



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. QC2019082

September 25, 2019



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

QC2019082 | September 25, 2019

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. To meet this requirement, the Surface Transportation Board (STB) requested that we perform its fiscal year 2019 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

While there are no new recommendations issued for fiscal year 2019, STB concurs with the audit's findings with respect to the remaining eight open recommendations from the fiscal year 2017 and fiscal year 2018 FISMA audits.



U.S. Department of
Transportation

Office of Inspector General
Washington, DC

September 25, 2019

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

Dear Ms. Begeman:

I respectfully submit our report on the quality control review (QCR) of an 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 2019 FISMA review. We contracted with Williams Adley & Company DC LLP (Williams Adley), an independent public accounting firm, to conduct this review 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.

Williams Adley found that STB's information security program and practices were not effective. There are no new recommendations developed for the five functions, as the issues identified within these functions for fiscal year 2019 audit were consistent with those identified in the prior year.

We appreciate the cooperation and assistance of STB representatives. If you have any questions about this report, please call me at (202) 366-1407.

Sincerely,

A handwritten signature in cursive script, appearing to read "Louis C. King".

Louis C. King

Assistant Inspector General for Financial and
Information Technology Audits

cc: STB Audit Liaison

Attachment

Our Quality Control Review

We performed a QCR of Williams Adley's report, dated August 30, 2019 (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 19, 2019, Williams Adley provided STB with its draft report and received STB's response on August 23, 2019. STB's response is included in its entirety in the attached independent auditor's report.

While there are no new recommendations issued for fiscal year 2019, STB concurs with the audit's findings with respect to the remaining eight open recommendations from the fiscal year 2017 and fiscal year 2018 FISMA audits.

STB provided documentation to close fiscal year 2017 recommendations 9, 10, and 11 after the completion of the contractor's work. We will review this documentation to determine if it provides sufficient evidence to close these recommendations.

Actions Required

We consider the remaining prior year recommendations resolved but open pending completion of planned actions and our review of the documentation for the fiscal year 2017 recommendations 9, 10, and 11.

Exhibit. List of Acronyms

FISMA	Federal Information Security Modernization Act
OMB	Office of Management and Budget
QCR	quality control review
STB	Surface Transportation Board

Attachment. Independent Auditor's Report

FINAL REPORT

**Fiscal Year 2019 Federal Information Security Modernization Act of 2014 Audit of the
Surface Transportation Board's Information Security Program and Practices**

August 30, 2019



Contents

Results in Brief	2
Background	3
Results of the FY 2019 FISMA Audit	4
I. Identify	4
II. Protect	4
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	19



August 30, 2019

Mr. Louis King
Assistant Inspector General for Financial and Information Technology Audits
1200 New Jersey Avenue, SE
Washington, DC 20590

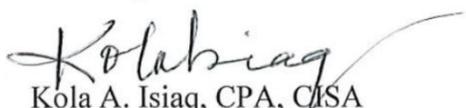
Dear Mr. King:

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 the fiscal year (FY) 2019 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,¹ as required by OMB, for the period October 1, 2018 to May 31, 2019.² To address OMB's 2019 FISMA reporting metrics, Williams Adley interviewed STB officials, and analyzed data pertaining to STB's information security program and practices.

Sincerely,



Kola A. Isiaq, CPA, CISA
Managing Partner

¹ A web-based application that collects security data from each Federal agency. OMB compiles the data and generates reports, as required by FISMA.

² Williams Adley performed its audit procedures from February 19, 2019 to May 31, 2019. The results of the FY 2019 audit are as of May 31, 2019.

Results in Brief

OMB required independent auditors to assess metrics across five security function areas to determine the maturity level of STB’s information security program. Program maturity was assessed at one of five 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 2019 audit.

Based on the audit procedures performed, we concluded that STB’s information security program remains ineffective.³ Although STB’s information security program was deemed ineffective for FY 2019, we determined that STB made progress in maturing its overall information security program through the development of its policies and procedures to address prior year recommendations and improving three FISMA functions, as outlined in the table below.

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

Table 1 - FY 2019 IG FISMA Reporting Metric Ratings

While STB has made significant efforts to define its program and address prior year recommendations, additional work is needed to define and implement an effective information security program. New recommendations were not developed for the five functions as the issues identified within these functions for FY 2019 audit were consistent with those identified in the prior year. Appendix B, Status of Prior Year Recommendations, contains a detailed analysis of STB’s progress in addressing prior year recommendations from the OIG report FI2018002, FISMA 2017: The Surface Transportation Board’s Information Security Program Is Not Effective, dated October 26, 2017 and 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. In summary, thirteen (13) recommendations were closed and eight (8) remain open at the conclusion of the FY 2019 audit.

Appendix C within this report contains criteria and guidance used in the report and Appendix D documents Management’s response to the results of the FY 2019 audit. STB concurred with all recommendations and provided appropriate actions and completions dates. Williams Adley did not audit management’s response and provides no opinion or conclusions, thereto. Any corrective actions will be assessed during the FY 2020 FISMA audit.

³ An information security program rated at a level 4, Managed and Measurable, is considered to be effective.

Background

STB is an independent, adjudicatory body that, until passage of the Surface Transportation Board Reauthorization Act in December 2015, was within the DOT. While part of DOT, STB shared many information security controls, such as policy and procedures, with DOT and its Operating Administrations. As a stand-alone Agency, STB became 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.

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 2019, 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 maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies’ High Value Asset programs;
- Gauge agencies’ preparedness in addressing the new requirements outlined in the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure (SECURE) Technology Act of 2018 for supply chain risk management; and
- Reflect changes to criteria references.

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 2019 IG Evaluation Maturity Levels, Source: DHS

Results of the FY 2019 FISMA Audit⁴

I. Identify

The Identify function, which includes 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. However, Williams Adley identified the following 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 recommend a new adjustment in FY 2019 because Recommendation 2018-1 addresses the current conditions noted.

II. Protect

The Protect function, which includes configuration management, user identity and access management, security awareness training, and data protection and privacy, was rated at a level 2 maturity: defined.

⁴ The criteria used to support the conditions found within the FY 2019 audit are found in Appendix C – Criteria and Guidance.

Configuration Management

STB has taken steps towards improving its configuration management program, such as developing a Configuration Management Plan and Vulnerability Management Plan and updated supporting policies and procedures.

Williams Adley did not identify any issues related to the plan, policies, and procedures supporting STB's configuration management program. However, the plan, policies and procedures were finalized between March and May 2019. Therefore, controls were not implemented until May 2019 and thus there was not a sufficient period of time to appropriately assess whether the controls are implemented correctly, operating as intended, and producing the desired outcomes.

Based on the audit procedures performed, STB is in the process of implementing its configuration management program.

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) Plan and modifying its identity and access management policies and procedures. However, Williams Adley identified the following deficiencies within the Identity & Access Management IG FISMA metric domain:

- STB has not fully developed an ICAM strategy to guide its ICAM process and activities as its missing "as-is" assessment, identification of gaps (from a desired or "to-be state"), and a transition plan, in accordance with the Federal Identity, Credential, and Access Management (FICAM) Architecture.
- STB did not maintain a signed copy of the Rules of Conduct document for one sampled new hire, in accordance with STB's New Hire IT Orientation Procedures.

STB management stated that due to the partial federal government shutdown, work on the prior years' FISMA recommendations was impacted by the furlough of information security personnel. Additionally, the October closure of the FY 2018 STB FISMA Audit and the February start of the FY 2019 STB FISMA Audit compressed the STB working cycle to implement prior years' audit recommendations. Finally, as indicated in STB's March 19, 2019 letter to DOT OIG, the resolution of this recommendation is not planned to be completed by STB until after the conclusion of the assessment period of the FY 2019 FISMA Audit. As a result, at the time of the assessment, the STB had not completed the implementation of security controls associated with Identity and Access Management and the current policies and procedures do not meet all FISMA requirements.

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 will not recommend a new adjustment in FY 2019 because Recommendation 2018-3 addresses the current conditions noted.

Security Training

STB has taken steps towards improving its security training program, such as developing a security awareness and training policy. However, Williams Adley identified the following deficiencies within the Security Training IG FISMA metric domain:

- STB has not finalized its security awareness training program, in accordance with NIST SP 800-53, rev. 4.
- STB has not developed a security awareness training plan and supporting policies and procedures, in accordance with NIST SP 800-53, rev. 4.
- STB does not have a defined process to perform an assessment of the skills, knowledge, and abilities of its workforce to determine specialized security training needs, in accordance with NIST SP 800-53, rev. 4.

STB management stated that due to the partial federal government shutdown, work on the prior years' FISMA recommendations was impacted by the furlough of information security personnel. Additionally, as indicated in STB's March 19, 2019 letter to DOT OIG, the resolution of this recommendation is not planned to be completed until after the conclusion of the assessment period of the FY 2019 FISMA Audit. As a result, at the time of assessment, STB had not completed activities to address the recommendations for security controls associated to the development of strategies, processes, and procedures within the area of Security Training.

If all personnel—including IT personnel with specific security responsibilities—with access to STB's systems are not appropriately trained, users could compromise the security of the network.

Williams Adley will not recommend a new adjustment in FY 2019 because Recommendations 2017-9, 2017-10, and 2017-11 address the current conditions noted.

Data Protection and Privacy

STB has taken steps towards improving its privacy program, such as developing a Media Protection policy. However, Williams Adley identified the following deficiencies within the Data Protection and Privacy IG FISMA metric domain:

- STB does not have a defined privacy program plan and related policies and procedures, in accordance with NIST SP 800-122.
- STB has not developed a Data Breach Response plan, in accordance with NIST SP 800-122.
- STB has not developed policies, procedures, roles or responsibilities for determining the personnel responsible for performing data exfiltration exercises, in accordance with NIST SP 800-53, rev. 4.

STB management stated that due to the partial federal government shutdown, work on the prior years' FISMA recommendations was impacted by the furlough of STB privacy personnel. Additionally, as indicated in STB's March 19, 2019 letter to DOT OIG, the resolution of this recommendation is not planned to be completed until after the conclusion of the assessment period of the FY 2019 FISMA Audit. As a result, at the time of the assessment, the STB had not completed its work to implement security controls associated with Data Protection and Privacy.

Without effective data protection and privacy, the STB's PII and other sensitive agency data may be compromised and exfiltrated without the knowledge of STB management, resulting in a loss of information and an introduction of vulnerabilities to systems.

Williams Adley will not recommend a new adjustment in FY 2019 because Recommendation 2018-5 addresses the current conditions noted.

III. Detect

The Detect function, which includes the information security continuous monitoring (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 developing an ISCM Plan and performing daily and weekly agent-based and discovery-based scans that provide operational and executive level awareness of threats and vulnerabilities. However, Williams Adley identified the following deficiencies within the ISCM IG FISMA metric domain:

- STB does not have a fully defined ISCM strategy in accordance with NIST SP 800-53, rev. 4 and NIST SP 800-137.
- STB's does not have policies and procedures to provide guidance over the following areas, in accordance with NIST SP 800-137:
 - Ongoing assessments and monitoring of security controls;
 - Collecting security related information required for metrics, assessments, and reporting; and
 - Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy.
- STB has not identified and defined the performance measures and requirements to assess the effectiveness of its ISCM program, in accordance with NIST SP 800-137.
- STB did not fully define roles and responsibilities of ISCM stakeholders, in accordance with NIST SP 800-53, rev. 4.

According to STB management, the Agency believed it had completed all work needed to address the ISCM recommendation. However, all elements of the recommendation were not implemented by STB due to a misinterpretation of the National Institute of Standards and Technology (NIST) federal guidance. As a result, the existing ISCM Plan does not fully satisfy the FISMA requirements of the security domain.

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 information system security goals, allowing STB to consistently monitor a dynamic network environment with changing threats, vulnerabilities, technologies, missions, and business functions of STB.

Williams Adley will not recommend a new adjustment in FY 2019 because Recommendation 2017-12 addresses the current conditions noted.

IV. Respond

The Respond function, which includes the incident response domain, was rated at a level 2 maturity: defined.

Incident Response

STB has taken steps towards improving its Incident Response program, such as the development of its Incident Response Plan.

Williams Adley did not identify any issues related to the plan, policies, and procedures supporting STB's incident response program. However, the plan, policies and procedures were finalized in May 2019. Therefore, controls were not implemented until May 2019 and thus there was not a sufficient period of time to appropriately assess whether the controls are implemented correctly, operating as intended, and producing the desired outcomes.

Based on the audit procedures performed, STB has addressed prior year recommendations and is in the process of implementing its incident response program.

V. Recover

The Recover function, which includes the contingency planning domain, was rated at a level 1 maturity: ad hoc.

Contingency Planning

STB has taken steps towards improving its contingency planning program, such as conducting Business Impact Analysis (BIA), developing an agency-wide Contingency Planning document and Disaster Recovery Plan (DRP). However, Williams Adley identified the following deficiencies in the Contingency Planning IG FISMA metric domain:

- STB has not fully defined and communicated across the roles and responsibilities of STB stakeholders involved in information systems contingency planning, in accordance with NIST SP 800-53, rev. 4.

- STB did not develop Information System Contingency Plans (ISCPs), Business Continuity Plan (BCP), and Continuity of Operations Plan (COOP), in accordance with STB's Contingency Planning document.
- STB did not perform tests/exercises of its information system contingency planning processes, in accordance with NIST SP 800-34, rev. 1.

STB management stated that due to the partial federal government shutdown, work on the prior years' FISMA recommendations was impacted by the furlough of information security personnel. Additionally, the October closure of the FY 2018 STB FISMA Audit and the February start of the FY 2019 STB FISMA Audit compressed the STB working cycle to implement prior years' audit recommendations. As a result, the STB encountered delays implementing security controls associated with contingency planning.

Without fully developed and implemented contingency plans that include established and documented alternate sites for telecommunications, storage, and processing, and backup strategies, STB may be unable to access critical information and resources to perform mission-critical business functions in the event of an extended outage and disaster.

Williams Adley will not recommend a new adjustment in FY 2019 because Recommendation 2017-14 addresses the current conditions noted.

Conclusion

STB made significant improvements towards establishing the foundation for its information security program within the Identify, Protect, and Respond functions. However, activities within the Detect and Recover functions were not formalized during the audit period and continue to be performed in an ad-hoc, reactive manner. Until STB formalizes its governing documents and implements its defined processes, the Agency's information systems will be at increased risk of attack or compromise.

Recommendations

New recommendations were not developed for the five functions as the issues identified within these functions for the FY 2019 audit were consistent with those identified in the prior year. Refer to Appendix B, Status of Prior Year Recommendations, which contains a detailed analysis of prior year recommendations.

Appendix A – Scope and Methodology

The 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 the Federal Information Security Modernization Act of 2014 for the period October 1, 2018 to May 31, 2019.⁵ We 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 2019 audit, we selected STB Local Area Network, Amazon Web Services and CylanceProtect as our in-scope systems.

We performed our audit steps onsite from February 19, 2019 to May 31, 2019. To perform this audit, we 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 daily operations, conducted judgmental sampling where applicable, inspected STB policies and procedures, and obtained sufficient evidence to support the conclusions and recommendations presented in this report. New recommendations were not developed as existing recommendations address the areas needed to complete the foundation of an effective information security program.

⁵ Williams Adley performed its audit procedures from February 19, 2019 to May 31, 2019. The results of the FY 2019 audit are as of May 31, 2019.

Appendix B – Status of Prior Year FISMA Recommendations⁶

#	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 FY19.
2017-2	Complete the system reauthorization of the STB LAN	Closed in FY18.
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 FY18.
2017-4	Define specifications and acquire an automated solution to assist with the risk management program.	Closed in FY19.
2017-5	Develop policies and procedures for the implementation of an information security architecture.	Closed in FY19.
2017-6	Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.	Closed in FY19.
2017-7	Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.	Closed in FY18.
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 FY19.

⁶ 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 and 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.

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.	Open - STB does not have a defined process to perform an assessment of the skills, knowledge, and abilities of its workforce to determine specialized security training needs.
2017-10	Develop and implement a formal process for measuring the effectiveness of its security awareness and training program.	Open - STB has not finalized its security awareness training program. Furthermore, STB has not developed a security awareness training plan and supporting policies and procedures.
2017-11	Modify the training plan to include missing elements such as funding, goals and use of technology.	Open - STB has not developed a security awareness training plan and supporting policies and procedures.
2017-12	Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.	Open – STB does not have a fully defined ISCM strategy in accordance with National Institute of Standards and Technology (NIST) 800-137. Furthermore, STB's does not have policies and procedures to provide guidance over the following areas: <ul style="list-style-type: none"> • Ongoing assessments and monitoring of security controls; • Collecting security related information required for metrics, assessments, and reporting; and • Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy.
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 FY19.
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.	Open - STB did not perform tests/exercises of its information system contingency planning processes.
2018-1	Fully develop a risk management strategy and the supporting procedures for maintaining an accurate system inventory.	Open – STB did not develop an information security risk management strategy at all three levels of organization, in accordance with the National Institute of Standards and Technology (NIST) 800-39 guidelines. In addition, STB did not use a standard data elements/taxonomy to develop and maintain

		an up-to-date inventory of hardware and software assets.
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 FY19.
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. 	Open – STB has not fully developed an ICAM strategy to guide its ICAM process and activities as its missing “as-is” assessment, identification of gaps (from a desired or "to-be state"), and a transition plan.
2018-4	Full implement the use of PIV card for personnel to access STB’s facilities.	Closed in FY19.
2018-5	Develop a privacy program, including related plans, policies and procedures, for 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.	Open - STB does not have a defined privacy program plan and related policies and procedures.
2018-6	Develop an Incident Response plan in accordance with NIST SP 800-61, rev. 2.	Closed in FY19.
2018-7	Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.	Closed in FY19.

Appendix C – Criteria and Guidance

Williams Adley utilized the following criteria in assessing the effectiveness of the Surface Transportation Board’s information security program and support the conditions identified during the FY 2019 audit:

I. Risk Management

Williams Adley utilized the following criteria in assessing the effectiveness of the STB’s entity-wide Risk Management program:

- 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 utilized FY 2019 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Metrics as the criteria in assessing the implementation of STB’s Configuration Management program:

- FISMA Metric Question 14, Level 3 (consistently implemented) Requirements: Individuals are performing the roles and responsibilities that have been defined across the organization.
- FISMA Metric Question 15, Level 3 (consistently implemented) Requirements: The organization has consistently implemented an organization wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan.
- FISMA Metric Question 16, Level 3 (consistently implemented) Requirements: The organization consistently implements its policies and procedures for managing the

configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures.

- FISMA Metric Question 17, Level 3 (consistently implemented) Requirements: The organization consistently records, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.
- FISMA Metric Question 18, Level 3 (consistently implemented) Requirements: The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on least functionality. Further, the organization consistently utilizes Security Content Automation Protocol (SCAP) validated software assessing (scanning) capabilities against all systems on the network (see inventory from questions #1 - #3) to assess and manage both code-based and configuration-based vulnerabilities.
- FISMA Metric Question 19, Level 3 (consistently implemented) Requirements: The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days.
- FISMA Metric Question 20, Level 3 (consistently implemented) Requirements: The organization has consistently implemented its Trusted Internet Connection (TIC) approved connections and critical capabilities that it manages internally. The organization has consistently implemented defined TIC security controls, as appropriate and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate.
- FISMA Metric Question 21, Level 3 (consistently implemented) Requirements: The organization consistently implements its change control policies, procedures, and processes, including explicit consideration of security impacts prior to change implementation

III. Identity and Access Management

Williams Adley utilized the following criteria in assessing the effectiveness of the STB's entity-wide data protection & privacy program:

- According to the Federal Identity, Credential, and Access Management (FICAM) Architecture, an enterprise architecture is a conceptual blueprint that defines what an organization is and does. This "blueprint" uses principles and practices to define an approach for an organization to design, plan, and execute a strategy (<https://arch.idmanagement.gov/>). FISMA Metric Question 24, Level 2 (defined) Requirements: The organization has defined its ICAM strategy and developed milestones for how it plans to align with Federal initiatives, including strong authentication, the FICAM segment architecture, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate.
- STB's New Hire IT Orientation Procedures state that "employees are required to review and acknowledge Rules of Conduct document with receipt of signature" upon activation of STB accounts.

IV. Security Training

Williams Adley utilized the following criteria in assessing the effectiveness of the STB's entity-wide security training program:

- NIST SP 800-53, rev. 4, states that the organization will do the following:
 - Provides role-based security training to personnel with assigned security roles and responsibilities:
 - Before authorizing access to the information system or performing assigned duties;
 - When required by information system changes; and
 - [Assignment: organization-defined frequency] thereafter.
- NIST SP 800-53, rev. 4,² states that the organization provides basic security awareness training to information systems users
 - As part of new training for new users;
 - When required by information system changes; and
 - [Assignment: organization-defined frequency] thereafter.

V. Data Protection and Privacy

Williams Adley utilized the following criteria in assessing the effectiveness of the STB's entity-wide data protection and privacy program:

- NIST SP 800-122, states “to establish a comprehensive privacy program that addresses the range of privacy issues that organizations may face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices.”
- 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.

VI. Information Security Continuous Monitoring (ISCM)

Williams Adley utilized the following criteria in assessing the effectiveness of the STB's entity-wide ISCM program:

- NIST SP 800-53, rev. 4, states that the organization “develops a continuous monitoring strategy and implements a continuous monitoring program.”
- 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 800-53, CA-1 states that the organization develops, documents, and disseminates a security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance

VII. Incident Response

Williams Adley utilized FY 2019 IG FISMA Metrics as the criteria in assessing the implementation of STB’s incident response program:

- FISMA Metric Question 52, Level 3 (consistently implemented) Requirements: The organization consistently implements its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy and processes to update the program.
- FISMA Metric Question 53, Level 3 (consistently implemented) Requirements: Individuals are performing the roles and responsibilities that have been defined across the organization.
- FISMA Metric Question 54, Level 3 (consistently implemented) Requirements: The organization consistently utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software.
- FISMA Metric Question 55, Level 3 (consistently implemented) Requirements: The organization consistently implements its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations.
- FISMA Metric Question 56, Level 3 (consistently implemented) Requirements: The organization consistently shares information on incident activities with internal stakeholders. The organization ensures that security incidents are reported to the United States Computer Emergency Readiness Team (US-CERT), law enforcement, the Office of Inspector General, and the Congress (for major incidents) in a timely manner.
- FISMA Metric Question 57, Level 3 (consistently implemented) Requirements: The organization consistently utilizes on-site, technical assistance/surge capabilities offered by the Department of Homeland Security (DHS) or ensures that such capabilities are in place and can be leveraged when needed. In addition, the organization has entered into contractual relationships in support of incident response processes (e.g., for forensic support), as needed. The organization has fully deployed DHS’ Einstein 1 and 2 to screen all traffic entering and leaving its network through a Trusted Internet Connection (TIC).
- FISMA Metric Question 58, Level 3 (consistently implemented) Requirements: The organization has consistently implemented its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization's network, and have been

configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans

VIII. Contingency Planning

Williams Adley utilized the following criteria in assessing the effectiveness of the STB's entity-wide Contingency Planning program:

- NIST SP 800-53, rev. 4, states that the organization will do the following:
 - Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
 - A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
 - Reviews and updates the current:
 - Contingency planning policy [Assignment: organization-defined frequency]; and
 - Contingency planning procedures [Assignment: organization-defined frequency].
- STB's Contingency Planning document states that key elements to STB's comprehensive information system contingency planning capability are: BIA, BCP, COOP, DRP, ISCP, and Occupant Emergency Plan (OEP).
- NIST SP 800-34, rev. 1 states, "[Information System Contingency Plan] testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures

Appendix D – Management’s Response



SURFACE TRANSPORTATION BOARD
Washington, DC 20423

August 23, 2019

VIA E-MAIL: louis.king@oig.dot.gov
Mr. Louis C. King
Assistant IG for Financial and IT Audits
DOT Office of Inspector General
Headquarters
1200 New Jersey Ave., SE
W72-302
Washington, DC 20590

Re: Fiscal Year 2019 FISMA Audit of the Surface Transportation Board

Dear Mr. King:

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) 2019 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 this year’s FISMA audit finds that the Board’s overall information security maturity level has improved since last year’s assessment. This improvement is reflective of the STB’s strong 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 FISMA audit recognizes the Board’s significant efforts to define its security program through FY 2019, while also providing the Board a roadmap for continued IT security program improvements.

While there are no new recommendations issued for FY 2019, the STB concurs with the audit’s findings with respect to the remaining open recommendations from the FY 2017 and FY 2018 FISMA audits. The Board continues working to achieve a fully effective information security program and is committed to fully addressing those remaining recommendations and advancing to the next security maturation level. The recommendations that remain from the FY 2017 and FY 2018 audits and their estimated completion dates are discussed below.

Remaining FY 2017 Recommendations:

Since the conclusion of the FY 2018 audit, the Board has completed work and closed six FY 2017 recommendations, specifically recommendations 1, 4, 5, 6, 8, and 13. Additionally, the STB has completed its work as of its target date of July 2019 (after the close of the audit assessment period) and, on August 22, 2019, submitted artifacts for assessment for recommendations 9, 10,

and 11, as described below.

Recommendation 9: The STB has taken steps to improve its security training program by developing security awareness policies, plans, and procedures. The STB has conducted a needs assessment to formally determine the Board's awareness and training needs, which includes processes that assess the skills, knowledge, and abilities of the STB workforce. The STB has completed work related to this recommendation and awaits formal assessment for closure by DOT-OIG.

Recommendation 10: The STB has developed a formal process for measuring the effectiveness of its security awareness and training program. The STB has completed work related to this recommendation and awaits formal assessment for closure by DOT-OIG.

Recommendation 11: The STB has reviewed its training program and made modifications to its training plan to including missing elements such as funding, goals, and use of technology. The STB has completed work related to this recommendation and awaits formal assessment for closure by DOT-OIG.

The STB has established new target action dates to complete additional work needed to fully address the remaining two FY 2017 recommendations by the end of 2019, as described below.

Recommendation 12: The STB has made significant progress with its Information Systems Continuous Monitoring (ISCM) Program. These improvements include robust daily and weekly agent-based and discovery-based scans that provide operational and executive level awareness of threats and vulnerabilities. In addition, the Board developed an ISCM plan which incorporates the agency's strategic ISCM vision. Based upon further guidance received during the FY 2019 audit, the STB will modify this plan to ensure it is fully defined in accordance with NIST SP 800-53, rev. 4 and NIST SP 800-137. The STB expects to fully address this recommendation by December 31, 2019.

Recommendation 14: The STB is making progress on its contingency planning. The Board developed an agency-wide Contingency Planning document and Disaster Recovery Plan. Additionally, the STB has finalized the Business Impact Analysis and now has an Occupant Emergency Plan in place. The Board is in the process of defining and communicating contingency roles and responsibilities to STB staff. Additionally, the Board will ensure that additional documents such as the Information System Continuity Plan, Business Continuity Plan, and Continuity of Operations Plans are finalized, in accordance to NIST SP 800-34. The STB expects to fully address this recommendation by December 31, 2019.

Remaining FY 2018 Recommendations:

Since the conclusion of the FY 2018 audit, the Board has completed work and closed four of seven FY 2018 recommendations, specifically recommendations 2, 4, 6, and 7. Note, not all of the FY 2018 recommendations were assessed during the recent audit given that the target action date for completion of certain recommendations was after the FY 2019 assessment period. The

STB continues the work needed to meet target action dates and fully address the FY 2018 recommendations. The Board plans to address the remaining FY 2018 recommendations, as described below:

Recommendation 1: The STB continues to make steady improvements within its Risk Management Program. Based on further guidance received during the audit, the Board will fully develop and maintain an up-to-date inventory of hardware assets and software assets with detailed information for tracking and reporting. The STB expects to fully address this recommendation by May 30, 2020.

Recommendation 3: The STB is committed to developing a comprehensive Identity, Credential, and Access Management (ICAM) Program. The Board has developed an ICAM plan to guide its ICAM process and activities. Additionally, the STB is using a HSPD-12 credential to grant physical access to STB personnel. The Board will modify its exiting ICAM policies and procedures to ensure that an “as-is” assessment, desired state, and a transition plan is established. The expected date to fully address this recommendation remains September 30, 2019.

Recommendation 5: The STB is making progress toward developing a comprehensive privacy program, including preparing a privacy program plan and related policies and procedures, although implementing the privacy plan has taken longer than initially anticipated. Implementation of the Board’s privacy plan will add the necessary data protection and privacy controls for personally identifiable information that the Board collects, uses, maintains, shares, and disposes of through the Board’s information systems. The STB expects to fully address this recommendation by March 31, 2020.

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: 2019.08.23 14:31:34
-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