Institute of Standards and Technology standards and guidelines, in addition to applicable criteria that are identified in the body of this report and the accompanying report. It is the responsibility of DNFSB's managementto conduct the program in accordance with the criteria and program objectives. SBG's responsibility in accordance with our issued contract, is to report our findings and conclusions related to the objective of the independent evaluation.

2. Our independent evaluation involved performing procedures to obtain evidence about DNFSB's program to determine whether it was effective and consistent with the requirements of FISMA. Thenature, timing, and extent of the procedures selected depend on our subject matter expertise objective judgment. We believe the evidence we have obtained provides a reasonable basis for our findings and conclusions based on the objective of our

independent evaluation.

3. Reference a's response to our findings, which is presented in an attachment to this report, referencesthat DNFSB was subjected to an audit. To clarify, DNFSB was subjected to an independent evaluation by SBG, not an audit. Furthermore, the evidence of documented role-based cybersecuritytraining procedures and exercises of DNFSB's incident response program discussed in reference a, was not subjected to the procedures applied in the independent evaluation, and accordingly, we express no conclusion on the Agency's response.

4. Should you have any questions or require any additional information, please contact the undersigned at tfelten@sbgts.com or 703-299-9093 (Office); 443.939.5002 (Cell).

Tom Felten, PMP

President and Chief Executive Officer

1737 King Street, Suite 601,
Alexandria, VA 22314 Office|
703.299.9093|Fax |703.299.9240|

www.sbgts.com