



U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

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

Report No. QC2020049

September 28, 2020



Quality Control Review of the 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

QC2020049 | September 28, 2020

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 2020 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.

Recommendations

STB concurs with Williams Adley's six recommendations.



U.S. Department of
Transportation

Office of Inspector General
Washington, DC

September 28, 2020

The Honorable Ann D. Begeman
Chairman, Surface Transportation Board
395 E Street, SW
Washington, DC 20423-0001

Dear Ms. Begeman:

I respectfully submit our 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 2014¹ (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 2020 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.

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. Williams Adley made the following six recommendations to improve STB's information security program and practices.

1. Implement documented processes for granting and removing user access in a consistent manner, as required by STB policies and procedures.
2. Implement processes for conducting, documenting, and maintaining Position Risk Designations in a consistent manner, as required by STB policies and procedures.

¹ Pub. L. No. 113-283.

3. Develop a process for ensuring that the completion of role-based training is tracked and maintained.
4. Consistently implement the process to ensure all new users complete the mandatory security awareness training requirements prior to being granted access to STB systems.
5. Fully develop the Information Security Continuous Monitoring (ISCM) Strategy and all information system ISCM plans to include the required criteria documented in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 such as:
 - a. Considerations at the organization/business process level;
 - b. Considerations at the information system level; and
 - c. Processes to review and update the ISCM program and strategy.
6. Define the process to ensure the timely collection of established metrics across its operational systems and reporting evaluation process to assist ISCM Stakeholders to make informed decisions.

We appreciate the cooperation and assistance of STB representatives. If you have any questions about this report, please call me at (202) 366-1518.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin Dorsey".

Kevin Dorsey
Assistant Inspector General for
Information Technology Audits

cc: STB Audit Liaison

Attachment

Quality Control Review

We performed a quality control review (QCR) of Williams Adley's report, dated August 28, 2020 (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 July 30, 2020, Williams Adley provided STB with its draft report and received STB's response on August 14, 2020. STB sent us an updated response on September 17, 2020, which is included in its entirety in the attached independent auditor's report.

STB concurred with all six of Williams Adley's recommendations, and provided appropriate actions and completion dates.

Actions Required

We consider all six of Williams Adley's recommendations resolved but open pending completions of planned actions.

Exhibit. List of Acronyms

FISMA	Federal Information Security Modernization Act
ISCM	Information Security Continuous Monitoring
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
QCR	Quality Control Review
STB	Surface Transportation Board

Attachment. Independent Auditor's Report

**Fiscal Year 2020 Federal Information Security Modernization Act of 2014 Audit of the
Surface Transportation Board's Information Security Program and Practices**

August 28, 2020



Contents

Results in Brief 2

Background 2

Results of the FY 2020 FISMA Audit 4

I. Identify 4

II. Protect 5

III. Detect 7

IV. Respond 8

V. Recover 8

Conclusion 9

Recommendations 9

Appendix A – Scope and Methodology 10

Appendix B – Status of Prior Year FISMA Recommendations 11

Appendix C – Criteria and Guidance 14

Appendix D – Management’s Response 18



August 28, 2020

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

Dear Mr. Dorsey:

Williams, Adley & Company-DC, LLP (Williams Adley) was tasked by the Department of Transportation (DOT), Office of Inspector General (OIG), to conduct a performance audit of STB's information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), which requires agencies to perform an annual independent evaluation of its information security program and practices to determine its effectiveness and report the results of the audit to the Office of Management and Budget (OMB). This report presents the results of the fiscal year (FY) 2020 FISMA audit of the Surface Transportation Board (STB)'s information security program and practices.

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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our 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. As required by FISMA, Williams Adley reviewed a representative subset of STB's systems and will report on the results of FISMA security metrics and performance measures through CyberScope, as required by OMB, for the period October 1, 2019 to May 31, 2020. To address OMB's 2020 FISMA reporting metrics, Williams Adley interviewed STB officials, and analyzed data pertaining to STB's information security program and practices.

Sincerely,

A handwritten signature in black ink, appearing to read 'K. Isiaq'.

Kola A. Isiaq, CPA, CISA
Managing Partner

Results in Brief

OMB requires independent auditors to annually assess metrics across five (5) security function areas to determine the maturity level of STB's information security program. Program maturity was assessed at one (1) of five (5) levels as defined by OMB - Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized. Appendix A within this report outlines the audit scope and methodology followed to perform the FY 2020 audit.

Based on the audit procedures performed, we concluded that STB's information security program remains ineffective.¹ Although STB's information security program was deemed ineffective for FY 2020, STB made progress in maturing its overall information security program by addressing six (6) prior year recommendations² and improving the maturity level of the Recover FISMA function, as outlined in the table below.

FISMA Function	Rating in FY 2018	Rating in FY 2019	Rating in FY 2020
Identify	Level 1 – Ad-Hoc	Level 2 – Defined	Level 2 – Defined
Protect	Level 1 – Ad-Hoc	Level 2 – Defined	Level 2 – Defined
Detect	Level 1 – Ad-Hoc	Level 1 – Ad-Hoc	Level 1 – Ad-Hoc
Respond	Level 1 – Ad-Hoc	Level 2 – Defined	Level 2 – Defined
Recover	Level 1 – Ad-Hoc	Level 1 – Ad-Hoc	Level 2 – Defined

Table 1 - FY 2020 IG FISMA Reporting Metric Ratings

Based on the results of the FY 2020 audit procedures, Williams Adley determined that two (2) previously issued recommendations remain open. Furthermore, Williams Adley issued six (6) new recommendations to support STB's efforts to define and implement its information security program and processes. To supplement the content within this report, an overview of the criteria and guidance supporting the FY 2020 audit are outlined in Appendix C and management's response to the results of the FY 2020 audit are outlined in Appendix D.

Background

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 DOT. While part of DOT, STB shared an information security program with DOT and its Operating Administrations.

As a stand-alone Agency, STB is responsible for maintaining its own information security program and independently meeting FISMA's requirements. Under FISMA, each Federal agency must protect the information and information systems that support its operations, including those provided or managed by other agencies, entities, or contractors. Furthermore, FISMA requires each agency to report annually to OMB, Congress, and the Government Accountability Office (GAO) on the effectiveness of its information security policies, procedures, and practices.

¹ An information security program rated at a level 4, Managed and Measurable, is considered to be effective.

² The status of previously issued recommendations are found in Appendix B.

The FISMA metrics are organized around the five security functions—Identify, Protect, Detect, Respond, and Recover— as outlined in National Institute of Standards and Technology (NIST)’s cybersecurity framework. For FY 2020, OMB and Department of Homeland Security (DHS), in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and the Federal Chief Information Officer Council (FCIOC), revised the metrics to include additional focus areas to support federal agencies information security program:

- to assess agency’s progress in securing mobile endpoints and employing secure application development processes;
- to assess agency’s progress in planning for the effective implementation of the security capabilities outlined in M-19-26 and the Trusted Internet Connection (TIC) initiative.

OMB provides guidance to inspectors general and independent auditors for determining the maturity of their agencies’ security programs. In this guidance, OMB defines the five maturity levels to help inspectors general and auditors categorize the maturity of their agencies’ function areas and determine the effectiveness of their security programs. According to OMB, an effective program’s maturity is at the managed and measurable level; see table 2 for a definition of each maturity level.

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 Measureable	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 2 - FY 2020 IG Evaluation Maturity Levels, Source: DHS

Results of the FY 2020 FISMA Audit³

I. Identify

The Identify function, supported by the risk management domain, was rated at a Level 2 maturity (defined).

Risk Management

STB has taken steps towards improving its Risk Management program, such as developing a Risk Management Plan, Cybersecurity Architecture, and Security Assessment and Authorization process. Furthermore, in FY 2020, STB developed its system inventory process, which documents the minimum hardware and software taxonomy requirements for tracking. However, Williams Adley identified the following repeat issues within the risk management IG FISMA metric domain:

- STB did not develop an information security risk management strategy at all three levels of organization, in accordance with NIST Special Publication (SP) 800-39.
- STB did not use a standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting, in accordance with STB's Configuration Management Policy.
- STB did not use a standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting, in accordance with STB's Configuration Management Policy.

According to STB management, the Agency believed it had completed all work needed to address the Risk Management recommendation. However, all elements of the recommendation were not implemented by STB due to a misinterpretation of the NIST federal guidance. As a result, the STB has not completed the implementation of security controls associated with Risk Management and the current policies and procedures do not meet all FISMA requirements.

Without effectively implementing a comprehensive risk management process at all three levels of the organization, the STB may be unable to address the root causes associated with existing information security risks. In addition, appropriate resources may not be effectively assigned to make the correct risk decisions to ensure the results align with STB's business priorities.

Williams Adley will not issue a new recommendation within the risk management domain as Recommendation 2018-1 addresses the issues noted.

³ The criteria used to support the conditions found within the FY 2020 audit are found in Appendix C – Criteria and Guidance.

II. Protect

The Protect function, supported by the configuration management, identity and access management, security training, and data protection and privacy domains, was rated at a Level 2 maturity (defined). This rating was determined based on the mode of the metric questions across the four (4) aforementioned domains. Table 3 below summarizes the mode of ratings within each domain.

FISMA Domain	Rating in FY 2020
Configuration Management	Level 2 – Defined
Identity and Access Management	Level 2 – Defined
Security Training	Level 1 – Ad-Hoc
Data Protection and Privacy	Level 1 – Ad-Hoc

Table 3 – Ratings for Domains within the Protect Function

Configuration Management

Williams Adley did not identify any issues related to the plan, policies, and procedures supporting STB’s configuration management program and the STB is currently implementing the processes outlined in these documents. Changes to STB’s configuration management program will be evaluated during the FY 2021 FISMA audit.

Identity and Access Management

STB has taken steps towards improving its identity and access management program, such as developing an Identity, Credential, and Access Management (ICAM) strategy to guide its ICAM process and activities. In addition, STB has modified its existing identity and access management policies and procedures to adequately address (a) processes to request, modify, and revoke privileged and non-privileged access; and (b) processes to ensure separation of duties within the Agency. However, Williams Adley identified the following deficiencies within the Identity & Access Management IG FISMA metric domain:

- STB did not assign end-user access to the STB General Support System (GSS) Local Area Network (LAN) in a consistent manner. Specifically, of eight (8) sampled STB user access request forms:
 - Two (2) users access request forms were not appropriately completed and were missing the requestor signature;
 - Two (2) users access request forms were not appropriately approved by the System Owner; and
 - One (1) user account request form was requested and signed by the same individual.
- STB did not properly remove user access for three (3) terminated users in accordance with STB policies. Specifically, of ten (10) sampled users, three (3) user accounts were modified after the time of employment termination date.

- STB did not ensure that all its personnel, with access to STB systems, were properly screened or rescreened prior to granting them access to STB resources. Specifically:
 - Four (4) users did not complete the Personnel Security Action Request Form.
 - Four (4) Personnel Security Action Request Forms were not signed or approved.
 - Three (3) users did not receive email confirmation from the security office.

STB's identity and access management policies and procedures were recently modified to address previously identified issues. As a result, STB personnel did not execute the processes outlined within the updated policies and procedures in a consistent manner. In addition, STB did not maintain sufficient documentation to ensure that all STB personnel with access to STB systems were properly screened or rescreened prior to being granted access to STB resources, as required by NIST SP 800-53.

Without an effective identity and access management program, the risk of unauthorized access to STB's information systems is significantly increased. Furthermore, unauthorized access could potentially result in the submission of false transactions, improper access, dissemination of confidential data, and other malicious activities.

Williams Adley issued two (2) new recommendations in FY 2020 (Recommendation 2020-1 and 2020-2) to address the issues noted.

Security Training

STB has taken steps towards improving its security training program, such as implementing procedures to conduct annual awareness training. In addition, STB developed policies for required specialized trainings. However, Williams Adley identified the following deficiencies within the Security Training IG FISMA metric domain:

- STB has not developed a process to verify whether users with significant security responsibilities completed required specialized trainings.
- STB did not ensure that users completed required security awareness training prior to accessing their STB user accounts. Specifically of eight (8) sampled users, two (2) user accounts were accessed prior to taking the required training.

The STB does not have a defined and adequate process to verify that its users (employees and contractors) completed the required role-based training and does not have a reliable process to provide evidence that the training requirements have been fulfilled. Furthermore, STB confirmed that STB does not require users to provide specialized training completion certificates for tracking. Lastly, STB's policy does not follow Federal guidelines for issuing security training prior to a user being granted access to STB systems.

Without identifying significant security responsibilities (SSRs) within the agency and providing individuals assigned these responsibilities with appropriate role-based training, these users may not possess the adequate knowledge and skills necessary to perform their job responsibilities. Furthermore, ensuring that users assigned SSRs complete role-based training enhances an organization's security posture through a trained workforce and it increases the individual's

readiness to respond to security incidents. If all personnel with access to STB's systems are not appropriately trained, they could compromise the security of the network.

Williams Adley issued two (2) new recommendations in FY 2020 (Recommendation 2020-3 and 2020-4) to address the issues noted.

Data Protection and Privacy

STB has taken steps towards improving its privacy program, including conducting Privacy Impact Assessments (PIAs) for the information systems within STB's environment. However, Williams Adley identified the following repeat deficiencies within the Data Protection and Privacy IG FISMA metric domain:

- STB has not developed a Data Breach Response plan.
- STB has not developed policies, procedures, roles and responsibilities, for determining the personnel responsible for performing data exfiltration exercises.

In addition, Williams Adley identified two (2) new deficiencies as a part of the FY 2020 FISMA audit:

- STB has not finalized its procedures supporting its Privacy Impact Assessments (PIA) and Privacy Threshold Analysis (PTA).
- STB's General Support System's Information Security Continuous Monitoring (ISCM) Strategy is missing Personal Identifiable Information (PII) monitoring procedures.

STB management stated the resolution of this recommendation is not planned to be completed until after the conclusion of the assessment period of the FY 2020 FISMA Audit. As a result, the STB has not completed its work to implement security controls associated with Data Protection and Privacy.

Without an established policy that defines PII and is signed and authorized prior to distribution, STB's data and information systems are vulnerable to compromise.

Williams Adley will not issue a new recommendation within the data protection and privacy domain as Recommendation 2018-5 addresses the issues noted including the FY 2020 deficiencies.

III. Detect

The Detect function, supported by the ISCM domain, was rated at a Level 1 maturity (ad hoc).

Information Security Continuous Monitoring

STB has taken steps towards improving its ISCM program such as updating its overall Continuous Monitoring Plan to include awareness of threats and vulnerabilities. In addition, STB has documented system specific ISCM plans for all information systems in STB's environment. However, Williams Adley identified the following deficiencies within the ISCM IG FISMA

metric domain:

- STB's ISCM procedures do not define how the ISCM program will be monitored and account for changes in organizational missions and objectives, operational environments, and threats.
- STB's ISCM policy and procedures do not define the process to provide individuals with significant security responsibilities and/or key stakeholders with the information necessary to make informed improvements to its ISCM program.

According to STB management, the development of its ISCM policies and procedures is reliant on the implementation and support of DHS' Continuous Diagnostic and Monitoring (CDM) program. Due to the delays encountered with CDM's shared services program for micro agencies, STB's ISCM program cannot be fully defined.

Without fully developing and implementing an ISCM program, STB is unable to prioritize its organizational goals and objectives and, as a result, cannot fully and effectively execute its overall organization-wide information security program. In addition, without a fully developed and implemented organization-wide continuous monitoring strategy, STB cannot provide stakeholders—including senior officials, business owners, and information system owners—with a unified understanding of the performance of its information security program. This prevents STB from consistently monitoring its dynamic network environment to changing threats, vulnerabilities, technologies, missions, and business functions.

Williams Adley issued two (2) new recommendations in FY 2020 (Recommendation 2020-5 and 2020-6) to addresses the issues noted.

IV. Respond

The Respond function, supported by the incident response domain, was rated at a Level 2 maturity (defined).

Incident Response

Williams Adley did not identify any issues related to the plan, policies, and procedures supporting STB's incident response program and the STB is currently implementing the processes outlined in these documents. Changes to STB's incident response program will be evaluated during the FY 2021 FISMA audit.

V. Recover

The Recover function, supported by the contingency planning domain, was rated at a Level 2 maturity (defined).

Contingency Planning

Williams Adley did not identify any issues related to the plan, policies, and procedures supporting STB's contingency planning program and the STB is currently implementing the processes outlined in these documents. Changes to STB's contingency planning program will be evaluated during the FY 2021 FISMA audit.

Conclusion

STB made improvements towards defining, developing, and implementing the foundation of its information security program; specifically, within the Risk Management, Identity and Access Management, Security Training, Data Protection and Privacy, and ISCM metric domains. However, activities within the ISCM domain were not formalized during the audit period and continue to be performed in an ad-hoc, reactive manner.

Recommendations

To assist STB in addressing the challenges in developing a mature and effective information security program, we recommend that STB continue to address previously identified recommendations and incorporate the following items into their overall information security program:

- **Recommendation 2020-01.** Implement documented processes for granting and removing user access in a consistent manner, as required by STB policies and procedures.
- **Recommendation 2020-02.** Implement processes for conducting, documenting, and maintaining Position Risk Designations in a consistent manner, as required by STB policies and procedures.
- **Recommendation 2020-03.** Develop a process for ensuring that the completion of role-based training is tracked and maintained.
- **Recommendation 2020-04.** Consistently implement the process to ensure all new users complete the mandatory security awareness training requirements prior to being granted access to STB systems.
- **Recommendation 2020-05.** Fully develop the ISCM Strategy and all information system ISCM plans to include the required criteria documented in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 such as:
 - Considerations at the organization/business process level;
 - Considerations at the information system level; and
 - Processes to review and update the ISCM program and strategy.
- **Recommendation 2020-06.** Define the process to ensure the timely collection of established metrics across its operational systems and reporting evaluation process to assist ISCM Stakeholders to make informed decisions.

Appendix A – Scope and Methodology

Department of Transportation Office of Inspector General tasked Williams Adley with conducting a performance audit of Surface Transportation Board (STB)'s information security programs and practices in accordance with Federal Information Security Modernization Act of 2014 for the period October 1, 2019 to May 31, 2020. 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 objectives.

Our 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. As required by FISMA, we selected a representative subset of STB's systems to review. For the FY 2020 audit, we selected STB General Support System, ServiceNow and Okta as our in-scope systems.

To perform this audit, Williams Adley interviewed STB management to determine the effectiveness of STB's information security program and practices in 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 and recommendations presented in this report.

Appendix B – Status of Prior Year FISMA Recommendations⁴

#	Description of Recommendation	Status
2017-1	Complete implementation of policies and procedures for: <ol style="list-style-type: none"> a. Risk management, including a risk management plan and assessment; b. System authorization; and c. Plans of actions and milestones. 	Closed in FY 2019.
2017-2	Complete the system reauthorization of the STB LAN	Closed in FY 2018.
2017-3	Complete service level agreements or similar documents that permit STB or its auditor to perform tests and/or obtain supporting documentation to demonstrate that cloud systems are properly authorized to operate.	Closed in FY 2018.
2017-4	Define specifications and acquire an automated solution to assist with the risk management program.	Closed in FY 2019.
2017-5	Develop policies and procedures for the implementation of an information security architecture.	Closed in FY 2019.
2017-6	Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.	Closed in FY 2019.
2017-7	Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.	Closed in FY 2018.
2017-8	The STB is modifying its identity and access management policies and procedures to address: <ol style="list-style-type: none"> a. Reviews of as-is states, desired states and a transition plan; b. Processes for assigning personnel risk designations prior to granting access to its systems; c. Processes for developing, documenting, and maintaining access agreements for individuals with system access; and d. Requirements for remote access. 	Closed in FY 2019.

⁴ Recommendations outlined and assessed in Appendix B are sourced from OIG report FI2018002 (FISMA 2017: The Surface Transportation Board's Information Security Program Is Not Effective) dated October 26, 2017; OIG report QC2019001 (FISMA 2018: Quality Control Review of an Independent Auditor's Report on the Surface Transportation Board's Information Security Program and Practices) dated October 24, 2018; and OIG Report QC2019082 (FISMA 2019: Quality Control Review of an Independent Auditor's Report on the Surface Transportation Board's Information Security Program and Practices) dated September 25, 2019.

2017-9	Conduct a needs assessment to formally determine the organization’s awareness and training needs, including but not limited to developing and implementing a formal process for assessing the skills, knowledge, and abilities of its workforce.	Closed in FY 2020.
2017-10	Develop and implement a formal process for measuring the effectiveness of its security awareness and training program.	Closed in FY 2020.
2017-11	Modify the training plan to include missing elements such as funding, goals and use of technology.	Closed in FY 2020.
2017-12	Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.	Closed in FY 2020.
2017-13	Modify its policies and procedures to address missing components such as incident detection and analysis; incident prioritization, containment, eradication, and recovery; coordination, information sharing, and reporting; incident response training and testing, and considerations for major incidents.	Closed in FY 2019.
2017-14	Implement its contingency planning policy by performing business impact analyses, updating or completing system contingency plans, testing contingency plans, performing necessary backups and obtaining an adequate alternate processing site, if needed.	Closed in FY 2020.
2018-1	Fully develop a risk management strategy and the supporting procedures for maintaining an accurate system inventory.	Open.
2018-2	Develop a configuration management plan with supporting policies and procedures and ensure that the existing Change Management Charter aligns with the plan.	Closed in FY 2019.
2018-3	Develop an ICAM strategy to guide its ICAM process and activities, and modify existing policies and procedures to adequately address: <ul style="list-style-type: none"> a. Processes to request, modify, and revoke privileged and non-privileged access; and b. Processes to ensure separation of duties within the organization. 	Closed in FY 2020
2018-4	Full implement the use of PIV card for personnel to access STB’s facilities.	Closed in FY 2019.
2018-5	Develop a privacy program, including related plans, policies and procedures, for	Open.

	the protection of personally identifiable information that is collected, used, maintained, shared and disposed of by STB's information systems. Furthermore, identify roles and responsibilities for data exfiltration exercises.	
2018-6	Develop an Incident Response plan in accordance with NIST SP 800-61, rev. 2.	Closed in FY 2019.
2018-7	Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.	Closed in FY 2019.

Appendix C – Criteria and Guidance

Williams Adley utilized the following criteria to support the conditions identified during the FY 2020 audit of Surface Transportation Board’s information security program:

I. Risk Management

Williams Adley utilized the following criteria to identify the conditions within STB’s entity-wide risk management program as outlined within the “Results of the FY 2020 FISMA Audit” section of this report:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 states, “an organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating risk across the organization with respect to the organization’s risk tolerance, and approaches for monitoring risk over time.”
- STB’s Configuration Management Policy, control CM-8, Information System Component Inventory, states that the organization:
 - Develops and documents all inventory of information system components that:
 - Accurately reflect the current system;
 - Includes all components within the boundary of the system;
 - Is at the level of granularity deemed necessary for tracking and reporting; and
 - Includes any other pertinent information STB deems necessary to achieve system accountability.
 - Reviews and updates the system inventory whenever there is a change to the system, or at least annually.

II. Configuration Management

Williams Adley did not identify any conditions related to STB’s configuration management program during the FY 2020 FISMA Audit.

III. Identity and Access Management

Williams Adley utilized the following criteria to identify the conditions within STB’s identity and access management program as outlined within the “Results of the FY 2020 FISMA Audit” section of this report:

- STB Account Administration Process dated March 2019
 - “Following notification from either a Human Resources (HR) team member or a Contracting Officer’s Representative (COR), an STB user account request form will be submitted to the System owner for approval. The request will contain any details required for the Systems team to create new accounts for the user.”

- NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal government to meet the requirements of the Federal Information Processing Standard Publication (FIPS) 200, "Minimum Security Requirements for Federal Information Systems." This includes access control, identification and personnel security policy and procedures, and account management, position designation risk, access control policy & procedures (pg. 164), IA-1 Identification and Authentication policy and procedure (pg. 247) and PS-1 Personnel Security Policy and Procedures (pg. 302), Risk Designations PS-2 (pg. 302) and PS-3 (pg. 303).
- STB Access Control Policy, Issuance No. 9-169, Version 2.0, dated December 17, 2018
 - "System, Network Administrators and other Technical Support Staff shall: Access privileges terminated immediately upon notification of employee departure and change in job functions to ensure they no longer require access to the level to which they were previously granted".
- NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal government to meet the requirements of the Federal Information Processing Standard Publication 200, "Minimum Security Requirements for Federal Information Systems." This includes 1) access controls and account management (pg. 164) and 2) Account Management Removal of Temporary Accounts (pg. 166) of NIST 800-53 AC-1 & AC-2.
- STB Personnel Security Policy, Issuance No. 9-178, Version 3.0, dated February 26, 2019
 - The STB shall:
 - Assign a risk designation for all organizational positions (employee and contractor);
 - Establish screening criteria for individuals filling those positions;
 - Review and update position risk designations when recruitment actions are taken or when position descriptions are rewritten;
 - Screen individuals prior to authorizing access to STB information system; and
 - Rescreens individuals in accordance with all applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance and the criteria established for the risk designation of the assigned position.
- NIST SP 800-53, Revision 4, provides guidelines for selecting and specifying security controls for organization and information systems supporting the executive agencies of the Federal government to meet the requirements of the FIPS 200, "Minimum Security Requirements for Federal Information Systems." This includes access control, identification and personnel security policy and procedures, and account management, position designation risk, access control policy & procedures (pg. 164), IA-1 Identification and Authentication policy and procedure (pg.247) and PS-1 Personnel Security Policy and Procedures (pg. 302), Risk Designations PS-2 (pg. 302) and PS-3 (pg. 303).

IV. Security Training

Williams Adley utilized the following criteria to identify the conditions within STB's security training program as outlined within the "Results of the FY 2020 FISMA Audit" section of this report:

- NIST SP 800-53, rev.4, section AT -3, requires organization to provide role-based security to personnel with assigned security roles and responsibilities (pg.195).
- OMB Circular A-130, Appendix I, Management of Federal Information Resources, "ensure that the security and privacy awareness and training programs are consistent with applicable policies, standards, and guidelines issued by OMB, NIST, and OPM".

V. Data Protection and Privacy

Williams Adley utilized the following criteria to identify the conditions within STB's data protection and privacy program as outlined within the "Results of the FY 2020 FISMA Audit" section of this report:

- NIST SP 800-122, states that "organizations should build their response plans for breaches involving PII into their existing incident response plans. The development of response plans for breaches involving PII requires organizations to make many decisions about how to handle breaches involving PII, and the decisions should be used to develop policies and procedures."
- NIST SP 800-53, rev. 4, states that the organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [Assignment: organization-defined interior points within the system (e.g., subsystems, subnetworks)] to detect covert exfiltration of information.
- E-Government Act of 2002 states, "Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form".
- OMB Circular A-130 states that, "the SAOP shall establish and maintain an agency-wide privacy continuous monitoring program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. Agencies shall ensure that a robust privacy continuous monitoring program is in place before agency information systems are eligible for ongoing authorization".

VI. Information Security Continuous Monitoring (ISCM)

Williams Adley utilized the following criteria to identify the conditions within STB’s ISCM program as outlined within the “Results of the FY 2020 FISMA Audit” section of this report:

- NIST SP 800-53, rev. 4, states that the organization “develops a continuous monitoring strategy and implements a continuous monitoring program.”
- NIST SP 800-1372 states, “part of the implementation stage of the continuous monitoring process is effectively organizing and delivery ISCM data to stakeholders in accordance with decision-making requirements.”
- NIST SP 800-137 states, “the criteria for ISCM are defined by the organization’s risk management strategy, including how the organization plans to assess, respond to, and monitor risk, and the oversight required to ensure that the risk management strategy is effective.” Furthermore, “Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance.”
- NIST SP 800-137 states, “the ISCM program itself must be monitored so that it can evolve with changes in organizational missions and objectives, operational environments, and threats.

VII. Incident Response

Williams Adley did not identify any conditions related to STB’s incident response program during the FY 2020 FISMA Audit.

VIII. Contingency Planning

Williams Adley did not identify any conditions related to STB’s contingency planning program during the FY 2020 FISMA Audit.

Appendix D – Management’s Response

SURFACE TRANSPORTATION BOARD Washington, DC 20423



September 17, 2020

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 2020 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) 2020 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 2020 while providing the STB with a roadmap for continued improvements.

The STB concurs with the six new recommendations for FY 2020 and the two remaining open recommendations from FY 2018. The STB is committed to addressing the recommendations and continuing to improve its information security posture. The estimated completion dates for the work on the remaining open FY 2018 audit recommendations and the FY 2020 audit recommendations are discussed below.

STB Response to Remaining FY 2018 Recommendations:

Two recommendations remain open from the FY 2018 audit. The STB has established the following target action dates to complete the work needed to satisfy those FY 2018 recommendations.

Recommendation 2018-1: The STB continues to make improvements within its risk management program including developing a standard taxonomy for maintaining its inventories of hardware assets and software. Based on the further guidance received during the FY 2020 audit, the STB will define its information security risk strategy at all three levels of the organization, in accordance with NIST Special Publication (SP) 800-39. The STB expects to complete work on this recommendation by December 31, 2020.

Recommendation 2018-5: The STB continues to make progress toward developing a comprehensive privacy program, including finalizing a privacy program plan, incorporating privacy requirements into the STB incident response process, establishing privacy impact assessments, and developing policies and procedures associated with privacy. The STB will also develop privacy related processes and procedures, establish roles, and identify personnel responsible for performing data exfiltration exercises within the Board. The STB expects to complete work on this recommendation by December 31, 2020.

STB Response to FY 2020 Recommendations:

The STB is fully committed to addressing the six new recommendations from the FY 2020 audit. The STB has established the following target action dates to complete the work needed to satisfy the FY 2020 recommendations.

Recommendation 2020-1: The STB has taken steps to improve its access management processes by developing new, or modifying existing, access management policies, plans, and procedures. The STB will continue to refine its access management processes to ensure that processes for granting and removing users are implemented consistently, in accordance with established STB policies and procedures. The STB expects to complete work on this recommendation by February 28, 2021.

Recommendation 2020-2: The STB has established processes for conducting, documenting, and maintaining position risk designations. The STB will incorporate additional measures to ensure that those processes are conducted, documented, and maintained consistently. The STB expects to complete work on this recommendation by March 31, 2021.

Recommendation 2020-3: The STB improved its security training and awareness processes by developing procedures to ensure that individuals with elevated system privileges complete additional role-based security training requirements. The STB will establish processes to ensure role-based training is completed, tracked, and maintained. The STB expects to complete work on this recommendation by December 31, 2020.

Recommendation 2020-4: To ensure that new users are aware of security-related topics, the STB has established a security awareness training package for new personnel. The STB will align its existing access management policies and procedures with its security awareness and training requirements to ensure that all new users complete the mandatory security awareness training requirements prior to being granted access to STB systems. The STB expects to complete work on this recommendation by November 30, 2020.

Recommendation 2020-05: The STB has finalized its Information Security Continuous Monitoring (ISCM) plan, which defines the security controls that will be monitored on a recurring basis. The STB will establish processes to review and update the ISCM program and strategy, in accordance with NIST Special Publication (SP) 800-137. The STB expects to complete work on this recommendation by March 31, 2021.

Recommendation 2020-6: The STB continues to improve its ISCM program and has taken steps to collect continuous monitoring metrics for STB information systems. The STB will continue to develop processes to ensure that those collected metrics assist information system stakeholders to make informed, risk-based decisions. The STB expects to complete work on this recommendation by March 31, 2021.

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 202-2450357.

Sincerely,

RACHEL Digitally signed by RACHEL CAMPBELL

CAMPBELL Date: 2020.09.17 13:03:42 -04'00'

Rachel D. Campbell
Managing Director

U.S. DOT IG Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

<https://www.oig.dot.gov/hotline>

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590



www.oig.dot.gov