OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF TRANSPORTATION

Report QC2023044
September 11, 2023

Quality Control Review of an Independent Auditor's Report on the Surface Transportation Board's Information Security Program and Practices

U.S. Department of Transportation
Office of Inspector General

Highlights

Quality Control Review of an Independent Auditor's Report on the Surface Transportation Board's Information Security Program and Practices

Required by the Federal Information Security Modernization Act of 2014

QC2023044 | September 11, 2023

What We Looked At

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to implement information security programs. FISMA also requires agencies to have annual independent evaluations performed to determine the effectiveness of their programs and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, the Surface Transportation Board (STB) requested that we perform its fiscal year 2023 FISMA review. We contracted with Williams Adley & Company-DC LLP (Williams Adley), an independent public accounting firm, to conduct this audit subject to our oversight. The audit objective was to determine the effectiveness of STB's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

We performed a quality control review (QCR) of Williams Adley's report and related documentation. Our QCR disclosed no instances in which Williams Adley did not comply, in all material respects, with generally accepted Government auditing standards.

Our Recommendations

While there are no new recommendations issued for fiscal year 2023, STB concurs with the audit's findings with respect to the five open recommendations remaining from the fiscal year 2021 FISMA audit.

All OIG audit reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Government and Public Affairs at (202) 366-8751.

U. S. Department of Transportation
Office of Inspector General

September 11, 2023

The Honorable Martin J. Oberman
Chairman, Surface Transportation Board
395 E Street, SW
Washington, DC 20423-0001

Dear Mr. Oberman:

I respectfully submit our report on the quality control review (QCR) of the independent auditor's report on the Surface Transportation Board's (STB) information security program and practices.

The Federal Information Security Modernization Act of 2014[1] (FISMA) requires agencies to implement information security programs. The act also requires agencies to have annual independent evaluations performed to determine the effectiveness of their programs and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, STB requested that we perform its fiscal year 2023 FISMA review. Williams Adley & Company-DC LLP (Williams Adley) of Washington, DC, completed the audit of STB's information security program and practices (see attachment) under contract with the Office of Inspector General (OIG).

The audit objective was to determine the effectiveness of STB's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

Williams Adley found that STB's information security program and practices were not effective. There are no new recommendations to improve STB's information and security practices, as the issues identified within each of the five function areas for fiscal year 2023 were consistent with those identified in fiscal year 2021.

We appreciate the cooperation and assistance of the STB representatives. If you have any questions about this report, please contact me or Leon Lucas, Program Director.

Sincerely,

Kevin Dorsey
Assistant Inspector General for Information Technology Audits

cc: STB Audit Liaison
Attachment

[1] Pub. L. No. 113-283 (2014).

Quality Control Review

We performed a QCR of Williams Adley's report, dated July 31, 2023_ (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement and performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on STB's information security program and practices. Williams Adley is responsible for its independent auditor's report and the conclusions expressed in that report. Our QCR disclosed no instances in which Williams Adley did not comply, in all material respects, with generally accepted Government auditing standards.

Agency Comments and OIG Response

On June 16, 2023, Williams Adley provided STB with its draft report and received STB's response on June 29, 2023, which is included in its entirety in the attached independent auditor's report.

While there are no new recommendations issued for fiscal year 2023, STB concurs with the audit's findings with respect to the five open recommendations remaining from the fiscal year 2021 FISMA audit.

Actions Required

We consider the remaining recommendations 1, 5, 8, 15, and 17 from William Adley's fiscal year 2021 audit of STB's information security program and practices still applicable and resolved but open pending completion of planned actions.

Exhibit. List of Acronyms

DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act
OIG	Office of Inspector General
OMB	Office of Management and Budget
QCR	Quality Control Review
STB	Surface Transportation Board

Attachment. Independent Auditor’s Report

Fiscal Year 2023 Federal Information Security Modernization Act of 2014 Audit of the Surface Transportation Board's Information Security Program and Practices

July 31, 2023

Contents

Results in Brief 2

Background 4

Results of the FY 2023 FISMA Audit 6

I. Identify 6

II. Protect 8

III. Detect 13

IV. Respond 15

V. Recover 16

Conclusion 17

Recommendations 17

Appendix A – Objective, Scope, and Methodology 18

Appendix B – Status of Prior Year Federal Information Security Modernization Act of 2014 (FISMA) Recommendations 19

Appendix C – Management's Response 20

Mr. Kevin Dorsey
Assistant Inspector General for Information Technology Audits
1200 New Jersey Avenue, SE
Washington, DC 20590

Dear Mr. Dorsey:

We are pleased to provide our report outlining the result of the performance audit conducted to determine the effectiveness of Surface Transportation Board (STB)'s information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year (FY) 2023 audit. On December 2, 2022, the Office of Management and Budget (OMB) issued Memorandum M-23-03 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2023 FISMA reporting requirements.

To achieve this objective, we reviewed the FISMA security metrics and performance measures selected by OMB and conducted this performance audit in accordance with Generally Accepted Government Auditing Standards which requires that we 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 throughout the FY 2023 audit provides a reasonable basis for our conclusions and maturity ratings.

Overall, the STB has continued to make improvements to its overall information security program but has not met the requirements outlined within the FY 2023 FISMA reporting metrics to be operating at an effective level of security.

STB management has provided us with a response to the FY 2023 FISMA audit report and is presented in its entirety in the Management's Response section of the report. Please note that we did not audit the management's response and, accordingly, do not express any assurance on it.

Williams, Adley & Company-DC, LLP
June 30, 2023

Results in Brief

Williams Adley concluded that the Surface Transportation Board (STB)'s overall information security program was ineffective[1] for FY 2023 reporting period. However, the STB made improvements, since the previous reporting period, by taking corrective actions to address three (3) previously identified recommendations[2] and continuing to implement its defined processes.

The FY 2023 reporting period presents the first opportunity for an agency Inspector General or independent assessor to evaluate the core group of metrics, which represent a combination of Administration priorities and other highly valuable controls, that must be evaluated annually, and the remainder of the reporting metrics or supplemental group of metrics which are evaluated on a 2-year cycle. Presented below in ***Table 1*** and ***Table 2*** are the results of the FY 2023 audit from a core and supplemental metric perspective. Details regarding the calculation of each FISMA domain's rating are found within the body of the report.

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Consistently Implemented	3.2
Identify	Supply Chain Risk Management	Ad-Hoc	1
Protect	Configuration Management	Defined	2.5
Protect	Identity and Access Management	Managed and Measurable	3.7
Protect	Data Protection and Privacy	Defined	2.5
Protect	Security Training	Consistently Implemented	3
Detect	Information Security Continuous Monitoring	Defined	2.5
Respond	Incident Response	Consistently Implemented	3
Recover	Contingency Planning	Consistently Implemented	3

Table 1 - FY 2023 Core Maturity Ratings

Function	Domain	Maturity Rating	Calculated Average
Identify	Risk Management	Consistently Implemented	2.67
Identify	Supply Chain Risk Management	Ad-Hoc	1
Protect	Configuration Management	Defined	2.33
Protect	Identity and Access Management	Consistently Implemented	3

[1] An information security program rated at a level 4, Managed and Measurable, is effective.

[2] The status of previously issued recommendations is found in Appendix B.

Protect	Data Protection and Privacy	Consistently Implemented	3
Protect	Security Training	Consistently Implemented	3
Detect	Information Security Continuous Monitoring	Defined	2
Respond	Incident Response	Consistently Implemented	3.5
Recover	Contingency Planning	Consistently Implemented	3

Table 2 - FY 2023 Supplemental Maturity Ratings

Williams Adley did not identify any new conditions for the FY 2023 reporting period and determined that the five (5) outstanding recommendations from the FY 2021 reporting period account for the gaps that should be addressed by STB management before the agency can be evaluated at higher maturity levels.

Lastly, to supplement the content within this report, we have included a copy of STB management's response to the results of the FY 2023 audit in ***Appendix C***. Please note that we did not audit the management's response and, accordingly, do not express any assurance on it.

Background

Agency

The Surface Transportation Board (STB) is an independent, adjudicatory body that, until passage of the Surface Transportation Board Reauthorization Act in December 2015, was within the oversight of the Department of Transportation (DOT). While part of the DOT, STB shared an information security program with DOT and its Operating Administrations. Now as a stand-alone Agency, STB is responsible for maintaining its own information security program and independently meeting Federal Information Security Modernization Act of 2014 (FISMA)'s requirements.

The Surface Transportation Board is charged with the economic regulation of various modes of surface transportation, primarily freight rail. Furthermore, the agency has authority over railroad rate, practice, and service issues and rail restructuring transactions, including mergers, line sales, line construction, and line abandonments. The STB also has jurisdiction over certain passenger rail matters, the intercity bus industry, non-energy pipelines, household goods carriers' tariffs, and rate regulation of non-contiguous domestic water transportation (marine freight shipping involving the mainland United States, Hawaii, Alaska, Puerto Rico, and other U.S. territories and possessions)[3].

Federal Information Security Modernization Act of 2014 (FISMA)

The FISMA requires each Federal agency to protect the information and information systems that support its operations, including those provided or managed by other agencies, entities, or contractors. Furthermore, the FISMA requires each agency to report annually to the Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO) on the effectiveness of its information security policies, procedures, and practices.

FISMA Reporting Metrics

Williams Adley utilized the FISMA metrics published by the OMB and the Department of Homeland Security (DHS), in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to evaluate the effectiveness of an organization's information security program. The 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 2, 2022, the OMB issued Memorandum M-23-03 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements") to provide instructions for meeting the FY 2023 FISMA reporting requirements.

According to the memorandum, the FY 2023 reporting period presents the first opportunity for an agency Inspector General or independent assessor to evaluate the core group of metrics, which represent a combination of Administration priorities and other highly valuable controls, that must be

[3] Source : https://www.stb.gov/about-stb/

evaluated annually, and the remainder of the reporting metrics or supplemental group of metrics which are evaluated on a 2-year cycle.

Maturity Model and Scoring Methodology

The OMB provided guidance to agency Inspector General or independent assessors for determining the maturity of their agencies' security programs through the publication of the FY 2023 – 2024 Inspector General 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".

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.

Results of the FY 2023 FISMA Audit

I. Identify

The Identify function is supported by the Risk Management and Supply Chain Risk Management domains.

Risk Management – Core Reporting Metrics

The 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 2022 Maturity Rating
1	Comprehensive and accurate inventory of agency information systems.	Level 3	Level 3
2	An up-to-date inventory of hardware assets.	Level 4	Level 3
3	An up-to-date inventory of software and associated licenses.	Level 4	Level 3
5	Information system security risks are adequately managed at all organization tiers.	Level 3	Level 3
10	Use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.	Level 2	Level 2

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

Williams Adley determined that the STB continues to maintain a comprehensive and accurate inventory of information systems (Question 1) and supporting hardware and software component inventories (Question 2 and 3). Additionally, with the use of a solution obtained from the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program, the STB can ensure that the hardware and software within its environment are covered by an organization-wide asset management capability and subject to the monitoring processes defined within the organization's ISCM strategy.

Furthermore, the STB has continued to manage information security risks identified as a part of annual system risk assessments, which are then communicated to senior leadership and included within the Agency’s risk register (Question 5).

Lastly, the STB does not utilize technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities and is currently in process of assessing its information security capabilities and has historically signed a corresponding risk acceptance (Question 10).

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 3.2 and a maturity rating of Level 3 (Consistently Implemented).

Risk Management – Supplemental Reporting Metrics

The OMB identified three (3) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 5***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating[4]
7	Roles and responsibilities of internal and external stakeholders.	Level 3	Level 3
8	Plans of action and milestones (POA&Ms) are used to effectively mitigate security weaknesses.	Level 2	Level 2
9	Information about cybersecurity risks is communicated in a timely and effective manner to appropriate internal and external stakeholders.	Level 3	Level 3

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

Williams Adley determined that the STB remains consistent with the performance of activities related to the supplemental metrics since the FY 2021 FISMA audit. Specifically:

- Risk Management stakeholders are consistently performing the cybersecurity risk management roles and responsibilities defined within the organization (Question 7).
- The STB has defined how it utilizes POA&Ms to effectively mitigate security weaknesses but is still in progress of implementing their processes (Question 8). The STB currently has an informal process to track and manage POA&Ms.
- The STB utilizes a cybersecurity risk register to ensure that information about risks is communicated in a timely and effective manner to appropriate stakeholders (Question 9).

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 2.67 and a maturity rating of Level 3 (Consistently Implemented)[5].

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 2022 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 1	Level 1

[4] The FY 2023 supplemental FISMA reporting metrics were last evaluated during the FY 2021 reporting period.

[5] The FY 2023 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.

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

Per discussion with STB management, the agency is still in process of developing the foundation of its SCRM program and implementing its corrective actions to address prior year recommendation 2021-05 related to the development of a SCRM strategy and supporting policies and procedures (Question 14).

Based on the audit procedures performed and the score outlined in ***Table 6*** above, Williams Adley determined that the Supply Chain Risk Management core metric has a calculated average score of 1 and a maturity rating of Level 1 (Ad-Hoc).

Supply Chain Risk Management – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 7***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
12	Agency wide SCRM strategy to manage supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.	Level 1	Level 1
13	The agency ensures that products, system components, systems, and services of external providers are consistent with cybersecurity and supply chain requirements.	Level 1	Level 1

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

Per discussion with STB management, the agency is still in process of developing the foundation of its SCRM program and implementing its corrective actions to address prior year recommendation 2021-05 related to the development of a SCRM strategy and supporting policies and procedures (Questions 12 and 13).

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 1 and a maturity rating of Level 1 (Ad-Hoc).

II. Protect

The Protect function is supported by the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains.

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 2022 Maturity Rating
20	Use of configuration settings and common secure configurations.	Level 2	Level 2
21	Use of flaw remediation processes.	Level 3	Level 2

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

Per discussion with STB management, the agency is still in process of implementing its corrective actions to address prior year recommendation 2021-08 related to the evaluation of deviations from established baseline configuration and common secure configurations (Question 20).

The STB made improvements to the maturity of its flaw remediation processes by implementing its previously defined policies and procedures to ensure that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner (Question 21).

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 2.5 and a maturity rating of Level 2 (Defined)[6].

Configuration Management – Supplemental Reporting Metrics

The OMB identified three (3) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 9***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
19	Use of baseline configurations.	Level 2	Level 2
22	Adoption of the Trusted Internet Connection (TIC) 3.0 program to assist in protecting the agency's network.	Level 2	Level 3
24	Use of a vulnerability disclosure policy (VDP) as part of its vulnerability management program.	Level 3	Level 2

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

Per discussion with STB management, the agency is still in process of implementing its corrective actions to address prior year recommendation 2021-08 related to the evaluation of deviations from established baseline configuration and common secure configurations (Question 19).

[6] The FY 2023 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 core metrics do not allow the agency to ensure its assets are consistently configured to reduce the risk of new vulnerabilities introduced to its environment.

Additionally, Williams Adley identified a drop in the maturity rating for metric question 22 due to a change in applicable maturity descriptions for Level 3 since FY 2021. FISMA requirements were updated for FY 2023 to require agencies to migrate from the TIC 2.0 program and adopt the TIC 3.0 program. As of the date of this report, the STB is still in the process of migrating to the TIC 3.0 program.

Lastly, since the FY 2021 FISMA audit, the STB has integrated its VDP into its existing vulnerability management and flaw remediation activities (Question 24). Williams Adley determined, in question 21, that the STB's vulnerability management and flaw remediation activities are consistently implemented.

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 2.33 and a maturity rating of Level 2 (Defined).

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 2022 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 4	Level 3
31	Use of strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for privileged users.	Level 4	Level 3
32	Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties.	Level 3	Level 3

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

Williams Adley determined that privileged and non-privileged users use PIV cards to authenticate against STB's systems[7] (Questions 30 and 31). Additionally, Williams Adley found that privileged users use PIV authentication to make changes to Doman Name Services (DNS) records[8].

Lastly, we determined that the STB continues to implement its access management activities for its privileged users and limits their actions (Question 32).

[7] The use of PIV system is designed to meet the control and security objectives of Homeland Security Presidential Directive-12 which require initial identity proofing, infrastructure to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

[8] In response to attackers redirecting and intercepting web and mail traffic, the DHS issued Emergency Directive 19-01 to require agency to implement Multi-Factor Authentication to DNS Accounts. This requirement is reflected in the Level 4 maturity description for Question 31.

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 3.7 and a maturity rating of Level 4 (Managed and Measurable).

Identity and Access Management – Supplemental Reporting Metrics

The OMB identified four (4) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 11***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
26	Roles and responsibilities of identity, credential, and access management (ICAM) stakeholders.	Level 3	Level 2
27	Comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities.	Level 3	Level 2
29	Access agreements for individuals (both privileged and nonprivileged users) that access its systems are completed and maintained.	Level 3	Level 2
33	Configuration and connection requirements are maintained for remote access connections.	Level 3	Level 2

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

Williams Adley determined that the STB made the following improvements since the FY 2021 reporting period:

- Key stakeholders are performing the roles and responsibilities defined within its ICAM policy, procedure, and strategy document (Question 26).
- The STB implemented its ICAM policy, strategy, and processes within its environment. Additionally, the STB is making progress on its road map to achieve Federal ICAM requirements (Question 27).
- The STB ensures that access agreements for individuals are completed prior to obtaining access to agency systems (Question 29).
- FIPS 140-2 validated cryptographic modules were implemented for remote access connections, remote access sessions were configured to time out after 30 minutes (or less), and remote users' activities are logged and reviewed based on risk (Question 33).

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 3 and a maturity rating of Level 3 (Consistently Implemented).

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 2022 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 2	Level 2
37	Use of security controls to prevent data exfiltration and enhance network defenses.	Level 3	Level 3

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

Per discussion with STB management, the agency is still in process of implementing its corrective actions to address prior year recommendation 2021-15 and is related to the implementation of data protection policies and procedures for Data at Rest, prevention and detection of untrusted removable media, and destruction or reuse of media containing PII or other sensitive agency data (Question 36).

Additionally, Williams Adley determined that the STB has implemented security controls to prevent data exfiltration including but not limited to monitoring inbound and outbound traffic and reviewing traffic of exfiltration of data (Question 37).

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 2.5 and a maturity rating of Level 2 (Defined).

Data Protection and Privacy – Supplemental Reporting Metrics

The OMB identified one (1) supplemental reporting metric for evaluation in FY 2023, as outlined in ***Table 13***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
35	Privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems.	Level 3	Level 2

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

Williams Adley determined that STB has consistently implemented its privacy program, including but not limited to the following activities (Question 35):

- Maintaining an inventory of the collection and use of PII
- Conducting and maintaining privacy impact assessments and system of records notices for all applicable systems
- Reviewing and removing unnecessary PII collections on a regular basis (i.e., SSNs)

Based on the audit procedures performed and the score outlined in ***Table 13*** above, Williams Adley determined that the Data Protection and Privacy supplemental metric has a calculated average score of 3 and a maturity rating of Level 3 (Consistently Implemented).

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 2022 Maturity Rating
42	Use of assessments of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training.	Level 3	Level 3

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

Williams Adley determined that the STB has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Additionally, the STB is in the process of addressing its identified gaps through training or talent acquisition (Question 42).

Based on the audit procedures performed and the scores outlined in ***Table 14*** above, Williams Adley determined that the Security Training core metric has a calculated average score of 3 and a maturity rating of Level 3 (Consistently Implemented).

Security Training – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 15***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
41	Roles and responsibilities of security awareness and training stakeholders.	Level 3	Level 2
43	Use of security awareness and training strategy/plan.	Level 3	Level 2

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

Williams Adley determined that Security Training stakeholders are performing their defined roles and responsibilities (Question 41) and the STB has consistently implemented its organization-wide security awareness and training strategy and plan (Question 43).

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 average score of 3 and a maturity rating of Level 3 (Consistently Implemented).

III. Detect

The Detect function is supported by the Information Security Continuous Monitoring (ISCM) domain.

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 2022 Maturity Rating
47	Use of ISCM policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier.	Level 3	Level 2
49	Performance of ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls.	Level 2	Level 2

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

Williams Adley determined that the STB has implemented the activities associated with its ISCM policies and strategy at all organizational tiers. Additionally, the STB consistently captures lessons learned to make improvements to its ISCM policies and strategy (Question 47).

Lastly, per discussion with STB management, the agency is still in process of implementing its corrective actions to address prior year recommendation 2021-17 related to the transition from the traditional three (3) year authorizations to ongoing authorizations for STB GSS (Question 49).

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 2.5 and a maturity rating of Level 2 (Defined).

ISCM – Supplemental Reporting Metrics

The OMB identified one (1) supplemental reporting metric for evaluation in FY 2023, as outlined in ***Table 17***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
48	Roles and responsibilities of ISCM stakeholders.	Level 2	Level 2

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

Per discussion with STB management, the agency is still in process of implementing its corrective actions to address prior year recommendation 2021-17 related to the transition from the traditional three (3) year authorizations to ongoing authorizations for STB GSS (Question 48).

Based on the audit procedures performed and the score outlined in ***Table 17*** above, Williams Adley determined that the ISCM supplemental metric has a calculated average score of 2 and a maturity rating of Level 2 (Defined).

IV. Respond

The Respond function is supported by the Incident Response domain.

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 2022 Maturity Rating
54	Processes for incident detection and analysis.	Level 3	Level 3
55	Processes for incident handling.	Level 3	Level 3

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

Williams Adley determined that the STB continued to consistently perform the activities associated with its incident response process, from initial detection through resolution (Question 54 and 55).

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 3 and a maturity rating of Level 3 (Consistently Implemented).

Incident Response – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 19***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
57	Collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities.	Level 4	Level 3
58	Use of technology to support its incident response program.	Level 3	Level 1

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

Williams Adley determined that the STB has obtained Einstein 3 Accelerated capabilities to detect and proactively block cyberattacks or prevent potential compromises through its contract with DHS' CDM shared services contract (Question 57).

Additionally, we determined that the STB implemented the following incident response technologies to support its incident response program (Question 58):

- Web application protections
- Event and incident management
- Security information and event management (SIEM)
- Malware detection
- Data loss prevention

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 3.5 and a maturity rating of Level 3 (Consistently Implemented).

V. Recover

The Recover function is supported by the Contingency Planning domain.

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 2022 Maturity Rating
61	Business impact analyses (BIA) are used to guide contingency planning efforts.	Level 3	Level 3
63	Performance of information system contingency plan (ISCP) tests/exercises.	Level 3	Level 2

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

Williams Adley determined that the STB performed BIAs to support its information system contingency planning processes (Question 61). Additionally, the STB performed its annual tabletop exercise for its General Support System (GSS)'s ISCP (Question 63).

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 3 and a maturity rating of Level 3 (Consistently Implemented).

Contingency Planning – Supplemental Reporting Metrics

The OMB identified two (2) supplemental reporting metrics for evaluation in FY 2023, as outlined in ***Table 21***:

Metric Question	Topic	FY 2023 Maturity Rating	FY 2021 Maturity Rating
60	Roles and responsibilities of Contingency Planning stakeholders.	Level 3	Level 2
65	Planning and performance of recovery activities is consistently communicated to relevant stakeholders.	Level 3	Level 2

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

Williams Adley determined that Contingency Planning stakeholders are consistently performing their roles and responsibilities (Question 60). Additionally, information on the planning and performance of recovery activities is communicated to stakeholders via routine meetings with senior leadership (Question 65)

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 3 and a maturity rating of Level 3 (Consistently Implemented).

Conclusion

Williams Adley concludes that the STB has continued to make noted improvements towards implementing the elements of an effective information security program by addressing historically issued recommendations. However, outstanding recommendations covering the implementation of defined activities and gaps in the content of its governing documents, prevent the STB from having an effective information security program.

Recommendations

Williams Adley did not identify any new conditions related to the core metrics identified within the FY 2023 FISMA reporting metrics. As a result, Williams Adley will not issue any new recommendations for the FY 2023 reporting period but would like to bring to STB management's attention the open recommendations which impact the identified core metrics in ***Table 22*** below.

Function	Domain	CyberScope Question	Associated Open Recommendation
Identify	Supply Chain Risk Management	14	2021-05
Protect	Configuration Management	20	2021-08
Protect	Configuration Management	21	2021-08
Protect	Data Protection and Privacy	36	2021-15
Detect	ISCM	47	2021-17
Detect	ISCM	49	2021-17

Table 22 – Outstanding Recommendations Impacting Core FISMA Metrics

Appendix A – Objective, Scope, and Methodology

Objective

Williams Adley's main objective was to determine the effectiveness of Surface Transportation Board (STB)'s information security program and practices. We reviewed a group of Federal Information Security Modernization Act of 2014 (FISMA) security metrics and performance measures selected by Office of Management and Budget (OMB) and submit the results of our assessment through CyberScope to OMB, as required. Williams Adley's secondary objective was to evaluate the remediation efforts taken to address previously issued conditions and recommendations.

Scope

As required by FISMA, Williams Adley selected a representative subset of STB's systems to evaluate the Agency's information security program. For the FY 2023 FISMA audit, Williams Adley selected three (3) systems:

- STB General Support System (GSS)[9]
- Dynamic Case Management System (DCMS)[10]
- EconSys Federal HR Navigator[11]

Methodology

Williams Adley conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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.

Williams Adley interviewed STB management to determine the effectiveness of STB's information security program and practices across five function areas—Identify, Protect, Detect, Respond, and Recover.

In addition to interviews, we also observed operations remotely via screen sharing technology, conducted sampling where applicable, inspected STB policies and procedures, and obtained sufficient evidence to support the conclusions presented in this report.

[9] The STB-GSS is identified as a High Value Asset (HVA) and maintains personally identifiable information (PII). Furthermore, it is the only system hosted and maintained by the STB.

[10] DCMS is identified as a HVA and maintains PII.

[11] EconSys Federal HR Navigator is the "newest" system in STB's environment and was not tested in the past. Furthermore, EconSys Federal HR Navigator maintains PII.

Appendix B – Status of Prior Year Federal Information Security Modernization Act of 2014 (FISMA) Recommendations

#	Description	Status	Target Action Date
2021-01[12]	Develop an enterprise architecture that includes information security considerations and the resulting risk to the Agency, as well as incorporates Surface Transportation Board (STB)'s existing cyber security architecture.	Open	March 31, 2024
2021-05	Develop a Supply Chain Risk Management (SCRM) strategy and supporting policies and procedures 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.	Open	September 30, 2023
2021-08	Evaluate deviations from Center of Internet Security (CIS) benchmarks and determine if the associated configurations should align with best practices or if deviations should be risk accepted.	Open	September 30, 2023
2021-15	Implement data protection policies and procedures for Data at Rest, prevention and detection of untrusted removable media, and destruction or reuse of media containing PII or other sensitive agency data.	Open	March 31, 2024
2021-17	Complete the transition from traditional three (3) year authorizations to ongoing authorizations for STB-LAN.	Open	September 30, 2025
2021-18	Implement documented processes for collecting and reporting performance metrics at the organization and system level to assess the effectiveness of information security continuous monitoring (ISCM) program.	Closed	N/A
2021-19	Develop a process to make improvements to the effectiveness of its ISCM program through the collection and reporting of quantitative and qualitative performance metrics, and lessons learned.	Closed	N/A
2021-27	Conduct a tabletop exercise of the General Support System's information system contingency plan (ISCP) on an annual basis.	Closed	N/A

[12] Prior Year Recommendation is related to a FY 2024 supplemental metric and has no impact on the calculation of maturity ratings for the FY 2023 FISMA audit.

Appendix C – Management's Response

SURFACE TRANSPORTATION BOARD
Washington, DC 20423

June 29, 2023

VIA E-mail:kevin.dorsey@oig.dot.gov
Mr. Kevin Dorsey
Assistant IG for IT Audits
DOT Office of Inspector General
Headquarters
1200 New Jersey Ave., SE
W72-302
Washington, DC 20590

Re: Fiscal Year 2023 FISMA Audit of the Surface Transportation Board

Dear Mr. Dorsey:

Thank you for the opportunity to provide comments in response to the Department of Transportation Office of the Inspector General (DOT-OIG) Fiscal Year (FY) 2023 draft report for the Federal Information Security Modernization Act (FISMA) audit conducted at the Surface Transportation Board (STB or Board). The STB welcomes this audit report and is pleased that the Board's overall information security program continues to improve, year over year. This improvement reflects the STB's commitment to implementing a cost-effective, risk-based security program that is aligned with the National Institute of Standards and Technology (NIST) security standards and guidelines. The STB appreciates that this year's audit recognizes the work that has been done through FY 2023 while identifying information security areas where the STB can continue its improvements.

The STB concurs with no new recommendations for FY 2023. The STB also acknowledges the closure of three (3) FY 2021 recommendations during the FY 2023 assessment. The STB is committed to addressing the remaining FY 2021 recommendations and continuing to improve its information security posture. Please see the STB response to each FISMA domain and the established estimated completion dates for the work on the remaining FY 2021 audit recommendations below.

Previous year recommendations

STB Response to the FISMA Risk Management Domain

The STB has taken steps to improve its approach to Risk Management by developing processes that facilitate and communicate risk at all levels of the organization. Additionally, the STB has implemented Risk Management capability by leveraging Continuous Diagnostics and Mitigation shared services which give the agency better visibility and insight into the hardware and software inventories of STB information systems. The STB estimated completion date for the remaining recommendation associated with the Risk Management domain is:

- **Recommendation 2021-1:** March 31, 2024

STB Response to the FISMA Supply Chain Risk Management Domain

The STB will develop a Supply Chain Risk Management strategy as well as establish policies, processes, and procedures to address controls associated to the newly introduced Supply Chain Risk Management domain. The STB estimated completion date for the recommendation associated with the Supply Chain Risk Management domain is:

- **Recommendation 2021-05:** September 30, 2023

STB Response to the FISMA Configuration Management Domain

The STB continues to mature processes related to Configuration Management and has simplified the Configuration Management process that allows the STB to efficiently evaluate and implement proposed configuration changes. The STB estimated completion date for the remaining recommendation associated with the Configuration Management domain is:

- **Recommendation 2021-8:** September 30, 2023

STB Response to the FISMA Data Protection and Privacy Domain

The STB has continued to modify its policies, plans, and procedures that establish processes related to the collection, usage, maintenance, and sharing of personally identifiable information. The newly established privacy processes include the development of privacy threshold and impact metrics that identify privacy information being processed or stored within information systems. These activities help strengthen the STB privacy program and its ability to protect personally identifiable information. The estimated completion date for the remaining recommendation associated with the Data Protection and Privacy domain is:

- **Recommendation 2021-15:** March 31, 2024

STB Response to the FISMA Information Security Continuous Monitoring Domain

The STB has modified its Continuous Monitoring processes to align with NIST Special Publication 800-137 and other federal guidance, establishing a consistent, compliant approach to the STB Continuous Monitoring program. Additionally, the STB has incorporated processes to ensure the timely collection of established metrics across all operational systems and has established paths for those metrics to get communicated to agency leadership which allow the STB to make more informed data-driven decisions. The estimated completion date for the remaining recommendation associated with the Information Security Continuous Monitoring domain is:

- **Recommendation 2021-17:** September 30, 2025

Thank you again for the opportunity to provide comments regarding the most recent FISMA audit assessment. If you have any questions, please do not hesitate to contact me at 202-245-0357.

Sincerely,

RACHEL
CAMPBELL

Digitally signed by RACHEL CAMPBELL
Date: 2023.06.29 15:42:02 -04'00'

Rachel D. Campbell
Managing Director

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety Hotline

https://www.oig.dot.gov/hotline
hotline@oig.dot.gov
(800) 424-9071

OUR MISSION

OIG enhances DOT's programs and operations by conducting objective investigations and audits on behalf of the American public.

OFFICE OF INSPECTOR GENERAL • U.S. DEPARTMENT OF TRANSPORTATION

1200 New Jersey Ave SE
Washington, DC 20590
www.oig.dot.gov