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. QC2019001

October 24, 2018

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

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

Required by the Federal Information Security Modernization Act of 2014

QC2019001 | October 24, 2018

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 2018 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 seven recommendations.

U.S. Department of Transportation

Office of Inspector General
Washington, D.C. 20590

October 24, 2018

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 our 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 2014[1] (FISMA) requires agencies to implement information security programs. The act also requires agencies to have annual independent evaluations performed to determine the effectiveness of their programs and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, STB requested that we perform its fiscal year 2018 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. Williams Adley made the following seven recommendations to improve STB's information security program and practices.

1. Fully develop and implement a risk management strategy and the supporting procedures for maintaining an accurate system inventory.

2. Develop a configuration management plan with supporting policies and procedures and ensure that the existing Change Management Charter aligns with the plan.

[1] Pub. Law No. 113-283.

3. Develop an ICAM strategy to guide its ICAM process and activities, and modify 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 organization.

4. Fully implement the use of PIV cards for personnel to access STB's facilities.

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.

6. Develop an Incident Response plan in accordance with NIST 800-61, rev. 2.

7. Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.

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

Sincerely,

Louis C. King
Assistant Inspector General for Financial and
Information Technology Audits

cc: STB Audit Liaison

Attachment

Quality Control Review

We performed a quality control review (QCR) of Williams Adley's report, dated October 16, 2018 (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on the 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 Office of Inspector General Response

On September 28, 2018, Williams Adley provided STB with its draft report and received STB's response on October 15, 2018. STB's response is included in its entirety in the attached independent auditor's report.

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

Actions Required

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

Exhibit. List of Acronyms

DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act
ICAM	identity, credential, and access management
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
QCR	quality control review
STB	Surface Transportation Board
US-CERT	United States Computer Emergency Readiness Team

Attachment. Independent Auditor's Report

FINAL REPORT

Fiscal Year 2018 Federal Information Security Modernization Act of 2014 Audit of the Surface Transportation Board's Information Security Program and Practices

October 16, 2018

WILLIAMS ADLEY

Contents

WILLIAMS ADLEY

October 16, 2018

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) 2018 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, we 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 July 1, 2017 through September 30, 2018[2]. To address OMB's 2018 FISMA reporting metrics, we 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 was onsite from July 9, 2018 through September 6, 2018. The results of the FY 2018 audit are as of September 30, 2018.

Results in Brief

For the FY 2018 review, 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. An information security program rated level 4, Managed and Measurable, is considered to be effective.

Based on the audit procedures performed, we concluded that STB's information security program remains at a level 1 maturity, Ad-Hoc, for Identify, Protect, Detect, Respond, and Recover. Although STB's information security program was not deemed effective for FY 2018, we determined that STB made progress in maturing its overall program through the development of its policies and procedures to address prior year recommendations. While STB has made efforts to define its program, additional work is needed to complete the foundation of an effective information security program. Therefore, we are making a series of recommendations to assist the STB in its progress to improve its security program and practices in the following five domains[3]:

1. Risk Management (Identify)
2. Configuration Management (Protect)
3. Identity and Access Management (Protect)
4. Data Protection and Privacy (Protect)
5. Incident Response (Respond)

The seven (7) recommendations are contained in the Recommendations section of this report. STB concurred with all seven (7) recommendations and provided appropriate actions and completion dates (see Appendix D). We also reviewed fourteen (14) OIG prior year recommendations related to STB's security program and practices and to determine their status. In summary, three (3) of the prior year recommendations were implemented and closed, and eleven (11) remain open or partially open. Appendix B provides the STB's progress in addressing prior year recommendations from the OIG report FI2018002 dated October 26, 2017, FISMA 2017: The Surface Transportation Board's Information Security Program Is Not Effective. Appendix C contains criteria and guidance used in the report.

Background

STB is an independent, adjudicatory body that, until passage of the Surface Transportation Board Reauthorization Act in December 2015, was housed within 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.

[3] New recommendations were not developed for the Detect and Recover functions as the issues identified within these functions for FY 2018 audit were consistent with those identified in the prior year. Refer to Appendix B – Status of Prior Year Recommendations.

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; see table 1 for definitions of these functions and the number of metrics in each function. For FY 2018, 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 for inspectors general reviews and independent auditors' annual information security evaluations to include an additional domain, Data Protection and Privacy.

Cybersecurity Framework Function (Domains)	Definition	No. of metrics for FISMA 2018
Identify (Risk Management)	Requires agencies to develop the understanding needed to manage security risks to systems, assets, data, and capabilities. Includes metrics for risk management, weakness remediation, and security authorization.	13
Protect (Configuration Management, Identity and Access Management, Data and Privacy, Security Training)	Requires agencies to develop and implement appropriate safeguards to ensure delivery of infrastructure services. Includes metrics for configuration management, identity and access management, data and privacy, and security training.	32
Detect (Information Security Continuous Monitoring)	Requires agencies to develop and implement processes to identify incidents that may include security breaches. Includes metrics for information security continuous monitoring.	6
Respond (Incident Response)	Requires agencies to develop and implement processes for remediating detected cybersecurity incidents. Includes metrics for incident handling and reporting.	8
Recover (Contingency Planning)	Requires agencies to develop, implement, and maintain up-to-date plans for restoration of capabilities and services impaired during a security event or emergency shut down. Includes metrics for contingency planning.	8

Table 1 - FY 2018 IG FISMA Reporting Metrics, Source: DHS

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 (from lowest to highest)	Definition
Ad Hoc (Level 1)	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Defined (Level 2)	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Consistently Implemented (Level 3)	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable (Level 4)	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.
Optimized (Level 5)	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Table 2 - FY 2018 IG FISMA Reporting Metrics, Source: DHS

Results of the FY 2018 FISMA Audit[4]

I. Identify#

The Identify function, which includes the risk management domain, was rated at a level 1 maturity: ad hoc.

Risk Management

STB has taken steps towards improving its Risk Management program, such as developing a Risk Management Policy, a Risk Management Charter, a Risk Profile, and completing the system authorization of the STB Local Area Network (STB LAN)[5]. However, Williams Adley identified the following issues within the risk management IG FISMA metric domain:

1. 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.
2. STB does not have a defined process to maintain an accurate system inventory, as required by NIST SP 800-53, rev. 4.
3. STB did not use 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, as required by NIST SP 800-53, rev. 4.
4. STB did not use 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, as required by NIST SP 800-53, rev. 4.

[4] The criteria used to support the conditions found within the FY 2018 audit are found in Appendix C – Criteria and Guidance.

[5] An evaluation of the prior year FISMA recommendations is found in Appendix B – Status of Prior Year FISMA Recommendations.

5. STB did not categorize and did not communicate the importance/priority of information systems in enabling its missions and business functions, as required by NIST SP 800-39.
6. STB has not defined an information security architecture, as required by NIST SP 800-53, rev. 4.
7. Roles and responsibilities for each stakeholder involved in risk management are not defined, in accordance with NIST SP 800-39. Specifically, as it relates for the following roles:
    - Chief Risk Officer;
    - Senior Accountable Official for Risk Management; and
    - Chief Information Security Officer.
8. STB has not followed their Plan of Action and Milestones (POA&Ms) procedures for their existing POA&Ms. As a result, existing POA&Ms are missing required fields such as remediation plan, detection date, and prioritization, as required by NIST SP 800-53, rev. 4.
9. STB did not have defined policies and procedures for conducting system level risk assessments, in accordance with NIST SP 800-53, rev. 4.
10. STB does not have defined procedures to communicate risks at all three organizational tiers (agency, business, system) to all necessary internal and external stakeholders, in accordance with NIST SP 800-53, rev. 4
11. STB does not utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the STB, as required by NIST SP 800-39.

Prior to its separation from DOT, STB relied on DOT existing risk management controls and process to consistently evaluate risk across the organization at all three tiers. As a stand-alone Agency, STB became responsible for maintaining its own information security program and independently meeting FISMA's requirements. STB is still in process of developing its risk management program.

Without adequate identification, assessment, prioritization, and monitoring controls, security risks may not be resolved or communicated to senior management within a timely manner and may subsequently expose STB's sensitive data, systems, and hardware to unauthorized access and potentially malicious attacks.

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 1 maturity: ad hoc.

Configuration Management
STB has taken steps towards improving its configuration management program, such as developing a Change Management Charter and Microsoft Patching Procedure document, defining roles supporting STB's Configuration Management program, and adopting a Trusted Internet Connection (TIC). However, Williams Adley identified the following issues within the configuration management IG FISMA metric domain:

1. STB does not have a configuration management plan, consistent with NIST SP 800-53, rev. 4, that incorporates the following required areas:
    - Patching;
    - Baselines;
    - Software development life cycle (SDLC) process;
    - Vulnerability remediation; and
    - Monitoring of configuration items, for example auditing of completed changes or a process to identify or detect unauthorized changes.
2. STB has not fully developed a process, consistent with NIST SP 800-53, rev. 4, to patch all software found within the environment. Currently:
    - There is no defined process to patch third-party software;
    - The Microsoft patch procedures do not identify roles and responsibilities; and
    - The Microsoft patch process does not identify the need to have patches approved before implementation.
3. STB's Vulnerability Management procedures do not identify the specific procedures to handle identified vulnerabilities, as required by NIST 800-53, rev. 4. Additionally, prioritization due to vulnerability rating is not considered within the Vulnerability Management procedures document.
4. STB has not defined a process to implement or update baseline configurations, in accordance with NIST SP 800-53, rev. 4.
5. STB does not have a complete and accurate hardware and software inventory with all required details, as required by NIST SP 800-53, rev. 4.
6. STB's Configuration Management Policy does not define roles and responsibilities for a Chief Information Security Officer, Authorizing Official, Information System Owner and Information System Administrator, as required by NIST SP 800-128.

STB has not implemented an effective organization-wide configuration management program as critical processes and procedures to support the configuration management program are not documented. This is potentially a result of limited resources and the lack of a dedicated senior information security officer to develop an information security program with supporting policies and procedures as required by FISMA.

Without a documented configuration management plan that includes all required configuration management processes, STB may intentionally or unintentionally compromise its information systems. For example, if a patch is not appropriately deployed, a vulnerability, even after identification, could be exploited resulting in the loss of confidentiality, integrity and availability of STB services.

Identity and Access Management

STB has taken steps towards improving its identity and access management program, such as modifying its identity and access management policies and procedures establishing rules of conduct for individuals, and utilizing Personal Identity Verification (PIV) for authentication. However, Williams Adley identified the following issues within the Identity and Access Management IG FISMA metric domain:

1. STB has not developed an identity, credential, and access management (ICAM) strategy, in accordance with the Federal Identity, Credential, and Access Management Roadmap

and Implementation Guidance, to guide its ICAM process and activities, including but not limited to the following:
    - Identifying ICAM stakeholders; and
    - Defining roles and responsibilities of ICAM stakeholders.
2. STB does not have formally documented procedures, consistent with NIST SP 800-53, rev. 4, to support the following:
    - Separation of duties within the organization;
    - Defined security requirements for remote access to STB's IT environment;
    - Implementation of identifier and authenticator management controls;
    - Privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege; and
    - Defined requirements for cryptographic mechanisms, system time-outs, and monitoring of remote access sessions.
3. STB has not defined its existing processes for assigning personnel risk designations prior to granting users with access to its systems, in accordance with NIST SP 800-53, rev. 4.
4. STB has not fully implemented the use of PIV cards to gain physical access to its facilities, in accordance with Homeland Security Presidential Directive-12.
5. A sample Account Request Form did not specify the group memberships required for the creation of a general user account, as required by NIST SP 800-53, rev. 4.
6. A sample Administrator Account Request Form did not specify the group memberships required for the creation of an administrator account, as required by NIST SP 800-53, rev. 4.
7. Williams Adley was unable to obtain a complete and accurate population of terminated employees for FY 2018 to test the effectiveness of STB's access disablement and deletion, as required by NIST SP 800-53, rev. 4.

STB has not finalized documenting critical processes and procedures to support their identity and access management program. This is possibly due to limited resources and a dedicated senior information security officer to develop an information security program with supporting policies and procedures as required by FISMA. The implementation of PIV cards for personnel to access STB's facilities is in progress and awaiting a site renovation to be completed after FY 2018.

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.

Security Training

STB has taken steps towards improving its security training program, such as developing a security awareness and training policy. Williams Adley identified the following issues within the Security Training IG FISMA metric domain during the FY18 audit:

1. STB has not finalized its security awareness training program including a strategy and supporting procedures, as required by NIST SP 800-53, rev. 4.
2. 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, as required by NIST SP 800-53, rev. 4.

Prior to its separation from DOT, STB shared many information security controls, including DOT's Security Training program. As a stand-alone Agency, STB became responsible for maintaining its own information security program and independently meeting FISMA's requirements. As a result, STB is currently researching the elements for designing a needs assessment. Also, STB is developing for implementation a formal process to measure the effectiveness of its security and awareness training program and reviewing its training plan and will modify it to include the missing elements.

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.

Data Protection and Privacy
Data Protection and Privacy was recently added to the FISMA metric in FY 2018 and Williams Adley identified the following deficiencies within the Data Protection and Privacy IG FISMA metric domain:

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

Prior to its separation from DOT, STB inherited information security controls, including Data Protection and Privacy controls. As a stand-alone Agency, STB became responsible for maintaining its own information security program and independently meeting FISMA's requirements. As a result, STB is currently in the process of developing its Data Protection and Privacy policies and procedures.

Without effective data protection and privacy, the STB's personally identifiable information (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 its systems.

III. Detect

The Detect function, which includes the information security continuous monitoring (ISCM) domain, was rated at a level 1 maturity: ad hoc.

ISCM
STB is in the process of implementing and finalizing its ISCM program. For example, STB has developed robust daily and weekly agent-based and discovery-based scans that provide operational and executive level awareness of threats and vulnerabilities. Williams Adley identified the following deficiencies within the ISCM IG FISMA metric domain:

STB does not have an overall ISCM strategy, as required by NIST SP 800-53, rev. 4.

1. STB's does not have policies and procedures to provide guidance over the following areas, as required by 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.
2. STB has not defined roles and responsibilities of stakeholders, as required by NIST SP 800-53, rev. 4.
3. STB has not defined its process for performing ongoing assessments, as required by NIST SP 800-137.
4. STB has not identified and defined the performance measures and requirements to assess the effectiveness of its ISCM program, as required by NIST SP 800-137.

Prior to its separation from DOT, STB shared many information security controls, including DOT's ISCM program. As a stand-alone Agency, STB became responsible for maintaining its own information security program and independently meeting FISMA's requirements. As a result, STB is currently in the process of developing its ISCM strategy and supporting policy and procedures.

Without 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 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 issue a new recommendation as prior year recommendation 12 remains open. Refer to Appendix B – Status of Prior Year Recommendations for additional details.

IV. Respond

The Respond function, which includes the incident response domain, was rated at a level 1 maturity: ad hoc.

Incident Response
STB has taken steps towards improving its incident response program, such as developing an Incident Response Policy and Incident Response Procedure, and implementing Einstein 3 Accelerated (E3A) within the organization. However, Williams Adley identified the following issues within the Incident Response IG FISMA metric domain:

1. STB has not developed an Incident Response Plan, in accordance with NIST SP 800-61, rev. 2.
2. STB has not fully developed an incident response policy and supporting procedures, in accordance with NIST 800-53, rev. 4, to respond to cybersecurity events, as existing documents are missing the following components:
    - Incident response training procedures;

- Incident response testing procedures; and
- Fully defined and communicated incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies.

3. STB did not classify security incidents in accordance with STB's Incident Response Procedure document.
4. STB's Incident Response Procedure is not updated in accordance with new United States Computer Emergency Readiness Team (US-CERT) threat vector taxonomy requirements, as required by NIST SP 800-53, rev. 4.

Prior to its separation from DOT, STB relied on DOT existing incident response controls and process to detect, respond, and recover from security incidents. As a stand-alone Agency, STB became responsible for maintaining its own incident response program and independently meeting FISMA's requirements. STB is still in process of developing its incident response program, including developing an incident response plan and updating existing incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.

An inadequate incident response and reporting program may prevent the STB from detecting, identifying, containing, eradicating, and recovering from security incidents.

V. Recover

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

Contingency Planning
Williams Adley identified the following issue within the Contingency Planning IG FISMA metric domain. STB has not developed its information system contingency planning program through policies, procedures, and strategies, as required by NIST SP 800-34 and NIST SP 800-53, rev. 4. Specifically, STB has not:

- Fully defined and communicated the roles and responsibilities of STB stakeholders involved in information systems contingency planning;
- Conducted business impact analyses (BIAs) at both the organizational and information system levels;
- Developed information system contingency plans (ISCPs);
- Performed tests/exercises of its information system contingency planning processes;
- Performed information system backup and storage, including use of alternate storage and processing sites; and
- Ensured that information regarding the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions.

Prior to its separation from DOT, STB relied on DOT existing contingency planning controls and process to access critical information and resources to perform mission critical business

functions in the event of an extended outage and/or disaster. As a stand-alone Agency, STB became responsible for maintaining its own contingency planning and independently meeting FISMA's requirements. STB is still in process of developing its contingency planning program.

Without fully developed and implemented contingency plans that include business impact analyses, 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 issue a new recommendation as prior year recommendation 14 remains open. Refer to Appendix B – Status of Prior Year Recommendations for additional details.

Conclusion

STB has taken major steps in building the foundation for its information security program through the development of policies and procedures, acquiring tools, and completing the authorizations for its information systems. However, STB is encumbered by several outstanding security weaknesses in all five cybersecurity function areas, and its program, based on OMB metrics, has a low level of maturity. Until STB addresses these deficiencies, the Agency's information systems will be at increased risk of attack or compromise.

Recommendations

To assist STB address the challenges in developing a mature and effective information security program, we recommend that STB continue to address previously identified recommendations[6] and incorporate the following items into their overall information security program:

Risk Management
Recommendation 1: Fully develop and implement a risk management strategy and the supporting procedures for maintaining an accurate system inventory.

Configuration Management
Recommendation 2: Develop a configuration management plan with supporting policies and procedures and ensure that the existing Change Management Charter aligns with the plan.

Identity and Access Management
Recommendation 3: Develop an ICAM strategy to guide its ICAM process and activities, and modify existing identity and access management policies and procedures to adequately address:

1. Processes to request, modify, and revoke privileged and non-privileged access; and
2. Processes to ensure separation of duties within the organization.

[6] An evaluation of the prior year FISMA recommendations is found in Appendix B – Status of Prior Year FISMA Recommendations.

Recommendation 4: Fully implement the use of PIV cards for personnel to access STB's facilities.

Data Protection and Privacy
Recommendation 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.

Incident Response
Recommendation 6: Develop an Incident Response plan in accordance with NIST 800-61, rev. 2.

Recommendation 7: Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.

Appendix A – Scope and Methodology#

DOT OIG tasked Williams Adley with conducing a performance audit of STB's information security programs and practices in accordance with FISMA for the period July 1, 2017 through September 30, 2018[7]. 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. We evaluated security controls for one sampled STB system: STB LAN. Limited procedures were performed related to a sample of STB's cloud solutions (Amazon Web Services, Blackberry AtHoc, Cylance Protect, and Okta Identity as a Service) to determine the status of prior year recommendation number 3.

We performed our audit steps onsite from July 9, 2018 to September 6, 2018. 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 for the Detect and Recover functions as the issues identified within these functions for FY 2018 audit were consistent with those identified in the prior year. Refer to Appendix B – Status of Prior Year Recommendations.

[7] Williams Adley was onsite to conduct audit procedures from July 9, 2018 through September 6, 2018. The results of the FY 2018 audit are as of September 30, 2018.

Appendix B – Status of Prior Year FISMA Recommendations

#	Description of Recommendation	Status
1	Complete implementation of policies and procedures for: a. Risk management, including a risk management plan and assessment; b. System authorization; and c. Plans of actions and milestones.	Open - STB is in the process of defining policies and procedures: a. Open – STB does not have defined policies and procedures for conducting system level risk assessments b. Closed c. Closed
2	Complete the system reauthorization of the STB LAN	Closed.
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.
4	Define specifications and acquire an automated solution to assist with the risk management program.	Open – Although STB has implemented tools to identify system level risks within the Agency, STB does not utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks.
5	Develop policies and procedures for the implementation of an information security architecture.	Open - STB has not defined an information security architecture.
6	Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.	Open - STB's Vulnerability Management procedures do not identify the specific procedures to handle identified vulnerabilities. Additionally, prioritization due to vulnerability rating is not considered within the Vulnerability Management procedures document.
7	Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.	Closed.
8	The STB is modifying its identity and access management policies and procedures to address: 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.	Open – STB is in process of modifying its identity and access management policies: a. Closed. b. Open - Processes for assigning personnel risk designations prior to granting users with access to its systems are not defined. c. Open - STB's access provisioning processes were not operating effectively within the audit period. d. Open - Defined requirements for cryptographic mechanisms, system time-outs, and monitoring of remote access sessions are not defined.

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.
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. Specifically, STB has not developed a security awareness training strategy/plan and its supporting procedures.
11	Modify the training plan to include missing elements such as funding, goals and use of technology.	Open - STB has not finalized its security awareness training program. Specifically, STB has not developed a security awareness training strategy/plan and its supporting procedures.
12	Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.	Open – STB has not developed an overall ISCM strategy and supporting policies and procedures.
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.	Open - STB has updated its procedure document with missing components such as incident detection and analysis; incident prioritization, containment, eradication, and recovery; coordination, information sharing, and reporting; and considerations for major incidents. However, STB's procedure document does not include procedures for incident response training and testing.
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, it needed.	Open - STB has not developed its information system contingency planning program through policies, procedures, and strategies.

Appendix C – Criteria and Guidance

The following NIST guidance, Federal standards, and STB policies were used to evaluate STB's information security program and practices.

I. Risk Management

1. NIST SP 800-39[8] states that 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.
2. NIST SP 800-53, rev. 4,[9] states that an organization develops and documents an inventory of information system components that:
    - Accurately reflects the current information system;
    - Includes all components within the authorization boundary of the information system;
    - Is at the level of granularity deemed necessary for tracking and reporting; and
    - Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability].
3. NIST SP 800-53, rev. 4,[10] states that an organization develops and documents an inventory of information system components that:
    - Accurately reflects the current information system;
    - Includes all components within the authorization boundary of the information system;
    - Is at the level of granularity deemed necessary for tracking and reporting; and
    - Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability].
4. NIST SP 800-53, rev. 4,[11] states that an organization develops and documents an inventory of information system components that:
    - Accurately reflects the current information system;
    - Includes all components within the authorization boundary of the information system;
    - Is at the level of granularity deemed necessary for tracking and reporting; and
    - Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability].
5. NIST SP 800-39 states that to integrate the risk management process throughout the organization, a three-tiered approach is employed that addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities

[8] NIST SP 800-39, AT 14.
[9] NIST SP 800-53, rev. 4, CM-8 Information System Component Inventory
[10] NIST SP 800-53, rev. 4, CM-8 Information System Component Inventory
[11] NIST SP 800-53, rev. 4, CM-8 Information System Component Inventory

and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.

6. NIST SP 800-53, rev. 4[12] states that the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.
7. NIST SP 800-39, Section 2.3.2 states that the risk executive is a functional role established within organizations to provide a more comprehensive, organization-wide approach to risk management. The risk executive (function) serves as the common risk management resource for senior leaders/executives, mission/business owners, chief information officers, chief information security officers, information system owners, common control providers, enterprise architects, information security architects, information systems/security engineers, information system security managers/officers, and any other stakeholders having a vested interest in the mission/business success of organizations.
8. NIST SP 800-53, rev. 4 states that the organization does the following:
   - Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
   - Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
9. NIST SP 800-53, rev. 4[13] states that the organization perform the following:
   - Assigns a senior-level executive or manager as the authorizing official for the information system;
   - Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
   - Updates the security authorization [Assignment: organization-defined frequency].
10. The NIST 800-53 standard further states that managing information security risk requires the involvement of the entire organization defined in three tiers: senior leaders providing the strategic vision and top-level goals and objectives for the organization; bureau leaders planning, executing, and managing projects; and system owners operating the information systems supporting the organization's business functions.
11. NIST SP 800-39, Section 3.4 states that the organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation.

[12] NIST SP 800-53, rev. 4, PM-7 Enterprise Architecture
[13] NIST SP 800-53, rev. 4, CA-6 Security Authorization

II. Configuration Management

1. NIST SP 800-53, rev. 4 CM-9 states following regarding the configuration management plan: The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification. Supplemental Guidance: Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified, and some existing configuration items may no longer need to be under configuration control.
2. NIST SP 800-53, rev. 4 SI-2 states the following regarding flaw remediation: The organization:
    - Identifies, reports, and corrects information system flaws;
    - Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
    - Installs security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process. Supplemental Guidance: Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error

handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures.

3. NIST SP 800-53, rev. 4 RA-5 states the following regarding vulnerabilities: The organization:
    - Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;
    - Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
        - Enumerating platforms, software flaws, and improper configurations;
        - Formatting checklists and test procedures; and
        - Measuring vulnerability impact;
    - Analyzes vulnerability scan reports and results from security control assessments;
        - Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk.
4. NIST SP 800-53, rev. 4 CM-2 states the following regarding baselines configurations: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.
5. NIST SP 800-53, rev. 4 CM-8 states following regarding maintaining a hardware and software inventory: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information

system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency]. Supplemental Guidance: Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.

6. NIST 800-128, rev. 4 Section 2.4 outlines the roles and responsibilities relevant to a security focused configuration management program, including but not limited to the following:
    - Chief Information Security Officer or Senior Information Security Officer;
    - Authorizing Official;
    - Information System Owner; and
    - Information System Administrator.

III. Identity and Access Management

1. The Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance version 2.0 states that "it is critical to identify all stakeholders, and not just those who may be positively affected by the project, in order to understand the needs, responsibilities, and potential impacts of program decisions."
2. NIST SP 800-53, rev. 4[14], states that the organization will develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
    - An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    - Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Furthermore, NIST SP 800-53, rev 4[15], states that the organization will establish and document usage restrictions, configurations/connection requirements, and implementation guidance for each type of remote access allow

3. NIST SP 800-53, rev 4[16], states that the organization will perform the following:
    - Assign a risk designation to all organizational positions;
    - Establish screen criteria for individuals filling those positions; and

[14] NIST SP 800-53, rev. 4, IA-1 Identification and Authentication Policy and Procedures
[15] NIST SP 800-53, rev.4, AC-17 Remote Access
[16] NIST SP 800-53, rev.4, PS-2 Position Risk Designation

- Review and update position risk designations [Assignment: Organization-defined frequency].

4. Homeland Security Presidential Directive-12[17] calls for a "mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."
5. NIST SP 800-53, rev 4[18], states that the organization will perform the following as it relates to account management:
    - Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; and
    - Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts.
6. NIST SP 800-53, rev 4[19], states that the organization will perform the following as it relates to account management:
    - Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; and
    - Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts.
7. NIST SP 800-53, rev 4[20], states that the organization will perform the following as it relates to account management:
   Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions].

IV. Security Training

1. NIST SP 800-53, rev. 4 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.
2. 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.

V. Data Protection and Privacy

[17] Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004#
[18] NIST SP 800-53, rev.4, AC-2 Account Management
[19] NIST SP 800-53, rev.4, AC-2 Account Management
[20] NIST SP 800-53, rev.4, AC-2 Account Management

1. NIST SP 800-122,[21] 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."
2. NIST SP 800-122,[22] 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."
3. NIST SP 800-53, rev. 4,[23] 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. ISCM

1. NIST SP 800-53, rev. 4[24], states that the organization "develops a continuous monitoring strategy and implements a continuous monitoring program."
2. NIST SP 800-53, rev. 4,[25] 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.
3. NIST SP 800-137,[26] states, "[T]he 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."

VII. Incident Response

1. NIST SP 800-61 rev. 2, Computer Security Incident Handling Guide, states "organizations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements, which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:
    - Mission;
    - Strategies and goals;
    - Senior management approval;

[21] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
[22] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
[23] NIST SP 800-53, rev. 4, PE-3 Physical Access Control#
[24] NIST SP 800-53, rev. 4, CA-7 Continuous Monitoring
[25] NIST SP 800-53, rev. 4, CA-1 Security Assessment and Authorization Policy and Procedures
[26] NIST SP 800-137, ISCM for Federal Information Systems and Organizations

- Organizational approach to incident response;
- How the incident response team will communicate with the rest of the organization and with other organizations;
- Metrics for measuring the incident response capability and its effectiveness;
- Roadmap for maturing the incident response capability; and
- How the program fits into the overall organization."

2. NIST SP 800-53, rev. 4,[27] states that the organization will develop an incident response plan that:
   - Provides metrics for measuring the incident response capability within the organization; and
   - Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

   Furthermore, NIST SP 800-61, rev. 2, Section 2.3.1 states that organizational structure and definition of roles, responsibilities, and levels of authority; should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing (e.g., what can be shared with whom, when, and over what channels), and the handoff and escalation points in the incident management process.
3. STB's Incident Response Procedure states that the incident category has to be documented in the incident ticket. Furthermore, STB's security team will categorize the incidents using the categories defined in the Incident Response Procedure.
4. NIST SP 800-53, IR-1, Incident Response Policies and Procedures, requires the organization's policy and procedures to reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.[28] Specifically, US-CERT requires the agencies to utilize the attack vectors taxonomy when sending cybersecurity incident notifications to US-CERT.

VIII. Contingency Planning

1. NIST SP 800-53, rev. 4, [29] 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

[27] NIST SP 800-53, rev. 4, IR-1 Incident Response Policy and Procedures
[28] NIST SP 800-53, rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, April 2013.
[29] NIST SP 800-53, rev. 4, CP-1 Contingency Planning and Procedures

- Contingency planning procedures [Assignment: organization-defined frequency].

2. NIST SP 800-34, rev. 1[30] states that [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.
3. NIST SP 800-34, rev. 1[31] states that the [Business Impact Analysis] is a key step in implementing the [Contingency Planning] controls in NIST SP 800-53 and in the contingency planning process overall. The BIA enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's [Continuity of Operations Plan, Business Continuity Plans, and Disaster Recovery Plan].

[30] NIST SP 800-34, rev. 1, Contingency Planning Guide for Federal Information System
[31] NIST SP 800-34, rev. 1, AT 15.

Appendix D – Management's Response

SURFACE TRANSPORTATION BOARD
Washington, DC 20423

October 15, 2018

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 2018 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) 2018 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 as it helps to ensure that the Board, in its third year as an independent agency, is implementing a cost-effective, risk-based security program that is aligned with the National Institute of Standards and Technology (NIST) security standards and guidelines.

Over the past year, the STB has worked hard to improve its information security program and remains committed to maturing its security processes. The Board has filled the vacancies of the Information Systems Security Manager (ISSM) and Information Systems Security Officer, who have focused their efforts on remediating the FY 2017 FISMA audit recommendations, prioritizing activities that increase the STB's overall security posture. The ISSM and Chief Information Officer (CIO) meet weekly with agency leadership to review progress on these efforts and ensure results are being achieved. Additionally, the STB is now conducting an overall IT assessment to ensure that the structure and strategic focus of its IT group is properly aligned to meet mission needs and security requirements. The STB appreciates that this year's audit recognizes the work that has been done through FY 2018 while providing to the STB a roadmap for continued improvements.

The STB concurs with the seven recommendations in the FY 2018 FISMA audit and acknowledges that there is a significant amount of work ahead to achieve a fully effective information security program. The STB is committed to addressing the recommendations issued in FY 2018, completing its remaining FY 2017 audit recommendations, and advancing to the next security maturation level. Each of the recommendations in the FY 2018 audit and estimated completion dates are discussed below:

FY 2018 Recommendations:

***Risk Management* Recommendation 1:** Fully develop and implement a risk management strategy and the supporting procedures for maintaining an accurate system inventory.

STB Management Response: The STB continues to make steady improvements within its Risk Management Program. The STB has developed a risk management charter, which established the organizational Risk Management Committee, and it has developed risk-related policies. The committee meets at least quarterly to identify organizational risk management decisions. To improve the current risk management capabilities, the STB will fully develop and incorporate a risk management strategy into its existing process. Additionally, the STB will develop procedures for maintaining an authoritative system inventory that will allow the Board to accurately identify system-related risk. The STB expects to complete these tasks by March 31, 2019.

***Configuration Management* Recommendation 2:** Develop a configuration management plan with supporting policies and procedures and ensure that the existing Change Management Charter aligns with the plan.

STB Management Response: The STB continues to make configuration management improvements and is currently implementing an Information Technology Service Management system that will provide governance and automation to the configuration management process. Additionally, the STB has mitigated recently identified configuration management gaps by defining processes to patch third-party software and by implementing a prioritization process that aligns with vulnerability criticality. To enhance its configuration management capability, the STB will develop a configuration management plan and procedures that align with the existing Change Management Charter. The STB expects to complete these tasks by March 31, 2019.

***Identity and Access Management* Recommendation 3:** Develop an ICAM strategy to guide its ICAM process and activities, and modify existing identity and access management policies and procedures to adequately address:

- Processes to request, modify, and revoke privileged and non-privileged access; and
- Processes to ensure separation of duties within the organization.

STB Response: The STB is committed to developing a comprehensive Identity, Credential, and Access Management (ICAM) program. The STB is currently implementing certificate-based authentication for mobile devices, increasing the level of assurance that the right individuals are accessing the right STB data. As a part of the comprehensive program, the STB will develop an ICAM strategy to guide its ICAM process and activities, including procedures that address the request, modification, and revocation of privileged and non-privileged access. Additionally, the STB will implement processes to ensure separation of duties within the organization. The STB expects to complete these tasks by September 30, 2019.

***Identity and Access Management* Recommendation 4:** Fully implement the use of PIV cards for personnel to access STB's facilities.

STB Response: The STB currently issues Personal Identification Verification (PIV) cards to all STB personnel and leverages the cards as the authenticator for logical (system) access. To further enhance PIV capabilities, the STB expects to fully implement the use of PIV for personnel access to STB facilities. This PIV implementation will take place as a part of the STB's new headquarters lease and the accompanying construction required to reduce its footprint. Once construction is completed, STB personnel will use PIV as the authenticator for access to STB facilities. The STB expects to complete these tasks by September 30, 2019.

Data Protection and Privacy **Recommendation 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.

STB Response: The STB is making progress toward developing a comprehensive privacy program, including preparing a privacy program plan and related policies and procedures. Implementation of the STB's privacy plan will add the necessary data protection and privacy controls for personally identifiable information that the STB collects, uses, maintains, shares, and disposes of through the STB's information systems. The STB has also begun defining employee roles and responsibilities for performing data exfiltration exercises. The STB expects to complete these tasks by September 30, 2019.

Incident Response **Recommendation 6:** Develop an Incident Response plan in accordance with NIST 800-61, rev. 2.

STB Response: The STB has implemented Incident Response policies and procedures that outline steps for containment, eradication, and recovery from security events. These documents also include information on how to categorize, prioritize, and escalate security events within the organization and externally, in coordination with other government entities such as the United States – Computer Emergency Response Team (US-CERT). To mature its Incident Response capability, the STB will develop an Incident Response plan in accordance with NIST 800-61, rev. 2, and incorporate that plan into its existing Incident Response process. The STB expects to complete these tasks by January 31, 2019.

Incident Response **Recommendation 7:** Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.

STB Response: The STB will modify its Incident Response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT. The STB expects to complete these tasks by January 31, 2019.

FY17 FISMA Audit Recommendations:

Since its FY 2017 FISMA audit, the STB has strategically moved forward with the operational implementation of technical security controls, thereby reducing the attack surface and increasing the STB's overall information security posture. As the technical implementation wraps up, the

STB is able to provide increased attention to its control policies and procedures that align with the strategic mission of the Board. The STB is committed to completing these prior year recommendations through the development of strategy and process documentation and improvements that align with its strategic mission. The Board plans to addresses the outstanding FY 2017 recommendations, as follows:

Recommendation 1: The STB has completed the development of its Risk Management policy and charter and continues to make improvements to its Risk Management Program. The Risk Management Committee, which consist of senior leadership, was established to make organizational risk-based decisions. Additionally, the STB has completed its Authority to Operate for its six information systems and has developed and incorporated Plans of Actions and Milestones into its risk management process. To improve the current risk management capabilities, the STB will formally define polices and/or procedures for conducting system level risk assessments. The STB expects to complete this task by March 31, 2019.

Recommendation 4: The STB has acquired and completed initial configuration of automated information systems that assist with the organizational risk management program. These systems include: a vulnerability management system that identifies security vulnerabilities within information systems; a log-event management system that triggers automated notifications of suspicious activity events through the monitoring of system logs; and an intrusion detection system that monitors the network for malicious activity and policy violations. Deployment of these tools is the core of the STB's continuous monitoring capability and allows the STB to review up-to-date analytics that can assist with organizational risk management decisions. The STB will document and formalize this process within its existing risk management process. The STB expects to complete these tasks by March 31, 2019.

Recommendation 5: The STB is in the process of finalizing its Information Security Architecture, which is currently in draft. In support of the architecture, the STB has finalized 22 security related polices that are subcomponents to its structure. The STB expects to complete these tasks by December 31, 2018.

Recommendation 6: The STB has completed the development of policies and procedures that give it the ability to identify, report, and resolve information systems flaws and facilitate timely security patch installation. In addition, the STB has implemented a vulnerability management system that has the capability to detect, report, and show remediation of system flaws and applicable security patches. Scans, both agent-based and discovery-based, are initiated daily to detect flaws and applicable security patches to be remediated. Remediation reports are sent to the CIO and Authorizing Official on a weekly basis. The remediation reports are also used by system administrators to identify and apply applicable security updates to information systems. The STB will formalize the vulnerability management process and ensure that prioritization based on vulnerability rating is outlined within its vulnerability management procedures. The STB expects to complete these tasks by December 31, 2018.

Recommendation 8: The STB has made progress in modifying its identity and access management policies and procedures. The STB is in the process of completing documentation

with respect to personnel risk designations and testing regarding remote access. The STB has also established Rules of Conduct for individuals with system access that have been signed by all system users. With respect to its ICAM program, the STB is completing its current and future state documentation, as well as ensuring that its transition plan is accurate given the STB's new lease and construction (during FY 2019) with revised security protocols. The STB expects to complete these tasks by December 31, 2018.

Recommendation 9: The STB has taken steps to improve its security training program by developing a security awareness policy and ensuring that all STB personnel completed annual security awareness training for FY 2018. The STB will conduct a needs assessment to evaluate skills, knowledge, and abilities of its workforce, to determine its awareness and training needs. The STB expects to complete this task by May 31, 2019.

Recommendation 10: Although the STB has implemented a security training program and provides annual security training through its shared service learning management system, it also needs to develop a process for measuring the effectiveness of its security awareness and training program. The STB will implement a process to evaluate the effectiveness of its established security training program. The STB expects to complete this task by May 31, 2019.

Recommendation 11: The STB has reviewed its training program and will modify its training plan to including missing elements such as funding, goals, and use of technology. The STB expects to complete this task by May 31, 2019.

Recommendation 12: The STB has made significant progress in 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 STB has implemented a log-event management system that triggers automated notifications during suspicious activity events through the monitoring of system logs. The STB has also implemented an intrusion detection system that monitors the network for malicious activity and policy violations. Deployment of these tools are the core of the STB's continuous monitoring capability and will allow the STB to review up-to-date analytics that assist with organizational risk management decisions. In March 2018, the STB began to coordinate with the Department of Homeland Security to implement several security-related tools through the Continuous Diagnostics and Mitigation program, which gives the STB additional continuous monitoring capabilities. The ISCM program strategy is currently in draft. The STB expects to complete these tasks by December 31, 2018.

Recommendation 13: The STB has developed the Incident Response Policy and Incident Response Procedure (IRP) documents that establish the incident response process for the organization. The IRP outlines steps for containment, eradication, and recovery from security events. These documents include information on how to categorize, prioritize, and escalate security events within the organization and externally, in coordination with other government entities such as US-CERT. Additionally, Einstein 3 Accelerated (E3A) capability is operational within the STB and incorporated into the STB's Managed Trusted Internet Protocol Service solution. E3A provides a common baseline of security practices across the federal executive

branch and assists the STB with managing its cyber risk. The STB will incorporate processes for incident response training and testing into its current IRP. The STB expects to complete these tasks by December 31, 2018.

Recommendation 14: The STB is making progress on its contingency planning. The STB has finalized its high-level contingency policies and is developing its Business Impact Analysis documents, which will drive the identification of mission critical functions, ensuring that these critical functions and their correlated information systems are prioritized and operational in a contingency scenario. The STB has reviewed its existing materials and is examining best practices for contingency planning policies, with the goal of establishing a thorough and compliant plan, including testing. The STB expects to complete these tasks by March 31, 2019.

Sincerely,

RACHEL CAMPBELL Digitally signed by RACHEL CAMPBELL Date: 2018.10.15 12:29:41 -04'00'

Rachel D. Campbell
Managing Director
Surface Transportation Board
rachel.campbell@stb.gov
202-245-0357

U.S. DOT OIG

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