FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Gary Peters
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Peters:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Rand Paul
Ranking Member
Committee on Homeland Security
and Governmental Affairs
U.S. Senate
442 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Paul:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Maria Cantwell
Chair
Committee on Commerce, Science, and Transportation
U.S. Senate
420-A Hart Senate Office Building
Washington, D.C. 20510

Dear Chair Cantwell:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
U.S. Senate
512 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Cruz:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable James Comer
Chairman
Committee on Oversight and Accountability
U.S. House
2105 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Comer:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
U.S. House
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Raskin:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Mark Green
Chairman
Committee on Homeland Security
H2-117 Ford House Office Building
Washington, DC 20515

Dear Chairman Green:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
176 Ford House Office Building
Washington, DC 20515

Dear Congressman Thompson:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Frank Lucas
Chairman
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Lucas:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
2321 Rayburn House Office Building
Washington, DC 20515

Dear Representative Lofgren:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted].

Sincerely,

Ravindra Deo
Executive Director

Enclosures

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77 K Street, NE Washington, DC 20002

March 1, 2023

The Honorable Gene L. Dodaro
Comptroller General of the United States
Government Accountability Office
441 G St., NW
Washington, DC 20548

Dear Mr. Dodaro:

I am writing to provide you with the annual Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board.

I hope you find this information useful. If your staff has any questions concerning this report, please call Kim Weaver, Director of External Affairs, at 202-[redacted]

Sincerely,

Ravindra Deo

Ravindra Deo
Executive Director

Enclosures

Audit of the Effectiveness of Federal Retirement Thrift Investment Board's Information Security Program Under Federal Information Security Modernization Act of 2014

July 28, 2022

Williams, Adley & Company-DC, LLP issued this report to Federal Retirement Thrift Investment Board Internal Audit for further distribution to the Board Members of the FRTIB and the Executive Director in connection with their oversight roles of FRTIB operations. This report contains sensitive information which may be subject to the requirements of 18 United States Code 1905 or 5 U.S.C. 522a. Freedom of Information Act requests this report should be forwarded to FRTIB's Office of General Counsel, and congressional and media inquiries concerning this report should be forwarded to FRTIB's Office of External Affairs. The information in this report should not be used for other than the intended purposes without first discussing its applicability with FRTIB Internal Audit.

July 28, 2022

Barbara Holmes
Chief Audit Executive
Office of Executive Director
Federal Retirement Thrift Investment Board
77 K St NE #1000
Washington, District of Columbia 20002

Dear Ms. Holmes:

We are pleased to provide our report for the performance audit conducted to evaluate the effectiveness of the Federal Retirement Thrift Investment Board (FRTIB)'s information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year ending September 30, 2022. This report details the results of our evaluation that will be reported to the Office of Management and Budget on or before July 29, 2022, via the CyberScope reporting tool.

Based on the audit procedures performed, we conclude that FRTIB has the people, process, and technology supporting its information security program to achieve a Level 4 (Managed and Measurable) maturity rating across all five (5) FISMA functions and 19 of 20 core FISMA metric questions.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions and we believe that our audit procedures have met this requirement.

This report is issued to FRTIB Internal Audit for further distribution to the Board Members of the FRTIB and the Executive Director in connection with their oversight roles of FRTIB operations. We appreciate the opportunity to assist your agency with this audit.

FRTIB management provided us with a response to the conclusions outlined in the FY 2022 FISMA audit report which is included in Appendix D. However, we did not audit management's response and, accordingly, do not express any assurance on it.

Williams, Adley & Company-DC, LLP

Washington, District of Columbia

CONTENTS

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires agency Inspector General (IG) offices, or an independent external auditor, to conduct an annual independent audit to determine the effectiveness of the agency information security program and practices. Federal Retirement Thrift Investment Board (FRTIB or "Agency")'s Internal Audit contracted with an independent external auditor, Williams, Adley & Company-DC, LLP (Williams Adley), to conduct the Fiscal Year (FY) 2022 FISMA audit to provide a basis for the conclusions associated with the FY 2022 IG FISMA Reporting Metrics issued by the United States Department of Homeland Security (DHS).

The objective of the FY 2022 FISMA audit was to determine the effectiveness of FRTIB's information security program and practices, using laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

Starting with FY 2022, OMB introduced a new reporting cycle, shifting the reporting deadline from October to July. Furthermore, OMB introduced an updated metric methodology comprised of Core and Supplemental reporting metrics. The Core group of reporting metrics represent a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The supplemental reporting metrics will be evaluated on a two-year cycle starting in FY 2023.

Williams Adley assessed the Core FISMA reporting metrics and FRTIB's information security program and related practices across the following nine (9) FISMA domains:

- Risk Management;
- Supply Chain Risk Management;
- Configuration Management;
- Identity and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

Within each domain, Williams Adley reviewed a combination of entity-wide and system specific controls with a focus on two (2) of FRTIB's information systems: Financial and Reconciliation Services (FRS) and Converge. The in-scope systems were selected based on a risk-based approach to reflect the agency's current transition from legacy systems, such as FRS, to Converge. This allows for the potential to identify information security deficiencies that should be considered by the agency as a part of its transition. Please refer to Appendix A of this report for further information regarding the scope of the FY 2022 FISMA audit.

FY 2022 FISMA Audit Results

The FRTIB has an effective information security program.

20 Core FISMA Metrics Evaluated

3 Exceptions Identified

0 New Recommendations Issued

WILLIAMS ADLEY
Confidence Earned

Made with VISME

BACKGROUND

Federal Retirement Thrift Investment Board

The Federal Employees' Retirement System Act of 1986 (FERSA) established the Thrift Savings Plan (TSP). The TSP provides tax-deferred employee contributions and associated earnings for plan participants and began accepting contributions on April 1, 1987. The total TSP assets, as of December 31, 2021, was $811 billion for approximately 6.5 million participants.

In accordance with FERSA, FRTIB was created to administer the TSP on behalf of plan participants and beneficiaries and is an independent agency within the Executive Branch of the Federal Government.

FRTIB is governed by a Board with five members named "fiduciaries." The Executive Director (ED), who is also a fiduciary, is responsible for managing the TSP for its plan participants and beneficiaries.

Federal Information Security Modernization Act of 2014

Federal Information Security Modernization Act of 2014 (FISMA) was established to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Specifically, FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. Furthermore, FISMA "emphasizes a risk-based policy for cost-effective security," underscoring the importance of agencies to take a risk-based approach to protecting their information and information systems and addressing their unique cybersecurity challenges.

Cybersecurity Framework

In response to the growing concern related to cybersecurity, Executive Order 13636,[1] was issued which required the development of a set of industry standards and best practices to help organizations manage information security risks to combat cybersecurity challenges and resulting in the publication of the National Institute of Standards and Technology (NIST)'s "Framework for Improving Critical Infrastructure Cybersecurity [Cybersecurity Framework]."[2] The Cybersecurity Framework[3] provides guidelines for organizations to protect critical infrastructure[4] by using business drivers to direct information security activities and to consider information security risks as part of the organization's risk management processes.

To emphasize the importance of protecting critical infrastructure, Executive Order 13800[5] was issued to hold agency heads accountable for managing cybersecurity risk in their organizations. Specifically, Executive Order 13800 defines effective risk management as requiring agency heads to lead integrated teams of senior executives with expertise in information technology (IT), security, budgeting, acquisition, law, privacy, and human resources. Furthermore, Executive Order 13800 requires agency heads to use the

[1] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.
[2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014.
[3] Version 1.1 of the Cybersecurity Framework was published in April 2018 to provide refinements, clarifications, and enhancements to Version 1.0, including descriptions on how to manage supply chain cybersecurity.
[4] According to Executive Order 13636, critical infrastructure is defined as "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
[5] Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

Cybersecurity Framework to manage the agency's cybersecurity risk and hold agency heads accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

The Cybersecurity Framework provides Federal agencies with a common structure for identifying and managing information security risks across the enterprise and provides guidance for assessing the maturity of controls to address those risks. The Cybersecurity Framework is comprised of five (5) information security functions that give Federal agencies the ability to select and prioritize improvements in information security risk management. The five (5) information security functions are as follows:

- **Identify** – The "identify" function requires the development of organizational understanding to manage information security risk to systems, assets, data, and capabilities.
- **Protect** – The "protect" function requires the development and implementation of appropriate safeguards to ensure delivery of services.
- **Detect** – The "detect" function requires the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – The "respond" function requires the development and implementation of appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – The "recover" function requires the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity event.

The five (5) functions (identify, protect, detect, respond, and recover) of the Cybersecurity Framework provide agencies with the structure and guidance to improve their information security program by using an effective risk management strategy to govern and protect their environment. Furthermore, the five (5) functions support recurring risk assessments and validation of business drivers to help agencies implement the necessary information security activities that reflect desired outcomes. Each function places reliance on the development of those preceding it. For example, an organization cannot *protect* its IT environment correctly without first *identifying* its key information systems and the risks faced by each. Moreover, an organization cannot *respond* to cybersecurity events if it has not first implemented proper measures to *detect* them.

M-22-05 - Memorandum for the Heads of Executive Departments and Agencies

On December 6, 2021, the Office of Management and Budget (OMB) issued M-22-05, Memorandum for the Heads of Executive Departments and Agencies which introduced changes to the IG metrics and reporting to OMB and Department of Homeland Security (DHS).

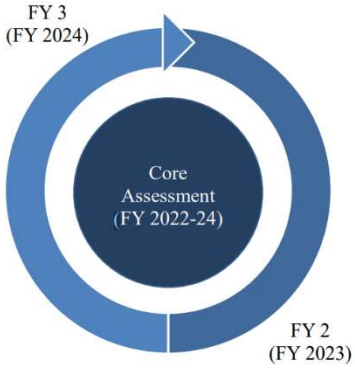

Figure 1. Multi-Year Cycle

Section III: Requirements for FISMA Reporting to OMB and DHS

Section III of M-22-05 establishes a new annual FISMA reporting deadline for FY 2022; moving the due date from the end of October to end of July. The OMB shifted the due date of the IG metrics from October to July to better align the release of IG assessments with the development of the President's Budget.

Section V: IG Reporting

Section V of M-22-05 outlines the transition to a multi-year evaluation cycle. Starting with FY 2022, OMB will select a core group of metrics,

representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle based on a calendar agreed to by Council of the Inspectors General on Integrity and Efficiency (CIGIE), the Chief Information Security Officer (CISO) Council, OMB, and Cybersecurity and Infrastructure Security Agency (CISA).

FY 2022 Inspector General (IG) FISMA Reporting Metrics

Overview

FISMA requires the OMB to ensure that guidance is developed for the independent audit of agency information security programs. On April 14, 2022, the OMB, United States DHS, and CIGIE released the "FY22 Core IG Metrics Implementation Analysis and Guidelines."

This guidance provides metrics to be used to gauge the maturity of agency practices in connection with the nine (9) IG FISMA metric domains that are organized around the five (5) information security functions outlined in the Cybersecurity Framework:

- Identify
    - Risk Management – The purpose of the risk management IG FISMA metric domain is to evaluate the maturity of an agency's risk management program.
        - An agency with an effective risk management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.

    - Supply Chain Risk Management (SCRM) – The purpose of the SCRM IG FISMA metric domain is to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements.
        - An agency with an effective SCRM program manages supply chain risks and ensures that third parties adhere to organizational cybersecurity and supply chain requirements; ensures that counterfeit components are detected and prevented from entering organization's systems; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.
- Protect
    - Configuration Management – The purpose of the configuration management IG FISMA metric domain is to evaluate the maturity of an agency's configuration management program.
        - An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.

- Identity and Access Management – The purpose of the identity and access management IG FISMA metric domain is to evaluate the maturity of an agency's identity and access management program.
    - An agency with an effective identity and access management program ensures that all privileged and non-privileged users utilize strong authentication to organizational systems; employs automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its program.

- Security Training – The purpose of the security training IG FISMA metric domain is to evaluate the maturity of an agency's security training program.
    - An agency with an effective security training program addresses all of its identified knowledge, skills, and abilities gaps; measures the effectiveness of its security awareness and training program; and ensures that staff are consistently collecting, monitoring, and analyzing qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

- Data Protection and Privacy – The purpose of the Data Protection and Privacy IG FISMA metric domain is to evaluate the maturity of an agency's data protection and privacy program.
    - An agency with an effective data protection and privacy maintains confidentiality, integrity, and availability of its data and is able to assess its security and privacy controls as well as its breach response capacities; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its privacy activities.

- Detect
    - Information Security Continuous Monitoring (ISCM) – The purpose of the information security continuous monitoring IG FISMA metric domain is to evaluate the maturity of an agency's ISCM program.
        - An agency with an effective ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its information security continuous monitoring policies, procedures, plans, and strategies.
- Respond
    - Incident Response – The purpose of the incident response IG FISMA metric domain is to evaluate the maturity of an agency's incident response program.
        - An agency with an effective incident response program utilizes profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents; manages and measures the impact of successful incidents; uses incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.
- Recover
    - Contingency Planning – The purpose of the contingency planning IG FISMA metric domain is to evaluate the maturity of an agency's contingency planning program.

- An agency with an effective contingency planning program employs automated mechanisms to more thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities.

Maturity Models

The effectiveness of an information security program is determined based on the ratings earned on a maturity model spectrum, which identifies whether an agency has developed policies and procedures, implemented documented processes, and established methods to improve over time. The maturity model spectrum is divided into five (5) levels outlined below:

- **Level 1: Ad-Hoc** – Policies, procedures, and strategy are not formalized; activities are performed in an Ad-Hoc, reactive manner.
- **Level 2: Defined** – Policies, procedures, and strategy are formalized and documented but not consistently implemented.
- **Level 3: Consistently Implemented** – Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
- **Level 4: Managed and Measurable** – Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
- **Level 5: Optimized** – Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Level 4, Managed and Measurable, is considered to be an effective level of security at the domain, function, and overall program level. Furthermore, maturity ratings at the domain, function, and overall program level are determined by a simple majority, where the most frequent level (i.e., the mode) across the questions will determine as the proper rating.

AUDIT RESULTS

Overview

Federal Retirement Thrift Investment Board (FRTIB) has implemented an effective information security program through the implementation of 19 out of 20 Core Federal Information Security Modernization Act of 2014 (FISMA) metrics[6] and achieving a maturity rating of Managed and Measurable (Level 4) across all five (5) information security functions, as outlined in **Table 1** below.

Security Function	Maturity Rating
Identify	Level 4 - Managed and Measurable
Protect	Level 4 - Managed and Measurable
Detect	Level 4 - Managed and Measurable
Respond	Level 4 - Managed and Measurable
Recover	Level 4 - Managed and Measurable

Table 1. FY 2022 Security Function Maturity Ratings

Furthermore, Williams Adley identified three (3) conditions for the FY 2022 reporting period related to the Risk Management, Configuration Management, and Information Security Continuous Monitoring (ISCM) security domains. Due to the nature of the conditions and pre-existing recommendations, Williams Adley will not issue any new recommendations for the FY 2022 reporting period. Lastly, Williams Adley determined that three (3) outstanding recommendations from prior reporting periods were addressed by FRTIB management through improvements made to the implementation of its defined control activities.

The following pages summarize the basis for each Function and corresponding Domain's maturity rating.

Identify

The Identify function, supported by the Risk Management and Supply Chain Risk Management domains, is rated at a Level 4 maturity (Managed and Measured). **Table 2** below summarizes the ratings of each domain within the Identify Function.

FISMA Domain	Rating in FY 2022
Risk Management	Level 4 - Managed and Measurable
Supply Chain Risk Management	Level 4 - Managed and Measurable

Table 2. Ratings for the Domains within the Identify Function

Risk Management

OMB identified the following FISMA reporting metric questions as core for the development of a Risk Management program:

- CyberScope Metric Question 1: Maintain a comprehensive and accurate inventory of Agency information systems;
- CyberScope Metric Question 2: Maintain an up-to-date inventory of hardware assets;
- CyberScope Metric Question 3: Maintain an up-to-date inventory of the software and associated licenses;

[6] Of the 20 Core metrics, FISMA metric 10 did not reach a Level 4 maturity.

- CyberScope Metric Question 5: Organization ensure that information system security risks are managed at the organizational, mission/business process, and information system levels; and
- CyberScope Metric Question 10: Use of technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization.

Williams Adley determined that the FRTIB has developed and maintained a comprehensive and accurate inventory of information systems and supporting hardware and software component inventories.

Furthermore, the FRTIB has consistently implemented its policies and procedures to manage cybersecurity risk management activities at all three (3) organizational tiers, including periodic risk assessments and maintaining its cybersecurity risk register. In addition, risks identified within the cybersecurity risk register are communicated to executive management on a periodic basis for review and inclusion within the organization's enterprise risk register.

Lastly, Williams Adley identified one condition related to missing technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities[7][8]. Per discussion with FRTIB management, the Agency is in process of implementing ServiceNow's Enterprise Risk Management, Cyber Security Risk Management and Supply Chain Risk Management modules to support its risk management activities.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 2** below, Williams Adley concluded that the maturity rating of FRTIB's risk management program is Managed and Measurable (Level 4).

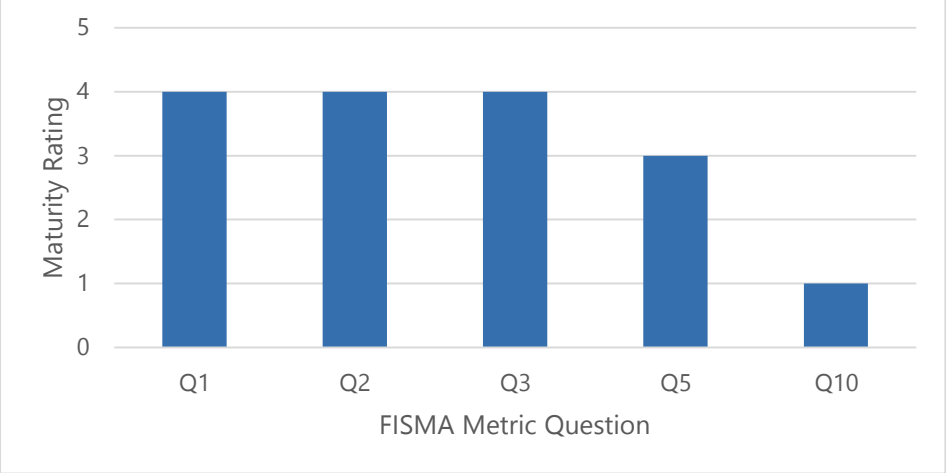

Figure 2. Risk Management Maturity by Question

Supply Chain Risk Management

OMB identified the following FISMA reporting metric question as core for the development of a Supply Chain Risk Management (SCRM) program:

[7] Historically, the FRTIB has used non-automated methods to manage its enterprise-wide view of cybersecurity risk management activities as the Agency determined it to be sufficient. This condition was added to the FY 2022 FISMA report as OMB has identified the use of technology and automation to support an agency's risk management activities as highly valuable.

[8] This condition will not result in a new recommendation as the existing open recommendation from the FY 2017 reporting period outlines the integration of people, process, and technology solutions to support an effective information security program.

- CyberScope Metric Question 14: The agency ensures that products, system components, systems, and services of external providers are consistent with the agency's cybersecurity and supply chain requirements

Williams Adley determined that FRTIB has implemented multiple process to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements:

- Monthly BitSight performance report to review key performance indicators for FRTIB's portfolio of third parties and the latest capabilities available through the BitSight Security Ratings Platform;
- Quarterly vendor risk assessment to identify any key vendor risks, including, but not limited to, financial health, operational, reputational, credit, cyber, and external risks that may affect the services these vendors provide to FRTIB and therefore their capability to fulfill contractual obligations; and
- Quarterly board presentations to provide analysis of each key vendor to the Board members.

Furthermore, the Agency utilizes qualitative and quantitative performance metrics through its Process Health Management (PHM) process to measure, report on, and monitor information security and supply chain risk management performance.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 3** below, Williams Adley concluded that the maturity rating of FRTIB's supply chain risk management program is Managed and Measurable (Level 4).

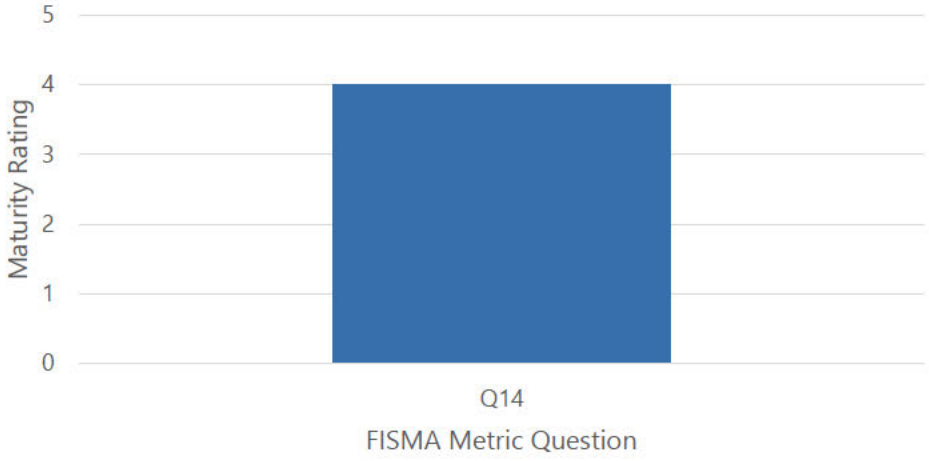

Figure 3. Supply Chain Risk Management Maturity by Question

Protect

The Protect function, supported by the Configuration Management, Identity and Access Management, Security Training, and Data Protection and Privacy domains, is rated at a Level 4 maturity (Managed and Measurable). **Table 3** below summarizes the ratings of each domain.

FISMA Domain	Rating in FY 2022
Configuration Management	Level 4 - Managed and Measurable
Identity and Access Management	Level 4 - Managed and Measurable

Data Protection and Privacy	Level 4 - Managed and Measurable
Security Training	Level 4 - Managed and Measurable

Table 3. Ratings for the Domains within the Protect Function

Configuration Management

OMB identified the following FISMA reporting metric questions as core for the development of a Configuration Management program:

- CyberScope Metric Question 20: Use of settings/common secure configurations; and
- CyberScope Metric Question 21: Use of flaw remediation processes, including patch management, to manage software vulnerabilities.

FRTIB has designed and implemented its configuration management activities to maintain its common secure configurations across its information systems and manage vulnerabilities. However, Williams Adley identified the following low risk configuration failures associated with one host IP Address within FRS (10.20.7.117 [PRD-CAMI-AP3]) that do not have a documented deviation approval[9]:

- 1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'
- 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)'
- 2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on'

Furthermore, through its PHM process, the Agency evaluates the effectiveness of its configuration management activities using qualitative and quantitative performance measures to govern and make changes, as necessary.

Based on the results of the audit procedures performed and the distribution of scores in **Figure 4** below, Williams Adley concluded that the maturity rating of FRTIB's supply chain risk management program is Managed and Measurable (Level 4).

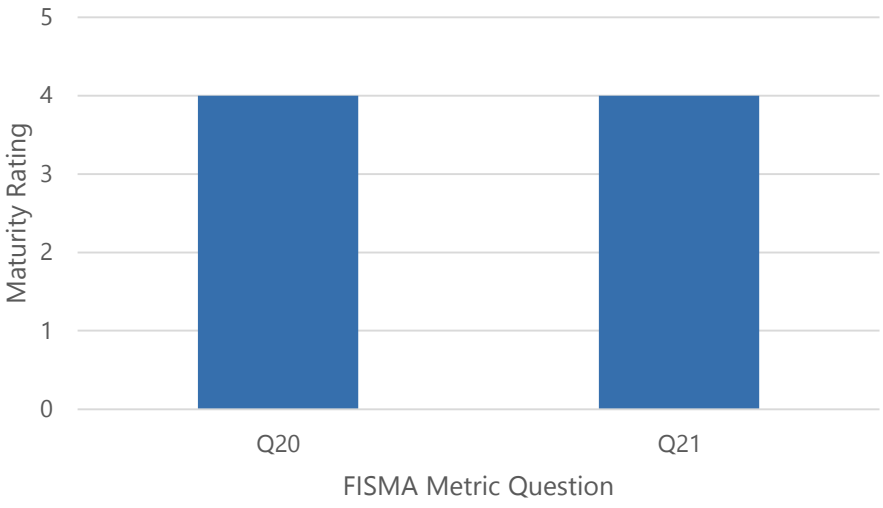

Figure 4. Configuration Management Maturity by Question

[9] This issue was deemed to be low risk as the CAMI application within FRS has a compensating control in place to reduce the risks associated with authenticating to the application. Williams Adley will not issue a recommendation associated within this condition but is included in the FY 2022 FISMA report for Management's awareness.

Identity and Access Management

OMB identified the following FISMA reporting metric questions as core for the development of an Identity and Access Management program:

- CyberScope Metric Question 30: Use of strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users;
- CyberScope Metric Question 31: Use of strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users; and
- CyberScope Metric Question 32: Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.

FRTIB has designed its method of authentication to require the use of PIV credentials for its non-privileged and privileged users. Furthermore, the Agency has consistently implemented its processes for provisioning, managing, and reviewing privileged accounts, as well as utilizes automated scripts to revoke /disable inactive accounts from its network[10].

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 5** below, Williams Adley concluded that the maturity rating of FRTIB's Identity and Access Management program is Managed and Measurable (Level 4).

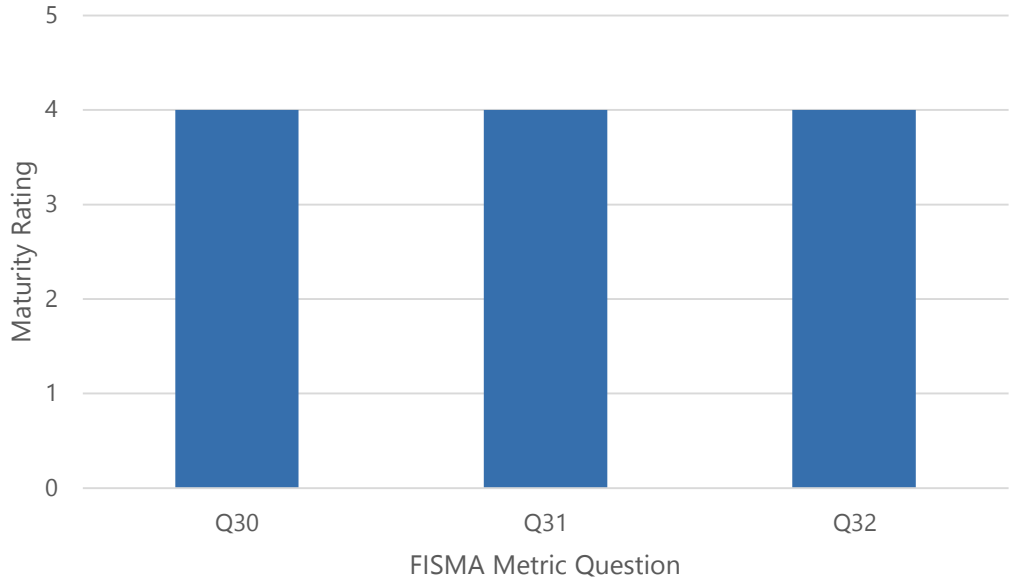

Figure 5. Identity and Access Management Maturity by Question

Data Protection and Privacy

OMB identified the following FISMA reporting metric questions as core for the development of a Data Protection program:

[10] Network access is required to access FRTIB information systems including FRS and Converge.

- CyberScope Metric Question 36: Use of encryption of data rest, in transit, limitation of transference of data by removable media, and sanitization of digital media prior to disposal or reuse to protect its PII and other agency sensitive data; and
- CyberScope Metric Question 37: Use of security controls to prevent data exfiltration and enhance network defenses.

FRTIB protects personally identifiable information (PII) collected, used, maintained, shared, and disposed by its information systems through the implementation of security controls designed to encrypt sensitive data and prevent data exfiltration. Furthermore, through the PHM process, the Agency evaluates the effectiveness of its privacy program activities using qualitative and quantitative performance measures to govern and make changes, as necessary.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 6** below, Williams Adley concluded that the maturity rating of FRTIB's Data Protection and Privacy program is Managed and Measurable (Level 4).

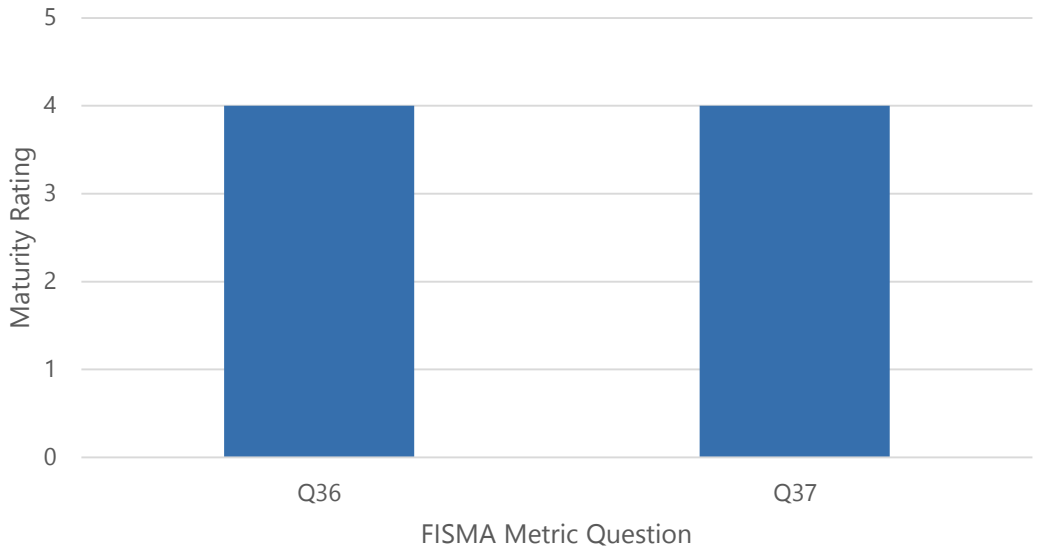

Figure 6. Data Protection and Privacy Maturity by Question

Security Training

OMB identified the following FISMA reporting metric question as core for the development of a Security Training program:

- CyberScope Metric Question 42: Perform assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training

FRTIB performs assessments of the skills, knowledge, and abilities of its workforce every two years to identify gaps and potential areas for improvement. During FY 2022, the Agency provided its workforce with multiple general, and role specific trainings tailored to address the gaps identified as a part of its FY 2020 assessment. Furthermore, the Agency utilizes its individual development plan (IDP) to address skill gaps identified by employee supervisors.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 7** below, Williams Adley concluded that the maturity rating of FRTIB's Security Training program is Managed and Measurable (Level 4).

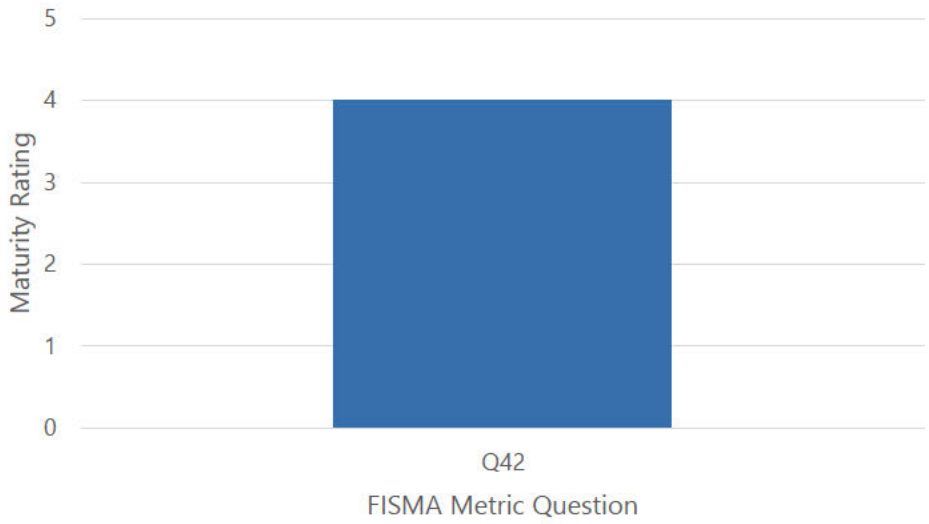

Figure 7. Security Training Maturity by Question

Detect

The Detect function, supported by the ISCM domain, is rated at a Level 4 maturity (Managed and Measured).

FISMA Domain	Rating in FY 2022
ISCM	Level 4 - Managed and Measurable

Table 4. Rating for the Domain within the Protect Function

Information Security Continuous Monitoring

OMB identified the following FISMA reporting metric questions as core for the development of an ISCM program:

- CyberScope Metric Question 47: Use of information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier; and
- CyberScope Metric Question 49: Performance of ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls.

FRTIB has established and implemented its information security continuous monitoring (ISCM) program to support continuous monitoring (ConMon) activities, as described within its ISCM strategy, across all three (3) organizational tiers.

In addition, FRTIB has continued their ongoing practice of collecting, evaluating, and analyzing data to maintain awareness of its information systems and make changes to its overall information security

program, as required. However, certain metrics within the PHM process rely on manual methods of data gathering and entry; hence leaving room for human errors. As a part of the FY 2022 FISMA audit, Williams Adley identified the values for PHM Metrics ISCM-10 and ISCM-18 were incorrectly input into the November 2021 dashboard. These issues were determined to be low risk as the difference between the true value and documented values were negligible and did not exceed any performance thresholds[11].

Based on the results of the audit procedures performed and the distribution of scores in **Figure 8** below, Williams Adley concluded that the maturity rating of FRTIB's ISCM program is Managed and Measurable (Level 4).

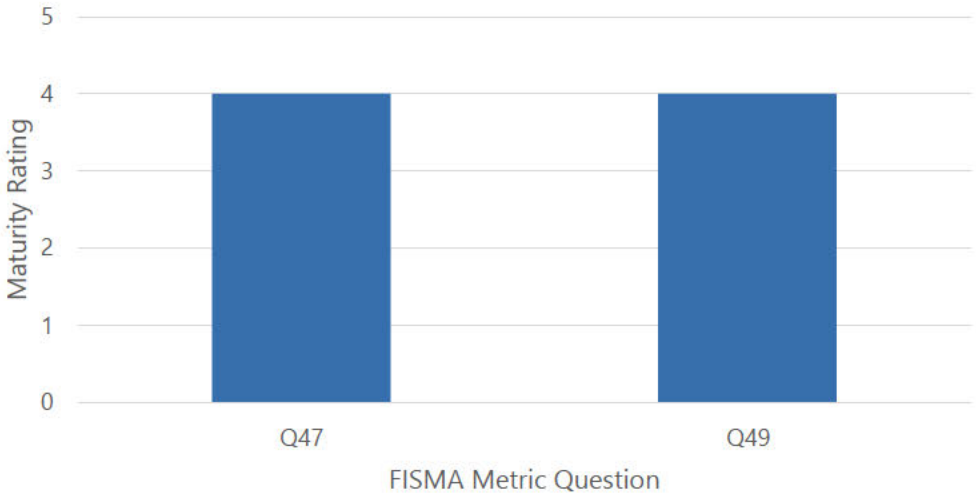

Figure 8. ISCM Maturity by Question

Respond

The Respond function, supported by the Incident Response domain, is rated at a Level 4 maturity (Managed and Measurable).

FISMA Domain	Rating in FY 2022
Incident Response	Level 4 - Managed and Measurable

Table 5. Rating for the Domain within the Respond Function

Incident Response

OMB identified the following FISMA reporting metric questions as core for the development of an Incident Response program:

- CyberScope Metric Question 54: Processes for incident detection and analysis; and
- CyberScope Metric Question 55: Processes for incident handling.

FRTIB has consistently implemented its incident response activities to ensure incidents are managed from initial detection through resolution in accordance with established policies and procedures and communicated to external stakeholders in a timely manner.

[11] Due to the negligible impact, Williams Adley will not issue a recommendation to support this condition but will include it in this report for Management's awareness.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 9** below, Williams Adley concluded that the maturity rating of FRTIB's Incident Response program is Managed and Measurable (Level 4).

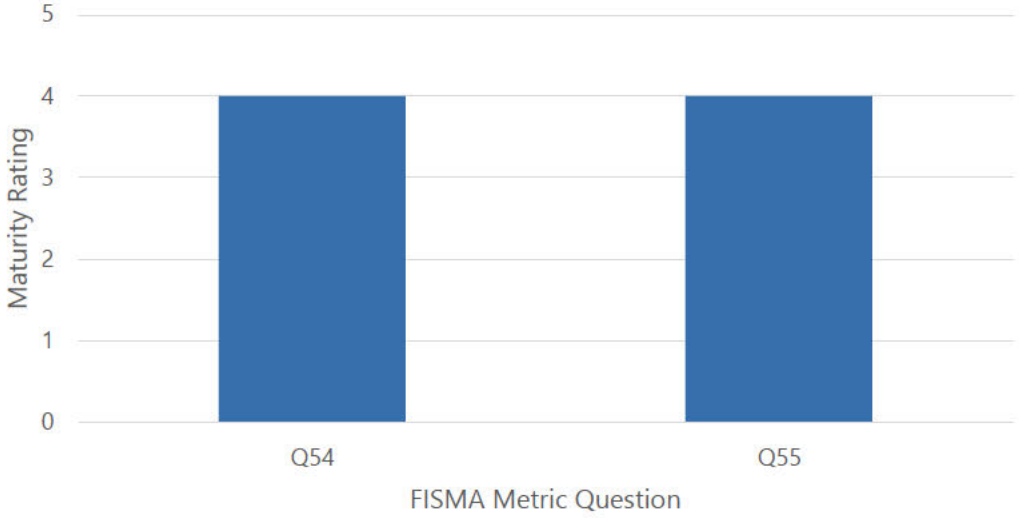

Figure 9. Incident Response Maturity by Question

Recover

The Recover function, supported by the Contingency Planning domain, is rated at a Level 4 maturity (Managed and Measurable).

FISMA Domain	Rating in FY 2022
Contingency Planning	Level 4 - Managed and Measurable

Table 6. Rating for Domains within the Recover Function

Contingency Planning

OMB identified the following FISMA reporting metric questions as core for the development of a Contingency Planning program:

- CyberScope Metric Question 61: Business impact analyses (BIA) are used to guide contingency planning efforts; and
- CyberScope Metric Question 63: Performance of tests/exercises of its information system contingency planning processes.

FRTIB made significant improvements to its Contingency Planning program by ensuring that BIAs are performed and used to guide contingency planning efforts, and tabletop exercises were performed to ensure supporting personnel understand their roles and responsibilities and identify potential areas of improvement. Furthermore, Williams Adley confirmed that BIAs were integrated with enterprise risk management processes to appropriately evaluate, record, and monitor enterprise assets.

No new conditions were identified related to this domain for the FY 2022 FISMA audit. Based on the results of the audit procedures performed and the distribution of scores in **Figure 10** below, Williams Adley

concluded that the maturity rating of FRTIB's Contingency Planning program is Managed and Measurable (Level 4).

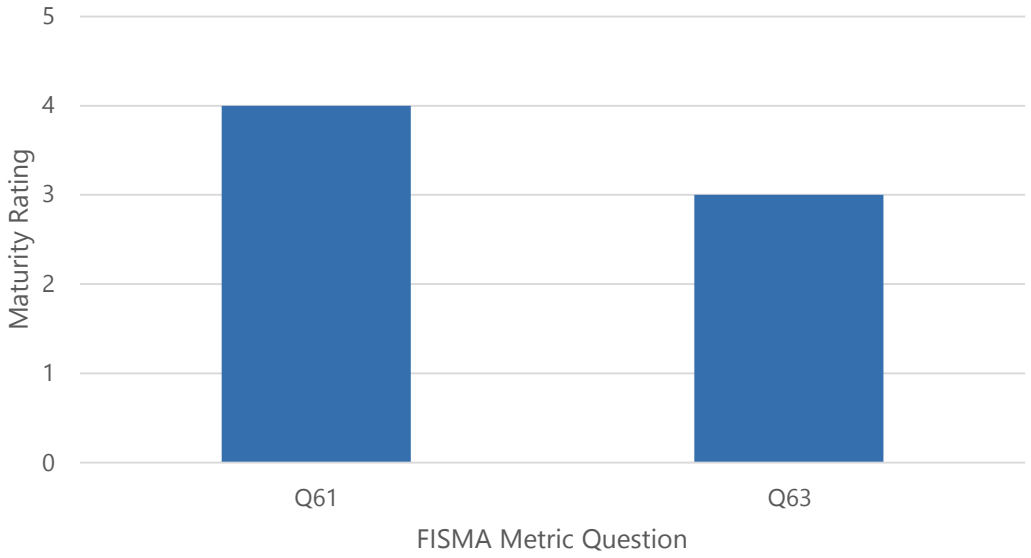

Figure 10. Contingency Planning Maturity by Question

Conclusion

Based on the results of the audit procedures performed for the FY 2022 FISMA audit, Williams Adley concludes that the FRTIB has effectively implemented 19 out of 20 Core FISMA metrics resulting in all five (5) FISMA security functions and all nine (9) associated domains rated at a Level 4 maturity (Managed and Measurable).

Furthermore, Williams Adley does not believe that there are any legacy issues that could be inherited by the new Converge system and/or other future systems. However, as the Agency continues its transition to managed services and legacy systems begin the decommissioning process, the FRTIB should continue to use a risk-based approach to manage cybersecurity risks in a cost-effective way based on business and organizational needs.

APPENDIX A: PURPOSE, SCOPE, CRITERIA AND METHODOLOGY

Purpose

To fulfill its responsibilities related to Federal Information Security Modernization Act of 2014 (FISMA)[12], Federal Retirement Thrift Investment Board (FRTIB) Internal Audit, contracted with Williams, Adley & Company-DC, LLP (Williams Adley), an independent public accounting firm, to determine the effectiveness of the FRTIB information security program and practices, as it relates to the Core FISMA metrics, in Fiscal Year (FY) 2022.

FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. To ensure the adequacy and effectiveness of these controls, FISMA requires an independent external auditor to perform annual reviews of the information security program and that the head of the agency report those results to Office of Management and Budget (OMB). The FY 2022 Inspector General (IG) FISMA Reporting Metrics[13] developed by the OMB, the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) is intended to provide guidance on the Office of Inspector General (OIG)'s annual audits, as required by the FISMA, 44 U.S. Code (USC) 3555(j).

Scope

Williams Adley conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) which requires that sufficient, appropriate evidence is obtained to provide a reasonable basis for the findings and conclusions outlined within this report.

To determine the effectiveness of FRTIB's information security program and practices in FY 2022, Williams Adley selected a representative subset of FRTIB's information systems to assess. The following two (2) systems were selected for the FY 2022 FISMA audit:

System Name	System Description[14]	High Value System (Yes/No)
Financial and Reconciliation Services (FRS)	FRS is one of FRTIB's major application boundaries and contains nine (9) subsystems and twelve (12) applications. Applications in the FRS boundary complete a wide variety of tasks for the FRTIB, such as: • General Ledgers or support General Ledger processes. • Create and print 1099R tax forms that are mailed to Thrift Savings Plan participants and payees. • Support the management of the Government Securities Investment Fund.	Yes

[12] Public Law. No. 113-283, FISMA, December 18, 2014.

[13] The OMB, the DHS, and the Council of Inspectors General on Integrity and Efficiency, "FY22 Core IG Metrics Implementation Analysis and Guidelines," April 14, 2022.

[14] System descriptions were sourced from each system's respective system security plan (SSP).

	• Support FRTIB budgeting and expenditure tracking processes, as well as the procurement of supplies and services for the FRTIB.	
Converge	The Converge program, a managed service provider, delivers a new system aligned with modern technical, operational, and functional capabilities to modernize participant and administrative services. These services seek to provide enhanced participant and beneficiary experience through the delivery of new services to increase plan participation, augment existing capabilities offered within the current plan, and deliver a secure platform.	Yes

Table 2. FY 2022 In-Scope Systems

Williams Adley acknowledges that 1) it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist at all in other information systems that were not tested and 2) it is possible that other deficiencies may exist that are unique to the information systems not included within this audit. However, a prudent person without any basis in fact would not automatically assume that these deficiencies are non-existent or existent with other systems. Such a supposition would be especially ill-advised for an issue as important as information security. Williams Adley will evaluate other information systems in subsequent years using rotational multi-year strategy.

Williams Adley's fieldwork was conducted offsite via secure Virtual Private Network (VPN) telework due to the Coronavirus Disease 2019 (COVID-19) pandemic and inaccessibility of FRTIB location at 77K St., NE in Washington, D.C.

Criteria

The FY 2022 FISMA audit was conducted using applicable laws, regulations, standards, and internal FRTIB policies and procedures as criteria, including, but not limited to the following:

- DHS Binding Operative and Emergency Directives;
- Federal Acquisition Supply Chain Security Act of 2018;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Enterprise Architecture Framework (Version 2);
- Federal Information Processing Standards (FIPS) 199 and 201-2;
- FISMA Inspector General and Chief Information Officer Metrics (FY 2022);
- FRTIB's policies and procedures relating to the nine FISMA domains;
- Homeland Security Presidential Directive 12 (HSPD-12);
- National Institute of Standards and Technology (NIST) Cybersecurity Framework;
- NIST Interagency/Internal Report (NIST IR) 8011;
- NIST IR 8276;
- NIST IR 8286;
- NIST SP 800-34, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (Revision 2 [rev.2]);
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View;
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program;

- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (rev. 5);
- NIST SP 800-61, Computer Security Incident Handling Guide (rev. 2);
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems;
- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations;
- NIST SP 800-152, A Profile for U.S. Federal Cryptographic Key Management Systems;
- OMB Circular A-123, Management's Responsibility for Internal Control;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Circular M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure;
- OMB Circular M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program;
- OMB Circular M-19-17, Enabling Mission Delivery through Improved Identity Credential, and Access Management;
- OMB M-22-05 - Memorandum for the Heads of Executive Departments and Agencies; and
- Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act.

Methodology

To perform this audit, Williams Adley interviewed FRTIB senior management, employees, and contractors to evaluate managerial effectiveness and operational controls in accordance with NIST and OMB guidance. Williams Adley observed FRTIB's operations, obtained evidence to support Williams Adley's conclusions and recommendations, tested effectiveness of established controls, conducted sampling where applicable, and collected written documents to supplement observations and interviews.

Use of Computer Processed Data

During the audit, Williams Adley used computer-processed data to obtain samples and information regarding the existence of information security controls. Williams Adley assessed the reliability of the computer-generated data primarily by comparing selected data with source documentation, data from prior years, inquiring with FRTIB personnel, and observing the selected data being generated. Williams Adley determined that the information was sufficiently reliable for assessing the adequacy of related information security controls.

Sampling Methodology

For all samples selected during the audit, Williams Adley used non-statistical audit sampling techniques where applicable and appropriate. As guidance, Williams Adley used the *American Institute of Certified Public Accountants (AICPA) Audit Guide: Audit Sampling*.[15] This guidance assists in applying audit sampling in accordance with auditing standards.

American Institute of Certified Public Accountants (AICPA) Audit Guide: Audit Sampling allows auditors to use non-statistical sampling for tests of controls. In addition, for a non-statistical sampling approach, audit guidance allows auditors to use professional judgment to relate the same factors used in statistical sampling in determining the appropriate sample sizes. For non-statistical sampling, Williams Adley used

[15] AICPA Audit Guide, Audit Sampling, March 1, 2014.

one (1) of the following two (2) sample selection approaches that approximates a random sampling approach:

- **Simple Random Sampling**. Every combination of sampling units has the same probability of being selected as every other combination of the same number of sampling units. The auditor may select a random sample by matching random numbers generated by a computer.
- **Haphazard Sampling**. A haphazard sample is a non-statistical sample selection method that attempts to approximate a random selection by selecting sampling units without a conscious bias, that is, without any special reason for including or omitting items from the sample. (It does not imply the sampling units are selected in a careless manner.)

For small populations (less than 2,000 items) and/or infrequently operating controls, Williams Adley used guidance from the AICPA, as shown in **Table 3**.

Control Frequency (Population Size)	Items to Test
Quarterly (4)	2
Monthly (12)	2
Semimonthly (24)	3
Weekly (52)	5

Table 3. Small Population Sample Sizes

For sample populations under 2,000, but greater than the small populations show in **Table 3**, Williams Adley selected a judgmental sample based on auditor judgment of risk to determine the appropriate sample size.

APPENDIX B: DETAILED AUDIT CONDITIONS AND CRITERIA

Function: Identify
Domain: Risk Management

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
RM-1	10	FRTIB does not currently utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.	**FISMA Reporting Metric 10, Maturity Level 4:** The organization uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data. In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools, such as a governance, risk management, and compliance tool), as appropriate.

Function: Identify
Domain: Supply Chain Risk Management

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

Function: Protect
Domain: Configuration Management

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
CM-1	20	The following configuration failures associated with IP Address 10.20.7.117 (PRD-CAMI-AP3) do not have documented deviation approval: • 1.1.3 Ensure 'Minimum password age' is set to '1 or more day(s)'	**FRTIB Configuration Management FISMA Baseline Policy Document:** • CM-6 (Configuration Settings) o Identify, document, and approve any deviations from established configuration

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
		• 1.1.1 Ensure 'Enforce password history' is set to '24 or more password(s)' • 2.3.7.4 Configure 'Interactive logon: Message text for users attempting to log on'	settings for [defined components such as, but not limited to mobile devices, desktops, servers, laptops, network devices, printers, copiers, etc.] based on [documented risk acceptance criteria]. **Security Configuration Settings Management, Development and Deployment Standard Operating Procedures:** • Section 2.9: Document Deviations and Exceptions o Deviations. These are variances from the default benchmark that apply enterprise wide. ▪ To document these: • The SCM team highlights Deviations in the Security Baseline document, preceded with the text "Deviation." • The SCM team includes justification for Deviations in the Security Baseline document. • The ISSM must approve any deviations before they are incorporated into the final baseline document associated with the MFR.

Function: Protect
Domain: Identity and Access Management

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

Function: Protect
Domain: Data Protection and Privacy

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

Function: Protect
Domain: Security Training

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

Function: Detect
Domain: Information Security Continuous Monitoring

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
ISCM-1	N/A	For two (2) of 10 metrics sampled, the data captured within PHM Dashboard does not match with source data: • ISCM-10: November 2021 • ISCM-18: November 2021	N/A – This condition was included in our report for management awareness and potential process improvement.

Function: Respond
Domain: Incident Response

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

Function: Recover
Domain: Contingency Planning

Item No.	Associated FISMA Metric Question	Condition Description	Criteria Reference
N/A	N/A	N/A – No Condition Identified	N/A

APPENDIX C: FOLLOW UP ON PRIOR FISMA AUDIT RESULTS

As a part of the audit procedures for FY 2022, Williams, Adley & Company-DC, LLP (Williams Adley) assessed the status of Federal Retirement Thrift Investment Board (FRTIB)'s remediation efforts to address the outstanding recommendations from prior Federal Information Security Modernization Act of 2014 (FISMA) audits and documented their status in the table below.

Fiscal Year	Recommendation Description	Status
2021	Develop a standard data elements/taxonomy to maintain a complete and accurate population of data breaches.	Open[1]
2021	Implement a penalty table to ensure users complete required training in a timely manner.	Closed
2021	Develop additional data validation processes to ensure manually tracked metrics are captured and recorded accurately within the Process Health Management (PHM) process.	Open[2]
2021	Update existing contingency planning policies, procedures, and processes to account for third party managed systems.	Closed
2020	Update and reconcile legacy plans of actions and milestones (POA&Ms) prior to their migration into Telos Xacta to ensure that all required fields are complete and duplicate POA&Ms are eliminated.	Open[3]
2017	Williams Adley recommends that FRTIB clearly define an organization-wide risk-based information security program that is tailored to FRTIB's IT environment and information security risks. At a minimum, the program should: • Integrate people, process, and technology solutions; • Adhere to NIST frameworks, including the Risk Management Framework and Cybersecurity Framework; and • Ensure that activities and processes are appropriately designed and effective across all eight (8) FISMA domains.	Open[4]
2016	Conduct testing for the FY 2016 in-scope systems and all other FRTIB systems.	Closed

[1] This recommendation was issued to FRTIB in FY 2021 to support FISMA reporting metric 38. However, FISMA reporting metric 38 was not selected as a Core FISMA metric and is out of scope for the FY 2022 FISMA evaluation.

[2] This recommendation remains open due to the condition identified in the Risk Management domain. Refer to Condition ISCM-1 within Appendix B for additional details.

[3] This recommendation was issued to FRTIB in FY 2020 to support FISMA reporting metric 8. However, FISMA reporting metric 8 was not selected as a Core FISMA metric and is out of scope for the FY 2022 FISMA evaluation.

[4] This recommendation remains open due to the condition identified in the Risk Management domain. Refer to Condition RM-1 within Appendix B for additional details.

APPENDIX D: MANAGEMENT RESPONSE

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
77K Street, NE Washington, DC 20002

July 27, 2022

Mr. Tony Wang, Principal
IT Risk Management
Williams Adley
Suite 350 West
1030 15th St, NW
Washington, D.C. 20005

Dear Mr. Wang:

Thank you for the opportunity to review the draft FY 2022 FISMA audit report. On behalf of the Agency, I am in agreement with the report.

There were no recommendations in this year's report, therefore the Agency will continue to focus on closing prior year findings, process improvement, and overall maturity of our cybersecurity program.

Regards,

[redacted]

cc: Ravindra Deo, Executive Director
Suzanne Tosini, Chief Operating Officer
Thomas Brandt, Director, Office of Planning and Risk
Gisile Goethe, Director, Office of Resource Management
Dharmesh Vashee, General Counsel
Patrick Bevill, Chief Information Security Officer
Barbara Holmes, Chief Audit Executive