



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

February 19, 2025

The Honorable Brian Babin
Chairman
Committee on Science, Space and Technology
U.S. House
2321 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Babin:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED].

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

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

Dear Ranking Member Lofgren:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED].

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

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

Dear Chairman Comer:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED].

Sincerely,

A black rectangular redaction box covering the signature of Ravindra Deo.

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

The Honorable Gerry Connolly
Ranking Member
Committee on Oversight and Accountability
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Ranking Member Connolly:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED]

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

The Honorable Mark Green
Chairman
Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Green:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED].

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

The Honorable Bennie Thompson
Ranking Member
Committee on Homeland Security
H2-117 Ford House Office Building
Washington, DC 20515

Dear Ranking Member Thompson:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED]

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

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

Dear Senator Cruz:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED]

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
U.S. Senate
254 Russell Senate Office Building
Washington, D.C. 20510

Dear Senator Cantwell:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED].

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

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

Dear Chairman Paul:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED]

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

February 19, 2025

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

Dear Senator Peters:

I am writing to provide you with the FY24 Federal Information Security Modernization Act report of the Federal Retirement Thrift Investment Board and a copy of our required notice to the Director of the Office Management and Budget and the Secretary of Homeland Security.

I hope you find this information useful. If your staff has any questions concerning this report, please call Jim Kaplan, Director of External Affairs, at [REDACTED]

Sincerely,

[REDACTED]

Ravindra Deo
Executive Director

Enclosure



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

July 29, 2024

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 the 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 the FRTIB's Office of General Counsel, and congressional and media inquiries concerning this report should be forwarded to the 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 the FRTIB Internal Audit.



July 29, 2024

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

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 (FY) ending September 30, 2024. This report details the results of our evaluation that will be reported to the Office of Management and Budget on or before July 31, 2024, via the CyberScope reporting tool.

Based on the audit procedures performed, we conclude that the FRTIB has the people, process, and technology supporting its information security program to achieve a Level 5 (Optimized) maturity rating across all nine FISMA domain areas.

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

The FRTIB management provided us with a response to the conclusions outlined in this report and their response is included in Appendix C. 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

Table of Contents

Results in Brief	3
Background	5
Federal Retirement Thrift Investment Board	5
Federal Information Security Modernization Act of 2014.....	5
FY 2023-2024 Inspector General FISMA Reporting Metrics	6
Fiscal Year (FY) 2024 Audit Results and Findings	8
Identify	8
Protect	11
Detect	16
Respond	18
Recover	19
Appendix A. Objectives, Scope, and Methodology	22
Objectives	22
Scope.....	22
Sampling Methodology.....	22
Use of Computer-Processed Data	23
Compliance with Standards	23
Appendix B. Status of Prior Year Recommendations	24
Appendix C. Management Response	25
Appendix D. FY 2024 Findings and Associated Criteria	26

Results in Brief

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. The 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) 2024 FISMA audit to provide a basis for the conclusions associated with the FY 2024 IG FISMA Reporting Metrics issued by the United States Department of Homeland Security (DHS) and Office of Management and Budget (OMB).

The objective of the FY 2024 FISMA audit was to determine the effectiveness of the FRTIB’s information security program and practices by utilizing the FY 2023-2024 IG FISMA reporting metrics¹, comprised of 20 core² and 17 supplemental³ reporting metrics.

The FY 2023-2024 IG FISMA reporting metrics are categorized into five (5) functional areas and nine (9) associated domains. Within each domain, Williams Adley reviewed a combination of entity-wide and system specific controls with a focus on the main information system supporting the FRTIB’s mission: Converge. Please refer to [Appendix A](#) of this report for further information regarding the scope of the FY 2024 FISMA audit.

At the conclusion of the FY 2024 audit, Williams Adley determined that the FRTIB continues to have an effective information security program across all nine (9) FISMA domains. Additionally, Williams Adley determined that the FRTIB achieved Level 5 (Optimized) for all FISMA domains⁴. *Table 1* and *Table 2* below outline the individual maturity ratings assigned to the core and supplemental metrics supporting the nine (9) FISMA domains, and the calculated average maturity scores. The [FY 2024 Audit Results and Findings](#) section of this report outlines the individual scores for each metric question evaluated and any findings identified.

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Optimized	5.00
Identify	Supply Chain Risk Management	Optimized	5.00
Protect	Configuration Management	Optimized	5.00
Protect	Identity and Access Management	Optimized	5.00
Protect	Data Protection and Privacy	Optimized	5.00
Protect	Security Training	Optimized	5.00
Detect	Information Security Continuous Monitoring	Optimized	5.00
Respond	Incident Response	Optimized	5.00
Recover	Contingency Planning	Optimized	5.00

Table 1 – FY 2024 Core Maturity Ratings

¹ [Final FY 2023 - 2024 IG FISMA Reporting Metrics v1.1 \(cisa.gov\)](#)

² Core metrics are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

³ Supplemental metrics are assessed at least once every two (2) years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

⁴ Within the context of the FISMA, Level 4 (Managed and Measurable) is considered effective.

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Optimized	5.00
Identify	Supply Chain Risk Management	Optimized	5.00
Protect	Configuration Management	Optimized	5.00
Protect	Identity and Access Management	Optimized	5.00
Protect	Data Protection and Privacy	Optimized	5.00
Protect	Security Training	Optimized	5.00
Detect	Information Security Continuous Monitoring	Optimized	5.00
Respond	Incident Response	Optimized	5.00
Recover	Contingency Planning	Optimized	5.00

Table 2 – FY 2024 Supplemental Maturity Ratings

Additionally, Williams Adley followed up on the status of any outstanding recommendations issued since the FY 2017 FISMA audit and determined that the FRTIB had implemented corrective actions to address its final outstanding recommendation. Refer to [Appendix B](#), Status of Prior-Year Recommendations, for additional details.

Lastly, Williams Adley prepared and submitted the responses to the 20 core and 17 supplemental metric questions to DHS via the CyberScope application by July 31, 2024, as required by OMB Memorandum M-24-04 (“Memorandum for the Heads of Executive Departments and Agencies: FY 2024 Guidance on Federal Information Security and Privacy Management Requirements”).

Background

The Federal Retirement Thrift Investment Board (FRTIB)

The FRTIB was created by the Federal Employees' Retirement System Act of 1986 (FERSA) to administer the Thrift Saving Plan (TSP) as one (1) element in the three-part retirement program for civilian employees covered under the Federal Employee Retirement System (FERS). Over the past thirty-seven years, the FRTIB has expanded to cover members of the uniformed services, initially as a voluntary supplement, and now as a key component of the Blended Retirement System (BRS). The TSP is the largest defined contribution retirement plan with over 7 million participants and over \$900 billion in assets under management.

The Converge Team

In 2020, the FRTIB awarded the recordkeeping contract to Accenture Federal Services (AFS). AFS, in collaboration with its contracting partner Alight (referred further as the Converge Team), serves as a managed service provider. The Converge Team is responsible for delivering a comprehensive solution aligned with modern technical, operational, and functional capabilities. This initiative aims to modernize participant and administrative services, enhancing the experience for participants and beneficiaries. By introducing new services, improving plan participation, and ensuring a secure platform, the Converge Team continues to drive positive outcomes.

Federal Information Security Modernization Act of 2014 (FISMA)

The Federal Information Security Management Act of 2002, part of the E-Government Act of 2002 (Public Law 107-347), recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act of 2002 required each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support operations and assets, including those provided or managed by another agency or contractor. The E-Government Act of 2002 also assigned specific responsibilities to the Office of Management and Budget (OMB), agency heads, chief information officers, and Inspectors General. The Act established that OMB is responsible for creating and overseeing policies, standards, and guidelines for information security and has the authority to approve agencies' information security program. Additionally, the Act established that the OMB is responsible for submitting an annual report to Congress, developing, and approving the cybersecurity portions of the President's Budget, and overseeing budgetary and fiscal issues related to the agencies' use of funds.

In 2014, the FISMA was enacted to update the Federal Information Security Management Act of 2002 by reestablishing the oversight authority of the Director of OMB with respect to agency information security policies and practices and setting forth authority for the Department of Homeland Security (DHS) Secretary to administer the implementation of such policies and practices for information systems. FISMA also provides several modifications that modernize Federal security practices to address evolving security concerns. These changes result in less overall reporting, stronger use of continuous monitoring in systems, increased focus on the agencies for compliance, and reporting that is more focused on the issues caused by security incidents. Furthermore, OMB regulations require Federal agencies to ensure that the appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. Specifically, the agency's chief information officer is required to designate a senior information security officer whose primary duty is to implement an agency information security program. Each agency must establish a risk-based information security program that ensures information security is practiced throughout the life cycle of each agency's systems.

FISMA requires agencies to have an annual independent evaluation of their information security program and practices and to report the results to OMB and DHS via the CyberScope reporting tool. FISMA states

that the independent evaluation is to be performed by the agency Office of Inspector General (OIG) or an independent external auditor. FISMA specifically mandates that each independent evaluation must include a test of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems and an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

FY 2023-2024 Inspector General FISMA Reporting Metrics

Williams Adley utilized the FISMA metrics published by the OMB and the DHS, in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to evaluate the effectiveness of the FRTIB’s information security program and practices. The Inspector General (IG) FISMA reporting metrics are organized around the five (5) security functions — Identify, Protect, Detect, Respond, and Recover — as outlined in National Institute of Standards and Technology (NIST)’s cybersecurity framework.

On December 4, 2023, the OMB issued Memorandum M-24-04 (“Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year (FY) 2024 Guidance on Federal Information Security and Privacy Management Requirements”) to provide instructions for meeting the FY 2024 FISMA reporting requirements.

According to the memorandum, the FY 2024 reporting period presents the opportunity for an agency Inspector General or independent assessor to evaluate the following group of metrics:

- Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.
- Supplemental Metrics – Metrics that are assessed at least once every two (2) years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

Maturity Model and Scoring Methodology

The OMB provided guidance to agency IGs or independent assessors for determining the maturity of their agencies’ security programs through the publication of the FY 2023 – 2024 IG FISMA Reporting Metrics. According to the reporting metrics, “the OMB believes that achieving a Level 4 (managed and measurable) or above represents an effective level of security”; see **Table 3** below for a definition of each maturity level.

Maturity Level	Description
Level 1 – Ad-Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner
Level 2 – Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented
Level 3 – Consistently Implemented	Policies, procedures, and strategies 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 strategies are collected across the organization and used to assess them and make necessary changes
Level 5 – Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 3 – IG Evaluation Maturity Level Descriptions

Additionally, IGs and independent auditors are instructed to use “a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (identify, protect, detect, respond, and recover) and the overall program.” As part of this approach, core metrics and supplemental metrics will be averaged independently to determine a domain’s maturity calculation and provide data points for the assessed program and function effectiveness. This presents a shift from the “mode” based scoring methodology used in previous years where a domain and function’s maturity rating were determined by a simple majority, the most frequent level across the questions served as the rating.

Furthermore, IGs and independent auditors are instructed that calculated averages will not be automatically rounded to a particular maturity level. Instead, the determination of maturity levels and the overall effectiveness of the agency’s information security program should focus on the results of the core metrics and the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program and function level effectiveness.

Fiscal Year (FY) 2024 Audit Results and Findings

Williams Adley assessed the effectiveness of the Federal Retirement Thrift Investment Board (FRTIB)'s information security program and practices on a maturity model where the foundational levels (Levels 1-2) ensure that policies and procedures are designed to support the requirements outlined within the Federal Information Security Modernization Act of 2014 (FISMA) and advanced levels (Levels 3-5) focus on the implementation, operating effectiveness, and continuous improvement of the defined policies and procedures. The following sections outline the results of our FY 2024 FISMA audit across all nine (9) FISMA domains.

Identify

The Identify security function is comprised of the Risk Management and Supply Chain Risk Management metric domains. Based on our audit of the two (2) program areas, Williams Adley determined that the Identify security function met the requirements of an effective information security program.

Risk Management

Risk management embodies the program and supporting processes to manage information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.

Risk Management – Core Reporting Metrics

The Office of Management and Budget (OMB) identified five (5) reporting metrics as core for the development of a Risk Management program, as outlined in **Table 4**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
1	Comprehensive and accurate inventory of agency information systems.	Level 5	Level 5
2	An up-to-date inventory of hardware assets.	Level 4	Level 5
3	An up-to-date inventory of software and associated licenses.	Level 4	Level 5
5	Information system security risks are adequately managed at all organization tiers.	Level 4	Level 5
10	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.	Level 4	Level 5

Table 4 – Ratings for Core Metric Questions within the Risk Management Domain

Based on the audit procedures performed and the scores outlined in **Table 4** above, Williams Adley determined that the Risk Management core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized)⁵.

⁵ The FY 2024 IG FISMA Metrics state that “calculated averages will not be automatically rounded to a particular maturity level.” Furthermore, IGs or independent assessors are provided with the discretion to select the appropriate maturity rating based on the results of the audit procedures performed. Williams Adley believes that the current maturity of the activities associated with supplemental metrics do not significantly impact the agency’s ability to manage risks within its organization.

Risk Management – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2024, as outlined in *Table 5*:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating⁶
4	Priority of information systems are categorized and communicated.	Level 4	Level 5
6	Information security architecture is used to provide a disciplined and structured methodology for managing risk and supply chain's risk.	Level 2	Level 5

Table 5 – Ratings for Supplemental Metric Questions within the Risk Management Domain

Based on the audit procedures performed and the scores outlined in *Table 5* above, Williams Adley determined that the Risk Management supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley determine that FISMA metric question 1 remains at Level 5 (Optimized) as the FRTIB continues to use automation within its environment to maintain a centralized inventory of its information system and its component hardware and software inventories. Additionally, Williams Adley confirmed that the Agency's centralized inventory is updated on a real time basis through a series of different discovery scans.

Williams Adley determined the maturity for FISMA metric question 2 to be Level 5 (Optimized) as the FRTIB utilizes automation to track the life cycle of the hardware assets and ensure that the hardware assets inventory is regularly updated. Further, Williams Adley confirmed that the FRTIB enforces the capability to deny access to its enterprise services when security the mobile devices do not adhere to established baselines.

Williams Adley determined the maturity for FISMA metric question 3 to be Level 5 (Optimized) as the FRTIB utilizes automation to track the life cycle of the software assets and license information. Both software assets and license information are tracked and managed and discovery scans are scheduled and run to identify the assets.

Williams Adley identified an increase in the maturity for FISMA metric question 4, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, Business Impact Analysis (BIA) was conducted based on the primary mission-critical business processes established by the FRTIB to identify critical data, systems, and business processes. In addition, the FRTIB has continued to use its risk register and the Cybersecurity Framework (CSF) profile to align cybersecurity outcome with its mission or business requirements, risk tolerance, and resources. The FRTIB utilizes both tools to ensure the risk-based allocation of resources based on system categorization.

Williams Adley identified an increase in the maturity for FISMA metric question 5 to Level 5 (Optimized) as the FRTIB developed and utilized the risk register and the CSF profile to manage security risk across the FRTIB and to align cybersecurity outcome with its mission or business requirements, risk tolerance, and

⁶ The FY 2024 supplemental FISMA reporting metrics were last evaluated during the FY 2021 reporting period.

resources. Further, the FRTIB continue to perform control activities which allow for the communication of cybersecurity across all organizational tiers and into its overall enterprise risk management program.

Williams Adley identified an increase in the maturity for FISMA metric question 6, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, Williams Adley confirmed that the Converge system's information security architecture is integrated with the FRTIB's systems development life cycle. Moreover, both the FRTIB and the Converge Team utilize advanced technologies and techniques to manage and mitigate supply chain risks.

Williams Adley identified an increase in the maturity for FISMA metric question 10 to Level 5 (Optimized) as the FRTIB considers various audits such as its annual FISMA audit as a benchmark to continuously improve its cybersecurity risk management program. Additionally, the FRTIB leverages reports and benchmarks from a continuous penetration testing provider to allow near real-time analysis of trends and performance that leads to continuous improvement in cybersecurity risk management program.

Supply Chain Risk Management

The Supply Chain Risk Management domain focuses on the maturity of agency strategies, policies and procedures, plans, and processes 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.

Supply Chain Risk Management – Core Reporting Metrics

The OMB identified one (1) reporting metric as core for the development of a Supply Chain Risk Management program, as outlined in **Table 6**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
14	The agency ensures that products, system components, systems, and services of external providers are consistent with cybersecurity and supply chain requirements.	Level 4	Level 5

Table 6 – Ratings for Core Metric Questions within the Supply Chain Risk Management Domain

Based on the audit procedures performed and the scores outlined in **Table 6** above, Williams Adley determined that the Supply Chain Risk Management core metric has a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Supply Chain Risk Management – Supplemental Reporting Metrics

The OMB identified one (1) supplemental reporting metrics for evaluation in FY 2024, as outlined in **Table 7**:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
15	The agency ensures that counterfeit components are detected and prevented from entering the organization's systems.	N/A	Level 5

Table 7 – Ratings for Supplemental Metric Questions within the Supply Chain Risk Management Domain

Based on the audit procedures performed and the scores outlined in *Table 7* above, Williams Adley determined that the Supply Chain Risk Management supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric question 14 and 15 to Level 5 (Optimized). Based on the audit procedures performed during the FY 2024 FISMA audit, Williams Adley concluded that both the FRTIB and the Converge Team implemented process to assess and review supply chain risks as well as component authenticity. Furthermore, both the FRTIB and the Converge Team utilizes qualitative and quantitative performance metrics to monitor the information security, supply chain risk management performance of external providers, and component authenticity policies and procedures. Lastly, the impact of material changes to security and supply chain risk management assurance requirements on its relationships with external providers are analyzed in a near real-time to ensure that acquisition tools, methods, and processes are updated as appropriately to evolving threats.

Protect

The Protect security function is comprised of Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training metric domains. Based on our audit of the four (4) program areas, Williams Adley determined that all four (4) security domains within the Protect function meet the minimum requirements of an effective information security program.

Configuration Management

Configuration management includes tracking an organization's hardware, software, and other resources to support networks, systems, and network connections. This includes software versions and updates installed on the organization's computer systems.

Configuration Management – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of a Configuration Management program, as outlined in *Table 8*:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
20	Use of configuration settings and common secure configurations.	Level 4	Level 5
21	Use of flaw remediation processes.	Level 4	Level 5

Table 8 – Ratings for Core Metric Questions within the Configuration Management Domain

Based on the audit procedures performed and the scores outlined in *Table 8* above, Williams Adley determined that the Configuration Management core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Configuration Management – Supplemental Reporting Metrics

The OMB identified three (3) supplemental reporting metrics for evaluation in FY 2024, as outlined in *Table 9*:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
17	The roles and responsibilities of configuration management stakeholders been defined, communicated, and implemented across the agency, and appropriately resourced.	Level 4	Level 5
18	Use of process for identifying and managing configuration items during the appropriate phase within an organization's Software Development Life Cycle (SDLC).	Level 4	Level 5
23	Use of implemented configuration change control activities.	Level 4	Level 5

Table 9 – Ratings for Supplemental Metric Questions within the Configuration Management Domain

Based on the audit procedures performed and the scores outlined in *Table 9* above, Williams Adley determined that the Configuration Management supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric question 17, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB reviewed and adjusted its configuration management roles and responsibilities to address the evolving cybersecurity landscape.

Williams Adley identified an increase in the maturity for FISMA metric question 18, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has implemented automation to adapt its configuration management plan and related processes and activities to a changing cybersecurity landscape on a near real-time basis.

Williams Adley identified an increase in the maturity for FISMA metric question 20 to Level 5 (Optimized) as the FRTIB has deployed system configuration management tools that automatically enforce and redeploy configuration settings to systems.

Williams Adley identified an increase in the maturity for FISMA metric question 21 to Level 5 (Optimized) as the FRTIB has implemented and utilized automated patch management and software update tools for all applications and network devices, including mobile devices.

Williams Adley identified an increase in the maturity for FISMA metric question 23, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has implemented automation to improve the accuracy, consistency, and availability of configuration change control and configuration baseline

information. Further, the automation provides data aggregation and correlation capabilities, alerting mechanisms, and dashboards on change control activities to support risk-based decision making across the organization.

Identity and Access Management

Identity and Access Management refers to identifying users, using credentials, and managing user access to network resources. It also includes managing the user's physical and logical access to Federal facilities and network. Remote access allows users to remotely connect to internal resources while working from a location outside their normal workspace. Remote access management is the ability to manage all connections and computers that remotely connect to an organization's network. To provide an additional layer of protection, remote connections should require users to connect using two-factor authentication.

Identity and Access Management – Core Reporting Metrics

The OMB identified three (3) reporting metrics as core for the development of an Identity and Access Management program, as outlined in **Table 10**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
30	Use of strong authentication mechanisms (Personal Identity Verification (PIV) or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL)3 credential) for non-privileged users.	Level 5	Level 5
31	Use of strong authentication mechanisms (PIV or an IAL3/AAL3 credential) for privileged users.	Level 5	Level 5
32	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.	Level 5	Level 5

Table 10 – Ratings for Core Metric Questions within the Identity and Access Management Domain

Based on the audit procedures performed and the scores outlined in **Table 10** above, Williams Adley determined that the Identity and Access Management core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Identity and Access Management – Supplemental Reporting Metrics

The OMB identified one (1) supplemental reporting metric for evaluation in FY 2024, as outlined in **Table 11**:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
28	Processes for assigning position risk designations and performing appropriate personnel screening prior to granting access to its systems.	Level 4	Level 5

Table 11 – Ratings for Supplemental Metric Questions within the Identity and Access Management Domain

Based on the audit procedures performed and the scores outlined in *Table 11* above, Williams Adley determined that the Identity and Access Management supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric questions 28, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has implemented automation to centrally document, track, and share risk designations and screening information with appropriate parties. Further, the FRTIB evaluates personnel security information and integrates this information with anomalous user behavior data and its insider threat activities to adjust permissions accordingly.

Williams Adley determined that FISMA metric questions 30, 31, and 32 remains at Level 5 (Optimized) as the FRTIB continued to use a centralized enterprise-wide authentication solution to manage end user access across all Converge system components. Furthermore, the FRTIB is making progress towards implementing Event Logging (EL)³'s advanced requirements for user behavior monitoring.

Data Protection and Privacy

Federal organizations have a fundamental responsibility to protect the privacy of individuals' Personally Identifiable Information (PII) that is collected, used, maintained, shared, and disposed of by programs and information systems. PII is any information about a person maintained by an agency that can be used to distinguish or trace a person's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other information that is linked or linkable to a person, such as medical, educational, financial, and employment information. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law.

Data Protection and Privacy – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of a Data Protection and Privacy program, as outlined in *Table 12*:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
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.	Level 4	Level 5
37	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 4	Level 5

Table 12 – Ratings for Core Metric Questions within the Data Protection and Privacy Domain

Based on the audit procedures performed and the scores outlined in *Table 12* above, Williams Adley determined that the Data Protection and Privacy core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Data Protection and Privacy – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metric for evaluation in FY 2024, as outlined in *Table 13*:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
38	Development and implementation of a Data Breach Response Plan.	Level 4	Level 5
39	The privacy aware training is provided to all individuals, including role-based privacy training.	Level 4	Level 5

Table 13 – Ratings for Supplemental Metric Questions within the Data Protection and Privacy Domain

Based on the audit procedures performed and the scores outlined in *Table 13* above, Williams Adley determined that the Data Protection and Privacy supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric questions 36 and 37 to Level 5 (Optimized) as the FRTIB continues to utilize security controls to ensure that data within its environment is appropriately encrypted, assets are properly sanitized prior to disposal or reuse, and the potential for data exfiltration is appropriately managed. Additionally, the FRTIB's data exfiltration and enhanced network defenses are fully integrated into the Information Security Continuous Monitoring (ISCM) and incident response programs.

Williams Adley identified an increase in the maturity for FISMA metric question 38, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has fully integrated its Data Breach Response plan with incident response, risk management, continuous monitoring, and other mission areas. Moreover, the FRTIB automated the privacy incident monitoring and takes immediate actions to mitigate the identified incidents.

Williams Adley identified an increase in the maturity for FISMA metric question 39, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has measured the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the FRTIB make updates to its training program based on feedback and changing regulatory landscape.

Security Training

Security awareness training is a formal process for educating employees and contractors about IT security pertaining to the confidentiality, integrity, and availability of information. This includes ensuring that all people involved in using and managing IT understand their roles and responsibilities related to the organizational mission; understand the organization's IT security policy, procedures, and practices; and have adequate knowledge of the various management, operational, and technical controls required to protect the IT resources for which they are responsible. For example, we judgmentally selected a small sample of new user accounts and verified that security training was completed.

Security Training – Core Reporting Metrics

The OMB identified one (1) reporting metric as core for the development of Security Training program, as outlined in *Table 14*:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
42	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training.	Level 4	Level 5

Table 14 – Ratings for Core Metric Questions within the Security Training Domain

Based on the audit procedures performed and the scores outlined in *Table 14* above, Williams Adley determined that the Security Training core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Security Training – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2024, as outlined in **Table 15**:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
44	Security awareness training is provided to all system users and is tailored based on its mission, risk environment, and types of information systems.	Level 3	Level 5
45	Specialized security training is provided to individuals with significant security responsibilities.	Level 4	Level 5

Table 15 – Ratings for Supplemental Metric Questions within the Security Training Domain

Based on the audit procedures performed and the scores outlined in *Table 15* above, Williams Adley determined that the Security Training supplemental metrics have a calculated 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase the maturity for FISMA metric question 42 to Level 5 (Optimized). Based on the audit procedures performed during the FY 2024 FISMA audit, Williams Adley concluded that the FRTIB security training stakeholders continued to perform their assigned roles and responsibilities, including addressing skill gaps and executing the FRTIB's security training program.

Williams Adley identified an increase in the maturity for FISMA metric questions 44 and 45, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has developed and incorporated qualitative and quantitative performance measures and successfully monitored and analyzed the effectiveness of its security awareness policies, procedures, and practices. Furthermore, in FY 2024, the FRTIB implemented a feedback mechanism and continued to adapt its security awareness policies, procedures, processes to a changing cybersecurity landscape on a near real-time basis.

Detect

The Detect security function is comprised of the ISCM metric domain. Based on our audit of the program area, Williams Adley determined that the ISCM security domain does meet the requirements of an effective information security program.

ISCM

Continuous monitoring of organizations and information systems determines the ongoing effectiveness of deployed security controls; changes in information systems and environments of operation; and compliance with legislation, directives, policies, and standards.

ISCM – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of a ISCM program, as outlined in **Table 16**:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
47	Use of ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier	Level 5	Level 5
49	Performance of ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls	Level 5	Level 5

Table 16 – Ratings for Core Metric Questions within the ISCM Domain

Based on the audit procedures performed and the scores outlined in **Table 16** above, Williams Adley determined that the ISCM core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

ISCM – Supplemental Reporting Metrics

The OMB identified one (1) supplemental reporting metric for evaluation in FY 2024, as outlined in **Table 17**:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
50	Process for collecting and analyzing ISCM performance measures and reporting findings.	Level 4	Level 5

Table 17 – Ratings for Supplemental Metric Questions within the ISCM Domain

Based on the audit procedures performed and the scores outlined in **Table 17** above, Williams Adley determined that the ISCM supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley determined that the maturity for FISMA metric questions 47 and 49 remain at Level 5 (Optimized) as the FRTIB continued to integrate its ISCM program with the activities outlined within its supply chain risk management, configuration management, incident response, and business continuity programs.

Williams Adley identified an increase the maturity for FISMA metric question 50 to Level 5 (Optimized). Based on the audit procedures performed during the FY 2024 FISMA audit, Williams Adley concluded that the FRTIB actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

Respond

The Respond security function is comprised of the Incident Response metric domain. Based on our audit of the program area, Williams Adley determined that the Incident Response security domain does meet the minimum requirements of an effective information security program.

Incident Response

An organization's incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited to prevent future occurrences, and restoring IT services. The goal of the incident response program is to provide surveillance, situational monitoring, and cyber defense services; rapidly detect and identify malicious activity and promptly subvert that activity; and collect data and maintain metrics that demonstrate the impact of the FRTIB's cyber defense approach, its cyber state, and cyber security posture.

Incident Response – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of an Incident Response program, as outlined in *Table 18*:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
54	Processes for incident detection and analysis.	Level 5	Level 5
55	Processes for incident handling.	Level 4	Level 5

Table 18 – Ratings for Core Metric Questions within the Incident Response Domain

Based on the audit procedures performed and the scores outlined in *Table 18* above, Williams Adley determined that the Incident Response core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Incident Response – Supplemental Reporting Metrics

The OMB identified three (3) supplemental reporting metrics for evaluation in FY 2024, as outlined in *Table 19*:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
52	Use an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents.	Level 4	Level 5
53	Roles, responsibilities, levels of authority, and level of dependencies of incident response team.	Level 4	Level 5

56	Incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders.	Level 4	Level 5
----	--	---------	---------

Table 19 – Ratings for Supplemental Metric Questions within the Incident Response Domain

Based on the audit procedures performed and the scores outlined in *Table 19* above, Williams Adley determined that the Incident Response supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric question 52, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has fully integrated its incident response plan with risk management, continuous monitoring, continuity of operations, and other mission/business areas. Furthermore, the FRTIB continuously makes near real-time updates to its incident response plan based on changing risk environments and threat information. Lastly, the FRTIB participated in DHS's Cyber Storm national level exercise.

Williams Adley identified an increase in the maturity for FISMA metric question 53, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has ensured that the resources are allocated in a risk-based manner for stakeholders to effectively implement the incident response activities and that the stakeholders are held accountable for carrying out their roles and responsibilities. Moreover, the FRTIB continuously evaluates and adapts its incident response-based roles and responsibilities to align with changing cybersecurity landscape.

Williams Adley determined that FISMA metric question 54 remains at a Level 5 (Optimized) as the FRTIB and the Converge Team continued to progress towards implementing EL3's requirements for its logging capabilities.

Williams Adley identified an increase in the maturity for FISMA metric question 55 to Level 5 (Optimized). Based on the audit procedures performed during the FY 2024 FISMA audit, Williams Adley concluded that the FRTIB consistently implements its incident handling policies, procedures, containment strategies, and incident eradication processes. Additionally, the FRTIB utilizes performance measures to evaluate the effectiveness of its incident response program and dynamic reconfiguration to prevent attacks, misdirect attackers, and to isolate components of systems.

Williams Adley identified an increase in the maturity for FISMA metric question 56, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has established and utilized metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. In addition, the FRTIB receives, retains, uses, and disseminates cyber threat indicators in accordance with the Cybersecurity Information Sharing Act of 2015.

Recover

The Recover security function is comprised of the Contingency Planning metric domain. Based on our audit of the program area, Williams Adley determined that the Contingency Planning security domain does meet the requirements of an effective information security program.

Contingency Planning

Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocating information systems and operations to an alternate site, recovering information system functions using alternate equipment, or performing information system functions using

manual methods.

Contingency Planning – Core Reporting Metrics

The OMB identified two (2) reporting metrics as core for the development of an Incident Response program, as outlined in *Table 20*:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2024 Maturity Rating
61	BIAs are used to guide contingency planning efforts.	Level 3	Level 5
63	Performance of Information System Contingency Plan (ISCP) tests/exercises.	Level 4	Level 5

Table 20 – Ratings for Core Metric Questions within the Contingency Planning Domain

Based on the audit procedures performed and the scores outlined in *Table 20* above, Williams Adley determined that the Contingency Planning core metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Contingency Planning – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2024, as outlined in *Table 21*:

Metric Question	Topic	FY 2021 Maturity Rating	FY 2024 Maturity Rating
62	ISCPs are developed, maintained, and integrated with other continuity plans.	Level 2	Level 5
64	Information system backup and storage, including use of alternate storage and processing sites.	Level 3	Level 5

Table 21 – Ratings for Supplemental Metric Questions within the Contingency Planning Domain

Based on the audit procedures performed and the scores outlined in *Table 21* above, Williams Adley determined that the Contingency Planning supplemental metrics have a calculated average score of 5.00 and a maturity rating of Level 5 (Optimized).

Changes in Metric Question Maturity

Williams Adley identified an increase in the maturity for FISMA metric question 61 to Level 5 (Optimized) as the FRTIB has integrated its BIA and asset management processes with its enterprise risk management program to improve risk identification, accurate exposure considerations, and effective risk response.

Williams Adley identified an increase in the maturity for FISMA metric question 62, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has established and utilized metrics on the effectiveness of its various contingency plans to deliver persistent situational awareness across the organization. Further, the FRTIB's ISCP activities are fully integrated with its enterprise risk management program.

Williams Adley identified an increase in the maturity for FISMA metric question 63 to Level 5 (Optimized) maturity as the FRTIB has performed tests of its contingency planning processes with external stakeholders. Additionally, the FRTIB has automated the testing of various contingency plans and performs a full recovery and reconstitution of systems to a known state based on risk.

Williams Adley identified an increase in the maturity for FISMA metric question 64, last evaluated in FY 2021, to Level 5 (Optimized). Since FY 2021, the FRTIB has ensured that its information system backup and storage process, including use of alternate storage and processing sites, are assessed. Further, the FRTIB demonstrated that its system backup and storage and alternate storage and processing sites are configured to facilitate recovery operations in accordance with recovery time and point objectives. Lastly, the FRTIB protects its backup data from infection or other compromises and maintains up-to-date recovery catalog for sensitive data and Executive Order (EO)-critical software.

Appendix A. Objectives, Scope, and Methodology

Objectives

The primary objective of the Fiscal Year (FY) 2024 Federal Information Security Modernization Act of 2014 (FISMA) audit was to determine whether the Federal Retirement Thrift Investment Board (FRTIB)'s overall information technology security programs and practices are effective as they relate to Federal information security requirements. The secondary objective of the FY 2024 FISMA audit was to determine the corrective actions taken by the FRTIB to address previously identified issues.

To accomplish the two (2) objectives, Williams Adley obtained an understanding of the FRTIB's information security program and processes across the 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
- Contingency Planning.

Scope

The FY 2024 audit covered the period October 1, 2023, to July 19, 2024. During the audit fieldwork, we conducted remote activities using Microsoft Teams as needed for walkthroughs and information validation.

To form the basis of the conclusion regarding the effectiveness of the FRTIB's overall information security program, Williams Adley evaluated the FRTIB's Converge system. The Converge system is referred to as a "system of systems" and includes the following subsystems:

- Participant Administrative Services (PAS) subsystems, which enable core Thrift Savings Plan functionality; and
- Non-PAS subsystems, which augment and support the PAS subsystems.

Subsystems are also grouped into five (5) High Value Assets (HVAs) and one (1) General Support System. From the list of HVAs, Williams Adley selected the Recordkeeping Services and Identity Services HVAs for the FY 2024 audit.

Sampling Methodology

Williams Adley used nonstatistical audit sampling techniques, where applicable and appropriate, and utilized the American Institute of Certified Public Accountants (AICPA) Audit Guide: Audit Sampling, First Edition. Chapter 3: Nonstatistical and Statistical Audit Sampling in Tests of Controls. This guidance has been conformed to Statement on Auditing Standards (SAS) Nos. 122-125 and assists in applying audit sampling in accordance with AU-C section 530, *Audit Sampling* (AICPA, *Professional Standards*).

AU-C section 530, *Audit Sampling* allows auditors to use nonstatistical sampling for tests of controls. In addition, for a nonstatistical 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 nonstatistical sampling, Williams Adley used a sample selection approach that approximates a random sampling approach, including the following:

- **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 nonstatistical 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).

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 the 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.

Compliance with Standards

Williams Adley conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B. Status of Prior Year Recommendations

As a part of the audit procedures for Fiscal Year (FY) 2024, Williams, Adley & Company-DC, LLP (Williams Adley) assessed the status of the Federal Retirement Thrift Investment Board (FRTIB)'s remediation efforts to address the outstanding recommendation from FY 2021 Federal Information Security Modernization Act of 2014 (FISMA) audit and documented its status in the table below.

FY	Recommendation Description	Status
2021	Develop a standard data elements/taxonomy to maintain a complete and accurate population of data breaches.	Closed

Appendix C. Management Response



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

July 29, 2024

Mr. Tony Wang, Partner
Cybersecurity Risk Services
Williams Adley
Unit 400
1016 16th St., NW
Washington, D.C. 20036

Dear Mr. Wang:

Thank you for the opportunity to review the draft FY 2024 FISMA audit report. On behalf of the agency, I am in agreement with the report.

All prior year audit recommendations have been closed and no new findings were identified for FY24. The FRTIB will continue to adapt its cybersecurity program to match the evolving threat landscape and will work with FISMA auditors to identify new opportunities for improvement.

Regards,



Vijay Desai
Chief Information Officer

cc: Ravindra Deo, Executive Director
Patrick Bevill, Chief Information Security Officer
Peter Robbins, Chief Privacy Officer
Barbara Holmes, Chief Audit Executive

Appendix D. FY 2024 Findings and Associated Criteria

Based on the audit procedures and testing conducted as part of the FY 2024 FISMA audit, Williams Adley did not identify any findings related to the core and second group of supplemental Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics.