OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Independent Evaluation of the Board's Implementation of the Federal Information Security Management Act for Fiscal Year 2014

DNFSB-15-A-02

November 12, 2014

All publicly available OIG reports (including this report) are accessible through NRC's Web site at
http://www.nrc.gov/reading-rm/doc-collections/insp-gen

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

OFFICE OF THE INSPECTOR GENERAL

November 12, 2014

MEMORANDUM TO: Mark T. Welch
General Manager

FROM: Stephen D. Dingbaum **/RA/**
Assistant Inspector General for Audits

SUBJECT: INDEPENDENT EVALUATION OF THE BOARD'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2014 (DNFSB-15-A-02)

Attached is the Office of the Inspector General's (OIG) report titled *Independent Evaluation of the Board's Implementation of the Federal Information Security Management Act for Fiscal Year 2014*.

The report presents the results of the subject evaluation. Following the November 5, 2014, exit conference, Board staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum.

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 Beth Serepca, Team Leader, at (301) 415-5911.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

DNFSB-15-A-02

November 12, 2014

Results in Brief

Why We Did This Review

The Federal Information Security Management Act (FISMA) of 2002 outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.

FISMA requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor. The Office of Management and Budget (OMB) requires OIG to report its responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

The evaluation objective was to perform an independent evaluation of the Board's implementation of FISMA for FY 2014.

Independent Evaluation of the Board's Implementation of FISMA for Fiscal Year 2014

What We Found

The Board has issued a directive and operating procedure for implementing its information systems security program (ISSP). However, the majority of the policies and procedures supporting the Board's ISSP are draft documents and, therefore, have not been fully implemented. While the Board's ISSP includes all of the elements required by FISMA, OMB, and the National Institute of Standards and Technology (NIST), we were not able to evaluate fully every element of the Board's ISSP due to the lack of final, approved policies and procedures. We were able to evaluate some elements of the Board's ISSP and identified the following ISSP weaknesses:

- Continuous monitoring is not performed as required.
- The security assessment and authorization of the Board's general support system did not follow the NIST risk management framework.
- The Board's plan of action and milestones management is inadequate.
- Oversight of systems operated by contactors or other agencies is inadequate.

What We Recommend

We made recommendations to improve the Board's ISSP and implementation of FISMA. Management stated their general agreement with the findings and recommendations in this report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS i

I. BACKGROUND 1

II. OBJECTIVE 2

III. FINDINGS 2

A. Continuous Monitoring Is Not Performed as Required 4

Recommendations 8

B. The NIST RMF Was Not Followed 9

Recommendations 12

C. POA&M Management Is Inadequate 13

Recommendations 16

D. Oversight of Contractor Systems Is Inadequate 17

Recommendations 21

IV. CONSOLIDATED LIST OF RECOMMENDATIONS 23

V. BOARD COMMENTS 25

APPENDIX

OBJECTIVE, SCOPE, AND METHODOLOGY 26

TO REPORT FRAUD, WASTE, OR ABUSE 29

COMMENTS AND SUGGESTIONS 29

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
Board	Defense Nuclear Facilities Safety Board
CIO	Chief Information Officer
CDM	Continuous Diagnostics and Mitigation
CSP	Cloud Security Provider
DHS	Department of Homeland Security
DNFSB	Defense Nuclear Facilities Safety Board
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSS	General Support System
ISCM	Information Security Continuous Monitoring
ISSP	Information Systems Security Program
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
P-ATO	Provisional ATO
PMO	FedRAMP Program Management Office
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SP	Special Publication

I. BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002.[1] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. The evaluation also must include an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines. FISMA requires the annual evaluation to be performed by the agency's Office of the Inspector General (OIG) or by an independent external auditor.[2] Office of Management and Budget (OMB) memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated November 18, 2013, and OMB M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, require OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Congress in 1988 (PL 100-456) created the Defense Nuclear Facilities Safety Board (Board) as an independent Executive Branch agency to identify the nature and consequences of potential threats to public health and safety at the Department of Energy's defense nuclear facilities, elevate those issues to the highest levels of authority, and inform the public. In operation since October 1989, the Board reviews and evaluates the content and implementation of health and safety standards, as well as

[1] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E Government Act of 2002 (Public Law 107-347) and replaces the Government Information Security Reform Act, which expired in November 2002.

[2] While FISMA uses the language "independent external auditor," OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, clarified this requirement by stating, "Within the context of FISMA, an audit is not contemplated. By requiring an evaluation but not an audit, FISMA intended to provide Inspectors General some flexibility…."

other requirements, relating to the design, construction, operation, and decommissioning of the Department of Energy's defense nuclear facilities.

The U.S. Nuclear Regulatory Commission (NRC) Inspector General holds the position of Inspector General for the Board.[3] The NRC OIG retained Richard S. Carson & Associates, Inc., to perform an independent evaluation of the Board's implementation of FISMA for fiscal year (FY) 2014. This report presents the results of that independent evaluation. Carson Associates will also submit responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool in accordance with OMB guidance.

II. OBJECTIVE

The evaluation objective was to perform an independent evaluation of the Board's implementation of FISMA for FY 2014. The report appendix contains a description of the evaluation objective, scope, and methodology.

III. FINDINGS

The Board has issued two documents for implementing its information systems security program (ISSP) – Directive D-411.2, *Information Systems Security Program*, and Operating Procedure OP-411.2-1, *Information Systems Security Program Certification and Accreditation Operating Procedures*. However, the majority of the policies and procedures supporting the Board's ISSP are draft documents, and therefore, have not been fully implemented. While the Board's ISSP includes all of the elements required by FISMA, OMB, and the National Institute of Standards and Technology (NIST), the evaluation team was not able to evaluate fully every element of the Board's ISSP due to the lack of final, approved policies and procedures.

[3] The Consolidated Appropriations Act, 2014 (Public Law 113-76), signed January 17, 2014, authorized the NRC Inspector General to exercise the same authorities with respect to the Board as the Inspector General exercises under the Inspector General Act of 1978 (5 U.S.C. App.) with respect to the NRC.

The evaluation team was able to evaluate some elements of the Board's ISSP and identified the following ISSP weaknesses:

- Continuous monitoring is not performed as required.
- The security assessment and authorization of the Board's general support system (GSS) did not follow the NIST risk management framework (RMF).
- The Board's plan of action and milestones (POA&M) management is inadequate.
- Oversight of systems operated by contactors or other agencies is inadequate.

A. Continuous Monitoring Is Not Performed as Required

Step 6 of the NIST RMF, ongoing or continuous monitoring, is a critical part of organization-wide risk management. A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. The Board's ISSP, as outlined in D-411.2 and OP-411.2-1, includes requirements for the monitoring of information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. The Board's GSS was issued an authorization to operate (ATO) October 3, 2012; however, the required continuous monitoring activities have not been performed, as the Board has not fully implemented an enterprise-wide continuous monitoring program. As a result, the Board cannot ensure the effectiveness of the GSS information security controls.

What Is Required

Federal and Internal Guidance

Federal Guidance Regarding Continuous Monitoring

FISMA requires that agencies establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA emphasizes the importance of continuously monitoring information system security by requiring agencies to conduct security control assessments at a frequency depending on risk, but no less than annually. FISMA also mandates that agencies follow NIST standards and guidelines to establish and secure that framework.

NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Step 6 of the RMF, ongoing or continuous monitoring, is a critical part of that risk management process.

Key activities performed during Step 6 include:

- Determining the security impact of proposed or actual changes to the information system and its environment of operation.

- Assessing a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

The implementation of a continuous monitoring program results in ongoing updates to the security plan (including the risk assessment), the security assessment report, and the POA&M.

OMB Memorandum M-14-03 requires agencies to develop and maintain an information security continuous monitoring (ISCM) strategy and implement an ISCM program in accordance with NIST. In conjunction with this effort, the Department of Homeland Security (DHS) established a Continuous Diagnostics and Mitigation (CDM) program. DHS will provide participants in the CDM with access to resources, such as tools and documentation, to support ISCM.

Internal Guidance Regarding Continuous Monitoring

As stated in D-411.2, the Board is required to perform the following continuous monitoring activities:

- Periodically assess security controls to determine if the controls are effective in their application and monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

- Periodically assess the risk resulting from the operation of information systems and the associated processing, storage, or transmission of information.

- Develop, document, periodically update, and implement plans for information systems that describe the security controls in place or planned and the rules of behavior for individuals accessing the information systems.

OP-411.2-1 requires monitoring information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. It describes the requirements for the ongoing monitoring of security controls, including periodic security control assessments, updating security authorization documentation, and performing POA&M reviews. POA&Ms must be updated monthly, and security plans at least annually.

What We Found

Noncompliance With Continuous Monitoring Guidance

The Board's GSS was issued an ATO on October 3, 2012; however, the required continuous monitoring activities have not been performed.

Security Impact Analyses Were Not Performed

A key activity performed during Step 6 of the NIST RMF is determining the security impact of proposed or actual changes to the information system and its environment of operation. Security impact analysis often includes an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Changes could be due to the addition of new technologies, the upgrade of existing technologies, or changes in policy or guidance. There have been several changes to the Board GSS and its environment of operation and no security impact analyses have been performed. For example, a new mobile device management system was put into place, the SharePoint infrastructure was updated, and the backup infrastructure was updated.

In April 2013, NIST issued SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Agencies have 1 year from the publication date of a revision to a standard to comply with the new standard. The Board has not performed a security impact analysis of the changes to NIST SP 800-53.

Annual Security Control Assessments Were Not Performed

Continuous monitoring also includes assessing a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the

organization-defined monitoring strategy. The GSS security plan states that security controls will be assessed at least annually. However, no security control assessments have been conducted on the GSS since the ATO was issued in 2012.

Security Authorization Documents Were Not Updated

The implementation of a continuous monitoring program results in ongoing updates to the security plan (including the risk assessment), the security assessment report, and the POA&M. There have been no updates to the GSS security plan, risk assessment, or security assessment report since the ATO was issued in 2012. The POA&M has not been updated as required. See finding C for additional details on POA&M management.

Why This Occurred

Enterprise-Wide Continuous Monitoring Program Is Not Fully Implemented

D-411.2 and OP-411.2-1 include requirements for continuous monitoring, but they do not include detailed procedures for ensuring required continuous monitoring activities are performed. As a participant in the DHS CDM, the Board was waiting for DHS to provide an ISCM template to use in developing their ISCM strategy and program. As DHS had not yet issued the template (which DHS has recently decided not to issue at all), the Board developed its own ISCM strategy, which remains in draft pending review. Lack of a continuous monitoring program was identified as a security weakness during the authorization of the Board GSS. There is an open POA&M item for developing and implementing an ISCM strategy and program.

Why This Is Important

Board Cannot Ensure Effectiveness of Security Controls

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly

dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. If continuous monitoring activities are not performed as required, the Board cannot ensure the effectiveness of the GSS information security controls.

Recommendations:

OIG recommends that the Board

1. Perform an annual security control assessment of the GSS. Since the Board has not identified the process for identifying which sub-set of controls should be tested each year, for FY 2015, OIG recommends the following controls should be tested at a minimum:

   - Any controls that are new or changed in NIST SP 800-53 Revision 4.
   - Any security control enhancements not tested during the 2012 security assessment.
   - Any controls impacted by changes to the GSS environment since the security assessment conducted in 2012.
   - Any controls associated with closed POA&M items.

2. Update the GSS security authorization documentation (e.g., security plan, risk assessment, security assessment report) as required.

B. The NIST RMF Was Not Followed

The NIST RMF is a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Step 4 is to assess the system's security controls and Step 5 is to authorize the system to operate. OP-411.2-1 describes the procedures for assessing security controls and authorizing systems to operate. The Board's GSS was issued an ATO October 3, 2012; however, a review of the authorization package documents found that key elements of the NIST RMF were not followed. As a result, the Board's risk response to the findings from the system authorization may be inadequate.

What Is Required

Federal and Internal Guidance

NIST RMF

The NIST RMF is a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. NIST SP 800-37, Revision 1, describes the process of applying the RMF to Federal information systems and includes a set of well-defined tasks for completing each step of the framework.

Step 4 of the RMF is to assess the system's security controls in accordance with the assessment procedures defined in the security assessment plan and to document the issues, findings, and recommendations in a security assessment report. During this step, the system security plan is updated based on the findings from the security control assessment. The updated security plan reflects the actual state of the security controls after the initial assessment.

Step 5 of the RMF is to authorize the system to operate. During this step, the authorizing official determines the risk to operations based on the findings from the assessment performed in Step 4, and determines if that risk is acceptable.

Board RMF

OP-411.2-1 describes the procedures for assessing security controls and authorizing systems to operate. Assessors must use the assessment methods and procedures described in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Appropriate responses to findings from the security assessment report are added to the system's security plan.

The Board developed the *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook* to facilitate the implementation of the RMF and security authorization processes within the Board. However, this document is still a draft and has not been formally adopted.

What We Found

NIST RMF Not Followed

The Board's GSS was issued an ATO in October 2012. Included in the authorization package were a system security plan, a risk assessment spreadsheet, and a security assessment report. A review of these documents found that key elements of the NIST RMF were not followed.

Security Assessment Report Did Not Include Control Enhancements

The GSS security assessment report describes a methodology for conducting the security assessment, including which security controls and security control enhancements are to be tested. However, the security assessment report does not include any results for testing the effectiveness of security control enhancements. There are more than 60 potential control enhancements for which security assessment results were not reported. If a security control with multiple enhancements was determined to be partially in place, the report does not clearly indicate which part of the control or enhancement was not properly implemented.

Error in Risk Assessment Resulted in Inaccurate Risk Acceptance

The GSS security assessment report included a risk assessment summary, derived from a separate risk assessment spreadsheet. Risks were designated as high, moderate, or low, based on results from the risk assessment spreadsheet. High and moderate risks were added to the POA&M. Low risks do not appear on the POA&M, as it is general practice to accept these risks due to either reduced budgets and constrained resources, compensating controls, or the environment, which reduce the likelihood of the risk being realized. The risk assessment spreadsheet uses a series of worksheets to calculate risk based on the likelihood and impact of a threat source for the controls not implemented as intended. One of the worksheets from the risk assessment spreadsheet was included in the security assessment report and used to determine which risks would be added to the POA&M (high and moderate) and which risk would be accepted (low). However, due to an error in the formulas on that worksheet, risk calculations from the other worksheets were assigned to the incorrect security controls. A total of 15 security controls identified as moderate risk in the risk assessment were incorrectly identified as low, and therefore accepted, risk in the security assessment report. Conversely, 20 security controls identified as low risk in the risk assessment were incorrectly identified as high or moderate risk in the security assessment report. As a result, the POA&M contains corrective actions for some risks that should have been accepted and does not contain corrective actions for some moderate risks.

Security Plan Not Updated To Reflect Assessment Results and Accepted Risk

The GSS security plan was not updated to reflect the actual state of the security controls after the initial assessment. The Board's ISSP requires appropriate responses to findings from the security assessment report to be added to the system's security plan. For example, the security assessment report recommended accepting the risk for some controls determined to be low risk. The security plan was not updated to indicate which partially implemented controls are an accepted risk.

Why This Occurred

Board RMF Is Not Fully Implemented

OP-411.2-1 describes the procedures for assessing security controls and authorizing systems to operate. The Board developed the *DNFSB Information Systems Risk Management Framework and Security Authorization Handbook* to facilitate the implementation of the RMF and security authorization processes within the Board. However, this document is still a draft and has not been formally adopted.

Why This Is Important

Risk Response May Be Inadequate

The NIST RMF provides an authorizing official with information for determining the risk to operations based on the findings from security assessments in order to determine if that risk is acceptable. Organizations can respond to risk in a variety of ways, including acceptance, avoidance, mitigation, sharing, transfer, or a combination of the above. Because key elements of the NIST RMF were not followed when the Board's GSS was authorized to operate, the Board's risk response to the findings from the system authorization may be inadequate.

Recommendations:

OIG recommends that the Board

3. Reevaluate the risk assigned to the controls impacted by the error in the 2012 GSS risk assessment and update the POA&M as needed.

4. Update the GSS system security plan to document accepted risk.

C. POA&M Management Is Inadequate

FISMA, OMB, and NIST define the requirements for a POA&M process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. The POA&M was updated when the Board's GSS was authorized to operate October 3, 2012. However, the POA&M has not been updated as required, does not include all known security weaknesses, and is missing required information. POA&M management is inadequate because the Board has not developed policies and procedures for POA&M management. As a result, the POA&M is not effective at monitoring the progress of corrective efforts relative to known weaknesses in information technology security controls and therefore does not provide an accurate measure of security program effectiveness.

What Is Required

Federal and Internal POA&M Guidance

Federal POA&M Guidance

FISMA requires agencies to develop, document, and implement a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

NIST requires organizations to implement a process for ensuring POA&Ms, for both the security program and associated organizational information systems, are maintained and document remedial security actions to mitigate risk. Organizations must develop a POA&M for each information system to document the planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. Organizations are required to update POA&Ms on an organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Key OMB POA&M reporting requirements include the following:

- Scheduled completion dates should not be changed.
- All weaknesses should have a scheduled completion date.
- All weaknesses should identify the source of the weakness.
- All closed weaknesses should have an actual completion date.
- Weakness should be reported as delayed once the scheduled completion date has passed.

Internal POA&M Guidance

OP-411.2 requires the Chief Information Officer (CIO) and information system owner to update POA&Ms on a regular basis – at least monthly. It also requires the authorizing official to review all POA&Ms at least quarterly to ensure adequate progress is being made on remediating known findings. The authorizing official can require more frequent reviews if necessary to ensure timely remediation of known findings and to reduce risk to the Board.

OP-411.2 also requires any new findings determined by ongoing security assessments or continuous monitoring to be added to the POA&M and remediated in a timely manner.

What We Found

Noncompliance With POA&M Guidance

POA&M Not Updated As Required

The POA&M was updated when the Board's GSS was issued an ATO October 3, 2012. Subsequent POA&M review and update occurred on October 29, 2012, December 10, 2012, March 4, 2013, September 9, 2013, and January 30, 2014. The Board is not reviewing POA&Ms on a monthly basis and is not consistently reviewing POA&Ms on at least a quarterly basis.

POA&M Does Not Include All Known Security Weaknesses

A vulnerability scan was conducted in conjunction with the security assessment and authorization of the GSS. None of the findings from the vulnerability scan, or subsequent scans, was added to the POA&M.

POA&M Is Missing Required Information

Some of the completed POA&M items do not have an actual completion date.

Why This Occurred

Board ISSP Lacks a POA&M Program

POA&M management is inadequate because the Board lacks policies and procedures for POA&M management. As stated in OP-411.2, the CIO and information system owner are required to update POA&Ms at least monthly and the authorizing official is required to review all POA&Ms at least quarterly. However, OP-411.2 does not include procedures for ensuring POA&Ms are updated as required, include all known security weaknesses, and include required information.

Why This Is Important

Progress of Corrective Efforts Cannot Be Effectively Monitored

POA&Ms are intended to track and monitor known information security weaknesses. POA&Ms that are not updated as required, do not include all known security weaknesses, and are missing required information are not effective at monitoring the progress of corrective efforts relative to known weaknesses in information technology security controls. As a result, the POA&M does not provide an accurate measure of security program effectiveness.

Recommendations:

OIG recommends that the Board

5. Develop, document, and implement POA&M management procedures.

6. Update the POA&M to include all known vulnerabilities and actual completion dates for completed POA&M items.

D. Oversight of Contractor Systems Is Inadequate

FISMA requires agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf. The Board has 11 contractor systems, of which 5 are operated by other Federal agencies and 6 are operated by a commercial vendor. Of the six contractor-operated systems, four are considered cloud-based services. The Board obtained copies of the ATO memoranda for all but one of the agency-operated systems. However, the Board has not authorized any of the contractor-operated systems in accordance with FISMA, NIST RMF, and the Federal Risk and Authorization Management Program (FedRAMP). Oversight of contractor systems is inadequate because the Board has not developed policies and procedures for oversight of contractor systems. As a result, the Board cannot determine whether systems that are owned or operated by contractors or other entities are compliant with FISMA requirements, OMB policy, applicable NIST guidelines, and FedRAMP.

What Is Required

Federal Requirements for Contractor Oversight

As specified in OMB Memorandum M-14-04, agencies must ensure their contractors are abiding by FISMA requirements. Section 3544(a)(l)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services that are provided (in full or in part) by another Federal agency, outsourced to a commercial vendor, and cloud solutions such as software-as-a-service.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed for all contractor systems. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk

assessments, security plans, security control assessments, contingency planning, and security authorization must also be performed for all contractor systems.

Federally Operated Systems

Systems operated by other Federal agencies are required to follow all FISMA and related policy requirements. Interagency agreements, memoranda of understanding, and other similar documents are used to describe the services to be provided and the responsibilities of the agency providing the system or service and the agency utilizing that system or service. To demonstrate federally operated systems meet all FISMA requirements, agencies typically do not perform their own assessments; rather, they request confirmation from the agency that owns or operates the system that the system has been issued an ATO in accordance with the NIST RMF, and has completed required annual contingency plan testing and annual security control testing.

Contractor-Operated Systems

For systems operated by commercial vendors, agencies can leverage the results of industry-specific security assessments performed by an independent auditor or the commercial service provider. However, agencies are still responsible for ensuring all FISMA requirements are implemented for the controls that are also their responsibility. This means that the Board is required to authorize their use of each contractor system and the controls for which they have responsibility. This includes performing all six steps of the NIST RMF.

Cloud Services

On December 8, 2011, OMB issued a memorandum on security authorization of information systems in cloud computing environments. The memorandum established FedRAMP, a Governmentwide program that provides a standard approach to security assessments, authorization, and continuous monitoring for cloud products and services. FedRAMP is mandatory for all Federal agency cloud deployments and service models at the low and moderate risk impact levels.

There are three ways to achieve FedRAMP compliance:

- A Cloud Service Provider (CSP) can submit the appropriate documentation to the FedRAMP Program Management Office (PMO) and to the Joint Authorization Board, which may grant a Provisional Authorization to Operate (P-ATO).

- A CSP can submit the appropriate documentation to the FedRAMP PMO and to an agency, which may grant an agency ATO. Using FedRAMP mechanisms, other agencies can then "leverage" this ATO for use in their agency, decreasing the time for approvals.

- A CSP can use the "CSP supplied" path by submitting the appropriate documentation to the FedRAMP PMO. While this does not grant the CSP, a P-ATO, or an agency ATO, it decreases the time for approvals because documentation and testing (by a third-party assessment organization) are complete and available for agency review.

A cloud system is compliant with FedRAMP if it meets the following requirements:

- The system security package has been created using the required FedRAMP templates.

- The system meets the FedRAMP security control requirements.

- The system has been assessed by an independent assessor.

- A P-ATO, and/or an agency ATO, has been granted for the system.

- An authorization letter for the system is on file with the FedRAMP PMO.

What We Found

Oversight of Contractor Systems Is Inadequate

Federally Operated Systems

The Board has five systems operated by other Federal agencies. The Board obtained copies of the ATO memoranda for all but one of the agency-operated systems. Appropriate agreements are in place, as needed, with agencies operating these systems.

Contractor-Operated Systems

The Board has two systems operated by commercial vendors. The Board has not authorized these systems to operate in accordance with FISMA and the NIST RMF. One of these systems is the Board's financial tracking system. Security controls for these systems have not been documented in a system security plan, and have not been assessed for effective implementation.

Cloud Services

The Board has four systems that are considered cloud-based services. None of the Board's cloud services is currently authorized by FedRAMP. Three of the cloud services are in the process of obtaining FedRAMP authorization. One of these, a mobile device management service, was issued an agency ATO by GSA, who will maintain the ATO through their continuous monitoring program until the responsibility is transitioned to FedRAMP. The agency ATO for the service specifically states that responsibility for implementing security controls is shared by the vendor and the customer agency. Customer agencies leveraging the GSA authorization shall separately authorize the operation of their "instance" for the security controls for which they have responsibility (e.g., user provisioning, access control, etc.). The Board has not performed a separate authorization of their "instance" of the service in accordance with the conditions in the ATO.

Why This Occurred

Board ISSP Lacks Contractor Oversight Process

Oversight of contractor systems is inadequate because the Board lacks policies and procedures for oversight of contractor systems. As stated in D-411.2, the Board's ISSP "establishes policy, requirements, and responsibilities for ensuring an adequate level of information security for all unclassified information collected, created, processed, transmitted, stored, or disseminated on the Board's internal and external information systems." It also states that the Board will "ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization." However, OP-411.2 does not describe the procedures for ensuring third-party providers employ adequate security measures to protection information in their systems.

Why This Is Important

FISMA Compliance for Contractor Systems Is Unknown

The Board cannot determine whether systems that are owned or operated by contractors or other entities are compliant with FISMA requirements, OMB policy, applicable NIST guidelines, and FedRAMP. As a result, the Board is not able to obtain assurance that security controls of such systems and services are effectively implemented.

Recommendations:

OIG recommends that the Board

7. Develop, document, and implement procedures for performing oversight of systems operated by contractors and other Federal agencies.

8. As a best practice, for federally operated systems, in addition to obtaining ATOs for those systems, also request confirmation of annual contingency plan testing and annual security control testing for those systems.

9. Develop a plan and schedule for authorizing contractor-operated systems, including cloud-based systems, in accordance with FISMA, the NIST RMF, and FedRAMP.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Board

1. Perform an annual security control assessment of the GSS. Since the Board has not identified the process for identifying which sub-set of controls should be tested each year, for FY 2015, OIG recommends the following controls should be tested at a minimum:

   - Any controls that are new or changed in NIST SP 800-53 Revision 4.
   - Any security control enhancements not tested during the 2012 security assessment.
   - Any controls impacted by changes to the GSS environment since the security assessment conducted in 2012.
   - Any controls associated with closed POA&M items.

2. Update the GSS security authorization documentation (e.g., security plan, risk assessment, security assessment report) as required.

3. Reevaluate the risk assigned to the controls impacted by the error in the 2012 GSS risk assessment and update the POA&M as needed.

4. Update the GSS system security plan to document accepted risk.

5. Develop, document, and implement POA&M management procedures.

6. Update the POA&M to include all known vulnerabilities and actual completion dates for completed POA&M items.

7. Develop, document, and implement procedures for performing oversight of systems operated by contractors and other Federal agencies.

8. As a best practice, for federally operated systems, in addition to obtaining ATOs for those systems, also request confirmation of annual contingency plan testing and annual security control testing for those systems.

9. Develop a plan and schedule for authorizing contractor-operated systems, including cloud-based systems, in accordance with FISMA, the NIST RMF, and FedRAMP.

V. BOARD COMMENTS

A discussion draft of this report was provided to the Board prior to an exit conference held on November 5, 2014. At this meeting, Board management stated their general agreement with the findings and recommendations in this report and opted not to provide formal comments for inclusion in this report.

OBJECTIVE, SCOPE, AND METHODOLOGY

Appendix

Objective

The objective was to perform an independent evaluation of the Board's implementation of FISMA for FY 2014.

Scope

The evaluation focused on reviewing the Board's implementation of FISMA for FY 2014. The evaluation included an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines, and a review of information security policies, procedures, and practices of a representative subset of the Board's information systems, including contractor systems and systems provided by other Federal agencies. As the Board has only one system, that system was selected for evaluation. There was not sufficient information about the Board's use of contractor systems and/or systems provided by other Federal agencies to select any contractor systems for evaluation in FY 2014.

The evaluation was conducted from April 2014 through September 2014. Any information received from the Board subsequent to the completion of fieldwork was incorporated when possible. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators were aware of the possibility of fraud, waste, and abuse in the program.

Methodology

Richard S. Carson & Associates, Inc., conducted an independent evaluation of the Board's implementation of FISMA for FY 2014. In addition to an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines, the evaluation included an assessment of the following topics specified in OMB's FY 2014 Inspector General FISMA Reporting Metrics:

- Continuous Monitoring Management.

- Configuration Management.
- Identity and Access Management.
- Incident Response and Reporting.
- Risk Management.
- Security Training.
- Plan of Action and Milestones.
- Remote Access Management.
- Contingency Planning.
- Contractor Systems.
- Security Capital Planning.

To conduct the independent evaluation, the team reviewed the following:

- Board policies, procedures, and guidance specific to the Board's information security program and its implementation of FISMA, and to the 11 topics specified in OMB's reporting metrics.
- Security assessment and authorization documents for the Board's GSS, including security assessment reports and vulnerability assessment reports prepared in support of system security assessment and authorization.

When reviewing security assessment reports, the team focused on security controls specific to the 11 topics specified in OMB's reporting metrics.

All analyses were performed in accordance with guidance from the following:

- NIST standards and guidelines.

- Council of the Inspectors General on Integrity & Efficiency, *Quality Standards for Inspection and Evaluation*, January 2012.

- Board ISSP policies, processes, procedures, standards, and guidelines.

- NRC OIG audit guidance.

The evaluation work was conducted by Jane M. Laroussi, CISSP, from Richard S. Carson & Associates, Inc.

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-270-2787

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report please, email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.