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

QC2022001 | October 4, 2021

What We Looked At
The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to implement information security programs. FISMA also requires agencies to have annual independent evaluations performed to determine the effectiveness of their programs and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, the Surface Transportation Board (STB) requested that we perform its fiscal year 2021 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 27 recommendations.
The Honorable Martin J. Oberman  
Chairman, Surface Transportation Board  
395 E Street, SW  
Washington, DC 20423-0001

Dear Mr. Oberman:

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

The Federal Information Security Modernization Act of 2014¹ (FISMA) requires agencies to implement information security programs. The act also requires agencies to have annual independent evaluations performed to determine the effectiveness of their programs and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, STB requested that we perform its fiscal year 2021 FISMA review. Williams Adley & Company-DC LLP (Williams Adley) of Washington, DC, completed the audit of STB’s information security program and practices (see attachment) under contract with the Office of Inspector General.

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

Williams Adley found that STB’s information security program and practices were not effective. Williams Adley made the following 27 recommendations to improve STB’s information security program and practices.

1. Develop an enterprise architecture that includes information security considerations and the resulting risk to the Agency, as well as incorporates STB’s existing cyber security architecture.

2. Identify and define all software programs that are not authorized to execute on STB information systems.

¹ Pub. L. No. 113-283.
3. Establish and implement procedure to manage hardware asset inventory connected to STB’s network.

4. Review all open Plan of Actions & Milestones (POA&M) and assign scheduled completion dates which account for the required resources and corrective actions, including milestones, to manage and mitigate the identified risk.

5. Develop a Supply Chain Risk Management (SCRM) strategy and supporting policies and procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain risk management requirements.

6. Develop a process to make improvements to its baseline configuration, secure configuration, and flaw remediation policies and procedures through the use of lessons learned.

7. Implement documented processes for configuration management changes as required by STB policies and procedures.

8. Evaluate deviations from Center for Internet Security (CIS) benchmarks and determine if the associated configurations should align with best practices or if deviations should be risk accepted.

9. Update vulnerability management procedures to support implementation of STB’s Vulnerability Disclosure Policy (VDP).

10. Update the Access Recertification Process document to align with STB’s existing practices to ensure users complete all required training and onboarding forms.

11. Define the Identity and Access Management policies and procedures for user monitoring program within STB Identity, Credential, and Access Management (ICAM) plan.

12. Develop a process to make improvements to the effectiveness of its ICAM policy, strategy, and road map.

13. Define procedures to review and remove unnecessary Personally Identifiable Information (PII) collection on an organization defined frequency.

14. Perform the review of Privacy Threshold Analysis (PTA) for STB General Support System (GSS), At Hoc, and Dynamic Case Management system on an annual basis.
15. Implement data protection policies and procedures for Data at Rest, prevention and detection of untrusted removable media, and destruction or reuse of media containing PII or other sensitive agency data.

16. Address the knowledge, skills, and abilities gaps identified during the fiscal year 2020 skill gap assessment through training or talent acquisition.

17. Complete the transition from traditional three (3) year authorizations to ongoing authorizations for STB-Local Area Network (LAN).

18. Implement documented processes for collecting and reporting performance metrics at the organization and system level to assess the effectiveness of Information Security Continuous Monitoring (ISCM) program.

19. Develop a process to make improvements to the effectiveness of its ISCM program through the collection and reporting of quantitative and qualitative performance metrics, and lessons learned.

20. Define the performance metrics for measuring the incident response capability.

21. Update STB Incident Response Plan to include requirements for the technologies utilized to support Incident Response processes.

22. Define the frequency for the performance of Post Incident activities.

23. Update STB Incident Response plan containment strategies to reflect the current agencies risk prioritization processes.

24. Implement documented processes for Incident Response resolutions of tickets in consistent manner, as required by STB policies and procedures.

25. Define the frequency for the performance of system level Business Impact Analyses (BIA).

26. Review the organization wide BIA on an annual basis.

27. Conduct a tabletop exercise of the General Support System (GSS)’s information system contingency plan (ISCP) on an annual basis.

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

Kevin Dorsey
Assistant Inspector General for
Information Technology Audits

cc: STB Audit Liaison

Attachment
Quality Control Review

We performed a quality control review (QCR) of Williams Adley’s report, dated August 27, 2021 (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement and performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on STB’s information security program and practices. Williams Adley is responsible for its independent auditor’s report and the conclusions expressed in that report. Our QCR disclosed no instances in which Williams Adley did not comply, in all material respects, with generally accepted Government auditing standards.

Agency Comments and OIG Response

On July 30, 2021, Williams Adley provided STB with its draft report and received STB’s response on August 20, 2021, which is included in its entirety in the attached independent auditor’s report.

STB concurred with all 27 of Williams Adley’s recommendations, and provided appropriate planned actions and estimated completion dates.

Actions Required

We consider all 27 of Williams Adley’s recommendations resolved but open pending completions of planned actions.
### Exhibit. List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>CIS</td>
<td>Center for Internet Security</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Modernization Act</td>
</tr>
<tr>
<td>GSS</td>
<td>General Support System</td>
</tr>
<tr>
<td>ICAM</td>
<td>Identity, Credential, and Access Management</td>
</tr>
<tr>
<td>ISCM</td>
<td>Information Security Continuous Monitoring</td>
</tr>
<tr>
<td>ISCP</td>
<td>Information System Contingency Plan</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>POA&amp;M</td>
<td>Plan of Actions and Milestones</td>
</tr>
<tr>
<td>PTA</td>
<td>Privacy Threshold Analysis</td>
</tr>
<tr>
<td>QCR</td>
<td>Quality Control Review</td>
</tr>
<tr>
<td>SCRM</td>
<td>Supply Chain Risk Management</td>
</tr>
<tr>
<td>STB</td>
<td>Surface Transportation Board</td>
</tr>
<tr>
<td>VDP</td>
<td>Vulnerability Disclosure Policy</td>
</tr>
</tbody>
</table>
Attachment. Independent Auditor’s Report

August 27, 2021
Contents
Results in Brief ........................................................................................................................................ 1
Background ............................................................................................................................................. 1
Results of the FY 2021 FISMA Audit .................................................................................................. 4
  I. Identify ............................................................................................................................................. 4
  II. Protect .......................................................................................................................................... 6
  III. Detect .......................................................................................................................................... 9
  IV. Respond ..................................................................................................................................... 10
  V. Recover .................................................................................................................................... 11
Conclusion .......................................................................................................................................... 12
Recommendations .............................................................................................................................. 12
Appendix A – Scope and Methodology .............................................................................................. 15
Appendix B – Status of Prior Year FISMA Recommendations ............................................................ 16
Appendix C – Criteria and Guidance .................................................................................................. 19
Appendix D – Management’s Response .............................................................................................. 24
Mr. Kevin Dorsey  
Assistant Inspector General for Information Technology Audits  
1200 New Jersey Avenue, SE  
Washington, DC 20590

Dear Mr. Dorsey:

We are pleased to provide our report outlining the result of the performance audit conducted to evaluate the effectiveness of the Surface Transportation Board (STB)’s information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year (FY) 2021 audit.

FISMA requires each executive branch agency Inspector General, or an independent external auditor, to conduct an annual evaluation of their agency’s information security program and practices, and to report to the Office of Management and Budget (OMB) on the results of their evaluations. OMB Memorandum M-21-02 (“Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements”) provides instructions for meeting FY 2021 reporting requirements.

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. Based on our audit procedures, the STB has made improvements to its overall information security program but has not met the requirements outlined within the FY 2021 FISMA reporting metrics to be operating at an effective level of security.

We have made recommendations related to the challenges faced by the STB that, if effectively addressed by STB management, should strengthen the STB’s information security program. STB management has provided us with a response to this FY 2021 FISMA audit report. Their response is presented in its entirety in the Management’s Response section of the report. We did not audit management’s response and, accordingly, do not express any assurance on it.

August 27, 2021
Results in Brief

Office of Management and Budget (OMB) requires independent auditors to annually assess metrics across five (5) security function areas to determine the maturity level of the Surface Transportation Board (STB)’s information security program. Program maturity was assessed at one (1) of five (5) levels as defined by OMB - Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized. Appendix A within this report outlines the audit scope and methodology followed to perform the FY 2021 audit.

Based on the audit procedures performed, we concluded that STB made improvement to its information security program. However, within the context of the Federal Information Security Modernization Act of 2014 (FISMA) reporting metrics, STB’s information security program remains ineffective.\(^1\) Although STB’s information security program was deemed ineffective for FY 2021, STB made progress in maturing its overall information security program by addressing all eight (8) prior year recommendations\(^2\) and improving the maturity level of the Data Protection and Privacy, Security Training, and Information Security Continuous Monitoring (ISCM) domains, as outlined in the table below.

<table>
<thead>
<tr>
<th>FISMA Function</th>
<th>FISMA Domain</th>
<th>FY 2021 Maturity Rating</th>
<th>FY 2020 Maturity Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify(^3)</td>
<td>Risk Management</td>
<td>Level 2 - Defined</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Protect</td>
<td>Configuration Management</td>
<td>Level 2 - Defined</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Protect</td>
<td>Identity and Access Management</td>
<td>Level 2 - Defined</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Protect</td>
<td>Data Protection and Privacy</td>
<td>Level 3 – Consistently Implemented</td>
<td>Level 1 – Ad-Hoc</td>
</tr>
<tr>
<td>Protect</td>
<td>Security Training</td>
<td>Level 2 - Defined</td>
<td>Level 1 – Ad-Hoc</td>
</tr>
<tr>
<td>Detect</td>
<td>ISCM</td>
<td>Level 2 - Defined</td>
<td>Level 1 – Ad-Hoc</td>
</tr>
<tr>
<td>Respond</td>
<td>Incident Response</td>
<td>Level 2 - Defined</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Recover</td>
<td>Contingency Planning</td>
<td>Level 2 - Defined</td>
<td>Level 2 – Defined</td>
</tr>
</tbody>
</table>

Table 1 - FY 2021 and FY 2020 FISMA Maturity Ratings

Based on the results of the FY 2021 audit procedures, Williams Adley issued 27 new recommendations to support STB’s efforts to mature its information security program and processes. To supplement the content within this report, an overview of the criteria and guidance supporting the FY 2021 audit are outlined in Appendix C and management’s response to the results of the FY 2021 audit are outlined in Appendix D.

Background

STB is an independent, adjudicatory body that, until passage of the Surface Transportation Board Reauthorization Act in December 2015, was within the oversight of the DOT. While part of DOT, STB shared an information security program with DOT and its Operating Administrations.

---

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

\(^2\) The status of previously issued recommendations are found in Appendix B.

\(^3\) As instructed within the FY 2021 FISMA reporting metrics, the Supply Chain Risk Management domain will not be scored for purposes of the FY 2021 FISMA audit.
As a stand-alone agency, STB is responsible for maintaining its own information security program and independently meeting FISMA’s requirements. Under FISMA, each Federal agency must protect the information and information systems that support its operations, including those provided or managed by other agencies, entities, or contractors. Furthermore, FISMA requires each agency to report annually to OMB, Congress, and the Government Accountability Office (GAO) on the effectiveness of its information security policies, procedures, and practices.

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 2021, OMB and Department of Homeland Security (DHS), in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and the Federal Chief Information Officer Council (FCIOC), revised the metrics to include additional focus areas to support federal agencies information security program. Specifically:

- The introduction of a new domain, Supply Chain Risk Management (SCRM), within the Identify function which focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain risk management requirements; and
- The introduction of a new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy (VDP) as part of their vulnerability management program for internet-accessible federal systems.

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.

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Maturity Level Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Ad-hoc</td>
<td>Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.</td>
</tr>
<tr>
<td>Level 2: Defined</td>
<td>Policies, procedures, and strategies are formalized and documented but not consistently implemented.</td>
</tr>
<tr>
<td>Level 3: Consistently Implemented</td>
<td>Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.</td>
</tr>
<tr>
<td>Level 4: Managed and Measureable</td>
<td>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.</td>
</tr>
<tr>
<td>Level 5: Optimized</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 2 - FY 2021 IG Evaluation Maturity Levels, Source: DHS

Since the FY 2017 FISMA reporting process, Inspector Generals (IGs) were directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most
frequent level (i.e., the mode) across the questions served as the domain rating. With the same logic applied at the function and overall information security program level.

Starting with the FY 2021 FISMA reporting process, IGs are directed to utilize a pilot concept of weighting specific FISMA metrics for assessment and scoring. Within the FY 2021 FISMA reporting metrics, ten (10) priority metrics were identified, as shown in Table 3 below. As part of the proposed weighted average approach to scoring, these priority metrics would be weighted twice as much in the maturity calculation.

![Table 3: Proposed Priority Metrics](image)

According to the FY 2021 FISMA reporting metrics, “the overall maturity of the agency’s information security program would be calculated based on the average rating of the individual function areas (Identify, Protect, Detect, Respond, and Recover). For example, if the weighted average maturity of two of the function areas is Level 3 – Consistently Implemented, and Level 4 – Managed and Measurable for the remaining three areas, then the information security program rating (average of 3.60) would be Level 4 – Managed and Measurable.” Furthermore, “this same approach would be used for all domains and function areas.”
Results of the FY 2021 FISMA Audit

I. Identify

The Identify function, supported by the Risk Management and Supply Chain Risk Management domains, was rated at a Level 2 maturity (Defined). Table 4 below summarizes the ratings of each domain.

<table>
<thead>
<tr>
<th>FISMA Domain</th>
<th>Rating in FY 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 4 – Ratings for Domains within the Identify Function

Risk Management

Williams Adley identified the following issues within the Risk Management IG FISMA metric domain:

- **Condition 1:** STB has not developed an enterprise architecture that includes information security considerations and the resulting risk to the Agency, as well as incorporates STB’s existing cyber security architecture.
- **Condition 2:** STB has not identified and documented all software programs that are not authorized to execute on its information systems.
- **Condition 3:** STB has not defined its procedures to provide oversight over the management of hardware assets connected to STB network by third party agency, DOT.
- **Condition 4:** STB has 63 critical open Plan of Action and Milestones (POA&Ms) and 171 high open POA&Ms with no scheduled completion dates.

Per discussion with STB management, each identified issue above has its own root cause:

- **Condition 1:** STB took an alternative approach to develop a structured methodology for managing risk across the three organization tiers (Tier I - Organization, Tier II - Business Process, and Tier III – Information Systems) by starting with the cyber security architecture and not the enterprise architecture.
- **Condition 2:** Per discussion with STB management, the agency has taken a phased approach to address FISMA requirements and related complex cyber security challenges. Due to limited resources to operate the information security program, the agency is still working to define risk management process.
- **Condition 3:** Per discussion with STB management, it was determined that the agency relies on the DOT’s processes for managing its hardware assets and has not developed its own guidance and requirements for maintaining and updating its hardware inventory.

---

4 The criteria used to support the conditions found within the FY 2021 audit are found in Appendix C – Criteria and Guidance.

5 As instructed within the FY 2021 FISMA reporting metrics, the Supply Chain Risk Management domain will not be scored for purposes of the FY 2021 FISMA audit.
• **Condition 4:** Per discussion with STB management, the agency has not prioritized the remediation of open POA&M's due to lack of resources needed for the activity and a focus on defining risk management process.

Each of the identified issues presents a different impact on the STB’s ability to manage and mitigate risk across the organization. Specifically:

• **Condition 1:** The lack of a defined current and target state enterprise architecture may foster inconsistent management of risk across the organization, ultimately impacting STB’s mission success.
• **Condition 2:** Without a defined and implemented blacklist, STB cannot easily block known malicious software from being installed on workstations and servers.
• **Condition 3:** Without a defined process to maintain an accurate hardware inventory and utilize its standard data elements/taxonomy, STB is unable to track, manage, and protect the physical components within the boundaries of its information systems.
• **Condition 4:** Without assigning scheduled completion dates for critical and high open POA&M’s, STB cannot effectively manage and mitigate organizational risk in a timely manner.

Williams Adley issued four (4) new recommendations in FY 2021 (Recommendation 2021-01, 2021-02, 2021-03, and 2021-04) to addresses the issues and root causes identified.

**Supply Chain Risk Management**

Per discussion with STB management, the agency is still in process of developing the foundation of its SCRM program. Specifically:

• **Condition 5:** STB has not defined and communicated an organization wide SCRM strategy.
• **Condition 6:** STB has not defined and communicated its SCRM policies, procedures, and processes.
• **Condition 7:** STB has not defined and communicated policies, procedures, and processes to ensure that [STB defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.
• **Condition 8:** STB has not defined and communicated its component authenticity policies and procedures.

The foundational components of STB’s SCRM program are still in progress as the agency’s existing cybersecurity program and its supporting plans, policies, and procedures are based on the requirements outlined within National Institute of Standards and Technology (NIST) 800-53, revision (rev) 4. The agency is in progress of updating its cybersecurity program to align with the requirements outlined in NIST 800-53, rev 5.

The delay in defining and implementing an SCRM program may result in unknown risks being introduced by new or existing products, system components, systems, and services of external providers.
Williams Adley issued one (1) new recommendation in FY 2021 (Recommendation 2021-5) to addresses the issues and root cause identified.

**II. Protect**

The Protect function, supported by the Configuration Management, Identity and Access Management, Security Training, and Data Protection and Privacy domains, was rated at a Level 2 maturity (Defined). Table 5 below summarizes the ratings of each domain.

<table>
<thead>
<tr>
<th>FISMA Domain</th>
<th>Rating in FY 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Management</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>Level 2 – Defined</td>
</tr>
<tr>
<td>Data Protection and Privacy</td>
<td>Level 3 – Consistently Implemented</td>
</tr>
<tr>
<td>Security Training</td>
<td>Level 2 – Defined</td>
</tr>
</tbody>
</table>

**Table 5 – Ratings for Domains within the Protect Function**

*Configuration Management*

Williams Adley identified the following issues within the Configuration Management IG FISMA metric domain:

- **Condition 9:** STB has not utilized lessons learned to make improvements to its baseline configuration, secure configuration, and flaw remediation policies and procedures.
- **Condition 10:** For one (1) out of two (2) emergency changes samples, the system owner did not review and accept the change.
- **Condition 11:** For all three (3) standard changes samples, documentation was not maintained to demonstrate testing performed and Change Advisory Board (CAB) approval prior to implementation.
- **Condition 12:** STB Local Area Network (LAN) General Support System is not configured to meet CIS Benchmarks Guidelines. Specifically, 23 deviations were identified due to either baseline configurations not being configured or implemented correctly.
- **Condition 13:** STB has not updated internal vulnerability management procedures to support implementation of their VDP.

Per discussion with STB management, two circumstances were identified as the root causes for the configuration management issues identified:

- **Condition 9:** Due to limited resources and the impact of COVID-19 pandemic on overall operations, STB has not developed a process to make improvements to its baseline configuration, secure configuration, and flaw remediation policies and procedures through the use of lessons learned.
- **Conditions 10-13:** STB Management has not dedicated the resources required to adequately develop, document, and implement adequate CM processes.

Each of the identified issues presents a different impact on the STB’s ability to manage and mitigate risk across the organization. Specifically:
- **Condition 9:** Without a process to continuously evaluate the implementation of existing policies and procedures, STB management runs the risk of repeating mistakes or process inefficiencies.

- **Condition 10:** Without approval and/or review of an emergency change after implementation, the STB cannot ensure that the original issue identified, and its associated risk were appropriately remediated.

- **Condition 11:** Without appropriate testing a standard change prior to implementation into the production environment, the STB may unknowingly introduce changes to functionality that impacts operations and risk to the system environment.

- **Condition 12:** Without appropriate implementation of CIS benchmarks, STB has not met the security best practices to reduce its overall exposure to cyber security attacks.

- **Condition 13:** Without appropriate guidance on how to manage vulnerabilities identified by the public, STB cannot utilize the experience and knowledge of ethical hackers to improve its overall information security posture.

Williams Adley issued four (4) new recommendations in FY 2021 (Recommendation 2021-06, 2021-07, 2021-08, and 2021-09) to addresses the issues and root causes identified.

*Identity and Access Management*

Williams Adley identified the following issues within the Identity and Access Management IG FISMA metric domain:

- **Condition 14:** STB’s Access Recertification Process document does not reflect the agency’s existing practices to ensure users complete all required training and onboarding forms.

- **Condition 15:** STB has not fully defined procedures for their user monitoring program.

- **Condition 16:** STB has not utilized lessons learned to make improvements to the effectiveness of its Identity, Credential, and Access Management (ICAM) policy, strategy, and road map.

Per discussion with STB management, each identified issue above has its own root cause:

- **Condition 14:** Per discussion with STB management, the agency’s existing practices were developed and implemented this year to address the potential of human error identified when performing the documented process. In addition, STB Management has not dedicated the appropriate resources to develop all the aspects of FICAM’s segment architecture.

- **Conditions 15 and 16:** Per discussion with STB management, the agency focused on defining and implementing other identify and access management activities.

Each of the identified issues presents a different impact on the STB’s identity and access management program. Specifically:

- **Condition 14:** Without clear instructions to perform access recertifications, STB risks inconsistent implementation of the detective control created and used to identify incomplete training and onboarding forms for users with access to its systems.
• **Condition 15:** Without automated audit logging, the agency does not have detective control in place to identify instances where account creation, modification, enabling, disabling, and removal activities were circumvented.

• **Condition 16:** Without a process to continuously evaluate the implementation of existing policies and procedures, STB management runs the risk of repeating mistakes or process inefficiencies.

Williams Adley issued three (3) new recommendations in FY 2021 (Recommendation 2021-10, 2021-11, and 2021-12) to addresses the issues and root causes identified.

**Data Protection and Privacy**

Williams Adley identified the following issues within the Data Protection and Privacy IG FISMA metric domain:

• **Condition 17:** STB has not defined procedures to review and remove unnecessary Personally Identifiable Information (PII) collection on a regular basis.

• **Condition 18:** STB did not perform its annual review of the Privacy Threshold Assessments (PTAs) for STB GSS, At Hoc, and Dynamic Case Management system1.

• **Condition 19:** STB has not implemented security controls for, (i) prevention and detection of untrusted removable media, (ii) destruction or reuse of media containing PII or other sensitive agency data, and (iii) data at rest.

Per discussion with STB management, due to limited resources and the impact of COVID-19 pandemic on overall operations, the agency focused on other priorities to start establishing its privacy program.

Each of the identified issues presents a different impact on the STB’s data protection and privacy program. Specifically:

• **Condition 17:** Without a defined process to continuously review and remove unnecessary PII, STB increases the likelihood of harm caused by a breach involving PII it uses, collects, and stores. An organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization ‘s business purpose and mission.

• **Condition 18:** By not reviewing system PTAs annually as required, STB increases the likelihood of not complying with privacy requirements that apply to its information systems. Furthermore, the periodic review offers STB with an opportunity to identify the types of PII captured by its information systems.

• **Condition 19:** Limited resources continue to make it difficult to implement procedures for the (i) use of FIPS-validated encryption of PII and other agency sensitive data for data (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

Williams Adley issued three (3) new recommendations in FY 2021 (Recommendation 2021-13, 2021-14, and 2021-15) to addresses the issues and root causes identified.

*Security Training*
Williams Adley identified one issue within the Security Training IG FISMA metric domain; Specifically:

- **Condition 20**: STB has not completed its remediation efforts to address the gaps identified as a part of its FY 2020 skill gap assessment.

Per discussion with STB management, due to limited resources and the impact of COVID-19 pandemic on overall operations, the agency focused on other priorities related to its security training program.

Without adequate training for those responsible for supporting STB’s overall information security program, the agency exposes itself to increased levels of risk due to improper implementation of agency- defined policies and procedures and not adequately understanding the domains outlined within the Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

Williams Adley issued one (1) new recommendation in FY 2021 (Recommendation 2021-16) to addresses the issues and root cause identified.

**III. Detect**

The Detect function, supported by the ISCM domain, was rated at a Level 2 maturity (Defined).

*Information Security Continuous Monitoring*

Williams Adley identified the following issues within the ISCM IG FISMA metric domain:

- **Condition 21**: STB did not perform ongoing security control assessments (ongoing authorization) for one (1) of ten (10) information systems, STB-LAN General Support System (GSS).
- **Condition 22**: STB is not collecting, and reporting data related to quantitative and qualitative performance metrics at the organizational and system level that are used to assess the effectiveness of its ISCM program.
- **Condition 23**: STB has not consistently captured lessons learned to make improvements to the ISCM program.

Per discussion with STB management, each identified issue above has its own root cause:

- **Condition 21**: STB will transition from traditional three (3) year authorizations to ongoing authorizations as it works towards implementing National Institute of Standards and Technology (NIST) 800-53 rev. 5.
- **Condition 22**: Per discussion with STB management, the agency has not established how they will use technology to capture performance measures for analysis due to the prioritization of its limited resources and the impact of COVID-19 pandemic on overall operations.
• **Condition 23:** Per discussion with STB management, the agency has not developed a process to continuously make improvements to its ISCM policies and strategy due to limited resources and the impact of COVID-19 pandemic on overall operations.

Each of the identified issues presents a different impact on the STB’s ISCM program. Specifically:

• **Condition 21:** By not transitioning to ongoing authorization for STB-LAN, the agency does not 1) monitor risk posture in a timely manner and 2) benefit from the efficient and cost-effective processes for monitoring risk posture.

• **Condition 22:** Without defined performance metrics and a process to consistently evaluate its ISCM program, STB cannot identify potential areas for improvement and determine whether the ISCM program is meeting desired objectives.

• **Condition 23:** Without a process to continuously evaluate the implementation of existing policies and procedures, STB management runs the risk of repeating mistakes or process inefficiencies.

Williams Adley issued three (3) new recommendations in FY 2021 (Recommendation 2021-17, 2021-18, and 2021-19) to addresses the issues and root causes identified.

**IV. Respond**

The Respond function, supported by the Incident Response domain, was rated at a Level 2 maturity (Defined).

*Incident Response*

Williams Adley identified the following issues within the Incident Response IG FISMA metric domain:

• **Condition 24:** STB has not defined performance metrics for measuring the incident response capability.

• **Condition 25:** STB has not defined its requirements for the use of technologies to support its incident response activities.

• **Condition 26:** STB has not defined the timeframe in which Post Incident Activities need to be performed.

• **Condition 27:** STB’s containment strategies do not reflect the agency’s incident prioritization process.

• **Condition 28:** STB has not consistently implemented its Incident Response processes for two sampled Incidents:
  
  o For incident INC-FY2021-000001:
    • STB did not identify the functional impact to the organization and recoverability of the incident; and
    • STB did not prioritize the Incident based on the classification level.

  o For incident INC-FY2021-000007:
    • STB did not define recoverability of the incidents within SharePoint; and
    • STB did not prioritize the Incident based on the classification level.
Per discussion with STB management, each identified issue above has its own root cause:

- **Condition 24:** Per discussion with STB management, the creation of defined performance metrics was not considered during the development of its incident response plan, policies, and procedures.
- **Condition 25:** Per discussion with STB management, the agency has not finalized its strategy for how technology will be used to support its incident response activities due to limited resources available to support the agency’s incident response program.

**Conditions 26-28:** Per discussion with STB management, the agency has not finalized how containment and post incident activities are designed and support the overall incident response program due to limited resources available to support the agency’s incident response program. Each of the identified issues presents a different impact on the STB’s Incident Response program. Specifically:

- **Condition 24:** Without defined performance metrics and a process to consistently evaluate its incident response program, STB cannot identify potential areas for improvement and determine whether the incident response program is meeting desired objectives.
- **Condition 25:** Without clear requirements for the use of technology, the agency cannot ensure that its existing technology is interoperable to the extent practicable, covers all components of the organization’s network, and are configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, plans, and procedures.
- **Condition 26:** Without a clear timeframe to conduct post incident activities, the agency may lose important information to improve its existing incident response activities.
- **Conditions 27-28:** Without clearly defined processes for incident prioritization, the agency may not execute the appropriate steps to address high risk incidents, including coordinating with external parties such as US-CERT and law enforcement, and communicating data breaches to the public.

Williams Adley issued five (5) new recommendations in FY 2021 (Recommendation 2021-20, 2021-21, 2021-22, 2021-23, and 2021-24) to addresses the issues and root causes identified.

V. Recover

The Recover function, supported by the Contingency Planning domain, was rated at a Level 2 maturity (Defined).

*Contingency Planning*

Williams Adley identified the following issues within the Contingency Planning IG FISMA metric domain:

- **Condition 29:** STB has not defined a frequency for the performance of system level Business Impact Analysis (BIA).
- **Condition 30**: STB has not conducted annual review of its organization wide BIA since 2019.
- **Condition 31**: STB did not conduct a yearly tabletop exercise of the GSS’s information system contingency plan (ISCP).

Per discussion with STB management, the COVID-19 pandemic had a significant impact on overall operations, including the execution of contingency planning activities.

Each of the identified issues presents a different impact on the STB’s Contingency Planning program. Specifically:

- **Conditions 29-30**: BIAs are a point in time assessment and agencies should reassess how systems support critical mission/business processes and services provided, and the consequences of a disruption.
- **Condition 31**: Without routinely testing an ISCP, an organization cannot determine the effectiveness of the plan and the organizational readiness to execute the plan.

Williams Adley issued three (3) new recommendations in FY 2021 (Recommendation 2021-25, 2021-26, and 2021-27) to addresses the issues and root cause identified

**Conclusion**

STB has continued to make noted improvements towards defining and developing the foundation of its information security program. However, inconsistent implementation of defined activities throughout the audit period and gaps in the content of its governing documents, prevent the STB from having an effective information security program.

**Recommendations**

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

- **Recommendation 2021-01**: Develop an enterprise architecture that includes information security considerations and the resulting risk to the Agency, as well as incorporates STB’s existing cyber security architecture.
- **Recommendation 2021-02**: Identify and define all software programs that are not authorized to execute on STB information systems.
- **Recommendation 2021-03**: Establish and implement procedure to manage hardware asset inventory connected to STB’s network.
- **Recommendation 2021-04**: Review all open POA&Ms and assign scheduled completion dates which account for the required resources and corrective actions, including milestones, to manage and mitigate the identified risk.
- **Recommendation 2021-05**: Develop a SCRM strategy and supporting policies and procedures to ensure that products, system components, systems, and services of external providers are consistent with the organization’s cybersecurity and supply chain risk management requirements.
- **Recommendation 2021-06.** Develop a process to make improvements to its baseline configuration, secure configuration, and flaw remediation policies and procedures through the use of lessons learned.
- **Recommendation 2021-07.** Implement documented processes for configuration management changes as required by STB policies and procedures.
- **Recommendation 2021-08.** Evaluate deviations from CIS benchmarks and determine if the associated configurations should align with best practices or if deviations should be risk accepted.
- **Recommendation 2021-09.** Update vulnerability management procedures to support implementation of STB’s VDP.
- **Recommendation 2021-10.** Update the Access Recertification Process document to align with STB’s existing practices to ensure users complete all required training and onboarding forms.
- **Recommendation 2021-11.** Define the Identity and Access management policies and procedures for user monitoring program within STB ICAM plan.
- **Recommendation 2021-12.** Develop a process to make improvements to the effectiveness of its ICAM policy, strategy, and road map.
- **Recommendation 2021-13.** Define procedures to review and remove unnecessary PII collection on an organization defined frequency.
- **Recommendation 2021-14.** Perform the review of PTAs for STB GSS, At Hoc, and Dynamic Case Management system on an annual basis.
- **Recommendation 2021-15.** Implement data protection policies and procedures for Data at Rest, prevention and detection of untrusted removable media, and destruction or reuse of media containing PII or other sensitive agency data.
- **Recommendation 2021-16.** Address the knowledge, skills, and abilities gaps identified during the FY 2020 skill gap assessment through training or talent acquisition.
- **Recommendation 2021-17.** Complete the transition from traditional three (3) year authorizations to ongoing authorizations for STB-LAN.
- **Recommendation 2021-18.** Implement documented processes for collecting and reporting performance metrics at the organization and system level to assess the effectiveness of ISCM program.
- **Recommendation 2021-19.** Develop a process to make improvements to the effectiveness of its ISCM program through the collection and reporting of quantitative and qualitative performance metrics, and lessons learned.
- **Recommendation 2021-20.** Define the performance metrics for measuring the incident response capability.
- **Recommendation 2021-21.** Update STB Incident Response Plan to include requirements for the technologies utilized to support Incident Response processes.
- **Recommendation 2021-22.** Define the frequency for the performance of Post Incident activities.
- **Recommendation 2021-23.** Update STB Incident Response plan containment strategies to reflect the current agencies risk prioritization processes.
- **Recommendation 2021-24.** Implement documented processes for Incident Response resolutions of tickets in consistent manner, as required by STB policies and procedures.
- **Recommendation 2021-25.** Define the frequency for the performance of system level Business Impact Analyses (BIA).
- **Recommendation 2021-26.** Review the organization wide BIA on an annual basis.
• **Recommendation 2021-27.** Conduct a tabletop exercise of the General Support System (GSS)’s information system contingency plan (ISCP) on an annual basis.
Appendix A – Scope and Methodology

Department of Transportation Office of Inspector General tasked Williams Adley with conducting a performance audit of Surface Transportation Board (STB)’s information security programs and practices in accordance with Federal Information Security Modernization Act of 2014 for the period October 1, 2020, to June 25, 2021. Williams Adley conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit objective was to determine the effectiveness of STB’s information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover. As required by FISMA, we selected a representative subset of STB’s systems to review. For the FY 2021 audit, we selected STB General Support System, AtHoc and Dynamix Case Management System as our in-scope systems.

We performed our audit steps from February 22, 2021 to June 25, 2021. To perform this audit, Williams Adley interviewed STB management to determine the effectiveness of STB’s information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover. In addition to interviews, we also observed operations remotely via screen sharing technology, conducted sampling where applicable, inspected STB policies and procedures, and obtained sufficient evidence to support the conclusions and recommendations presented in this report.
## Appendix B – Status of Prior Year FISMA Recommendations

<table>
<thead>
<tr>
<th>#</th>
<th>Description of Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-1</td>
<td>Complete implementation of policies and procedures for:</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td></td>
<td>a. Risk management, including a risk management plan and assessment;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. System authorization; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Plans of actions and milestones.</td>
<td></td>
</tr>
<tr>
<td>2017-2</td>
<td>Complete the system reauthorization of the STB LAN</td>
<td>Closed in FY 2018.</td>
</tr>
<tr>
<td>2017-3</td>
<td>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.</td>
<td>Closed in FY 2018.</td>
</tr>
<tr>
<td>2017-4</td>
<td>Define specifications and acquire an automated solution to assist with the risk management program.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2017-5</td>
<td>Develop policies and procedures for the implementation of an information security architecture.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2017-6</td>
<td>Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2017-7</td>
<td>Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.</td>
<td>Closed in FY 2018.</td>
</tr>
<tr>
<td>2017-8</td>
<td>The STB is modifying its identity and access management policies and procedures to address:</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td></td>
<td>a. Reviews of as-is states, desired states, and a transition plan;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Processes for assigning personnel risk designations prior to granting access to its systems;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. Processes for developing, documenting, and maintaining access agreements for individuals with system access; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Requirements for remote access.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Description of Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-9</td>
<td>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.</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td>2017-10</td>
<td>Develop and implement a formal process for measuring the effectiveness of its security awareness and training program.</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td>2017-11</td>
<td>Modify the training plan to include missing elements such as funding, goals and use of technology.</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td>2017-12</td>
<td>Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td>2017-13</td>
<td>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.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2017-14</td>
<td>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.</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td>2018-1</td>
<td>Fully develop a risk management strategy and the supporting procedures for maintaining an accurate system inventory.</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>2018-2</td>
<td>Develop a configuration management plan with supporting policies and procedures and ensure that the existing Change Management Charter aligns with the plan.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2018-3</td>
<td>Develop an ICAM strategy to guide its ICAM process and activities, and modify existing policies and procedures to adequately address:</td>
<td>Closed in FY 2020.</td>
</tr>
<tr>
<td></td>
<td>a. Processes to request, modify, and revoke privileged and non-privileged access; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Processes to ensure separation of duties within the organization.</td>
<td></td>
</tr>
<tr>
<td>2018-4</td>
<td>Full implement the use of PIV card for personnel to access STB’s facilities.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2018-5</td>
<td>Develop a privacy program, including related plans, policies and procedures, for</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>#</td>
<td>Description of Recommendation</td>
<td>Status</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>2018-6</td>
<td>Develop an Incident Response plan in accordance with NIST SP 800-61, rev. 2.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2018-7</td>
<td>Modify incident response policies and procedures to incorporate the most recent incident attack vectors taxonomy in accordance with US-CERT.</td>
<td>Closed in FY 2019.</td>
</tr>
<tr>
<td>2020-1</td>
<td>Implement documented processes for granting and removing user access in a consistent manner, as required by STB policies and procedures.</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>2020-2</td>
<td>Implement processes for conducting, documenting, and maintaining Position Risk Designations in a consistent manner, as required by STB policies and procedures.</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>2020-3</td>
<td>Develop a process for ensuring that the completion of role-based training is tracked and maintained.</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>2020-4</td>
<td>Consistently implement the process to ensure all new users complete the mandatory security awareness training requirements prior to being granted access to STB systems.</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td>2020-5</td>
<td>Fully develop the ISCM Strategy and all information system ISCM plans to include the required criteria documented in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 such as:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Considerations at the organization/business process level;</td>
<td>Closed in FY 2021.</td>
</tr>
<tr>
<td></td>
<td>- Considerations at the information system level; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Processes to review and update the ISCM program and strategy</td>
<td></td>
</tr>
<tr>
<td>2020-6</td>
<td>Define the process to ensure the timely collection of established metrics across its operational systems and reporting evaluation process to assist ISCM Stakeholders to make informed decisions</td>
<td>Closed in FY 2021.</td>
</tr>
</tbody>
</table>
Appendix C – Criteria and Guidance

Williams Adley utilized the following criteria to support the conditions identified during the FY 2021 audit of Surface Transportation Board’s information security program:

I. Risk Management

Williams Adley utilized the following criteria to identify the conditions within STB’s risk management program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 1:** According to National Institute of Standards and Technology (NIST) 800-53 Program Management (PM)-7: 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.
- **Condition 2:** According to STB’s Configuration Management Policy, the STB shall “[identify] and document all software programs that are not authorized to execute on the information system.”
- **Condition 3:** According to the Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metric 2, Level 3 requirements: “The organization consistently utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization’s network and uses this taxonomy to inform which assets can/cannot be introduced into the network.”
- **Condition 4:** According to STB’s POA&M Procedures Section 9.9, the agency assigns scheduled completion dates “based on a realistic estimate of the amount of time it will take to allocate the required resources, implement the corrective action(s), and complete all associated milestones.”

II. Supply Chain Risk Management (SCRM)

Williams Adley utilized the following criteria to identify the conditions within STB’s supply chain risk management program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 5:** According to FISMA reporting metric 12, Level 2 requirements: “The organization has defined and communicated an organization wide SCRM strategy. The strategy addresses:
  - SCRM risk appetite and tolerance
  - SCRM strategies or controls
  - Processes for consistently evaluating and monitoring supply chain risk
  - Approaches for implementing and communicating the SCRM strategy
  - Associated roles and responsibilities.”
- **Condition 6:** According to FISMA reporting metric 13, Level 2 requirements, “The organization has defined and communicated its SCRM policies, procedures, and processes.”
• **Condition 7:** According to FISMA reporting metric 14, Level 2 requirements, “The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirement.”

• **Condition 8:** According to FISMA reporting metric 12, Level 2 requirements, “The organization has defined and communicated its component authenticity policies and procedures.”

III. Configuration Management

Williams Adley utilized the following criteria to identify the conditions within STB’s configuration management program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

• **Condition 9:**
  - According to the FISMA Reporting Metric 19, Level 3 requirements: “The organization utilizes lessons learned in implementation to make improvements to its baseline configuration policies and procedures”.
  - According to the FISMA Reporting Metric 20, Level 3 requirements: “The organization utilizes lessons learned in implementation to make improvements to its secure configuration policies and procedures”.
  - According to FISMA Reporting Metric 21, Level 3 requirements: The organization “utilizes lessons learned in implementation to make improvements to its flaw remediation policies and procedures”.

• **Condition 10:** According to emergency request workflow outlined within STB’s Change Management Procedures, system owners are required to accept an emergency change once it is implemented into production.

• **Condition 11:**
  - According to standard change management request workflow outlined within STB’s Change Management Procedures, standard changes are required to be reviewed and approved by CAB.
  - According to the IT Change Management Charter, “standard [change management requests] (CMRs) should be tested once the Security team has approved a Standard change. Following successful testing, the CMR must be reviewed in the next scheduled Change Management Meeting and implemented once approved.”
  - According to the IT Change Management Charter, “once a standard process is approved, subsequent changes that would follow this process would not need approval at the CAB level.”

• **Condition 12:** According to STB’s Configuration Management Plan, the “STB uses [the] CIS benchmarks as a baseline configuration where applicable.”

• **Condition 13:** According to the FISMA Reporting Metric 24, Level 2 requirements: “the organization has updated its vulnerability disclosure handling procedures to support the implementation of its Vulnerability Disclosure Procedures.”

IV. Identity and Access Management
Williams Adley utilized the following criteria to identify the conditions within STB’s identity and access management program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 14:**
  - According to NIST 800-53 Planning (PL)-4 The organization:
    - Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
    - Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
    - Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and
    - Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

- **Condition 15:** According to STB's Access Control Policy Control Enhancement (AC-2 (4)) - Account Management | Automated Audit Actions, “the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies STB IT Security personnel.”

- **Condition 16:** According to FISMA Reporting Metric 27, Level 3 requirements: “the organization is consistently capturing and sharing lessons learned on the effectiveness of its ICAM policy, strategy, and road map and making updates as needed.”

**V. Data Protection and Privacy**

Williams Adley utilized the following criteria to identify the conditions within STB’s data protection and privacy program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 17:** According to Office of Management and Budget (OMB) Circular A-130, "Agencies shall maintain an inventory of the agency’s information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions”.

- **Condition 18:** According to STB’s Enterprise Privacy Plan, “PTAs will be reviewed annually to determine whether they are still valid”.

- **Condition 19:** According to FISMA, Level 3 requirements, “The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.”

**VI. Security Training**
Williams Adley utilized the following criteria to identify the condition within STB’s security training program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 20**: According to FISMA reporting metric 42, Level 3 requirements, “The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its awareness and specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization’s awareness and training strategy/plans.”

VII. Information Security Continuous Monitoring (ISCM)

Williams Adley utilized the following criteria to identify the conditions within STB’s ISCM program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 21**: According to STB’s Continuous Monitoring Plan, “STB is required to comply with the [National Institute of Standards and Technology Special Publication] 800-37 [Risk Management Framework (RMF)] to prepare, categorize, select, implement, assess, authorize, and monitor security controls for information systems.” The plan continues to describe the use of ongoing authorization to support step 6 of the RMF, monitoring security controls.

- **Condition 22**: According to FISMA reporting metric 50, Level 3 requirements, “the organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting.”

- **Condition 23**: According to FISMA reporting metric 47, Level 3 requirements, “The organization also consistently captures lessons learned to make improvements to the ISCM policies and strategy.

VIII. Incident Response

Williams Adley utilized the following criteria to identify the conditions within STB’s incident response program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

- **Condition 24**: According to the FISMA Reporting Metric 52, Level 2 requirements: “The organization has developed a tailored incident response plan that addresses metrics for measuring the incident response capability.”

- **Condition 25**: According to the FISMA Reporting Metric 58, Level 2 requirements: “The organization has identified and fully defined its requirements for the incident response technologies it plans to utilize in the specified areas.”

- **Condition 26**: According to the FISMA Reporting Metric 55, Level 3 requirements: “The organization is consistently capturing and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.”
• **Condition 27:** According to the FISMA Reporting Metric 55, Level 2 requirements: “The organization has defined its policies, procedures, and processes for incident handling to include containment strategies for each key incident type.”

• **Condition 28:** According to STB’s incident response workflow, the agency is required to prioritize an incident after the creation of an incident ticket and determine the incident’s functional impact to the organization and potential recoverability.

IX. Contingency Planning

Williams Adley utilized the following criteria to identify the conditions within STB’s contingency planning program as outlined within the “Results of the FY 2021 FISMA Audit” section of this report:

• **Condition 29:** According to NIST 800-53 Contingency Planning (CP)-2: The organization “reviews the contingency plan for the information system [Assignment: organization-defined frequency].”

• **Condition 30:** According to the authorization page of the STB organization wide BIA, “STB BIA is reviewed on an annual basis to ensure business continuity planning documents are properly maintained.”

• **Condition 31:** According to STB’s Contingency Planning Policy, STB is required to test “the contingency plan for the information system yearly using tabletop.”
Appendix D – Management’s Response

SURFACE TRANSPORTATION BOARD
Washington, DC 20423

August 20, 2021

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

Re: Fiscal Year 2021 FISMA Audit of the Surface Transportation Board

Dear Mr. Dorsey:

Thank you for the opportunity to provide comments in response to the Department of Transportation Office of the Inspector General (DOT-OIG) Fiscal Year (FY) 2021 draft report for the Federal Information Security Modernization Act (FISMA) audit conducted at the Surface Transportation Board (STB or Board). The STB welcomes this audit report and is pleased that the Board’s overall information security program continues to improve, year over year. This improvement reflects the STB’s commitment to implementing a cost-effective, risk-based security program that is aligned with the National Institute of Standards and Technology (NIST) security standards and guidelines. The STB appreciates that this year’s audit recognizes the work that has been done through FY 2021 while identifying information security areas where the STB can continue its improvements.

The STB concurs with the twenty-seven new recommendations for FY 2021. The STB also acknowledges the closure of all previous years’ recommendations during the FY 2021 assessment, which consisted of two FY 2018 recommendations and six FY 2020 recommendations. The STB is committed to addressing the new recommendations and continuing to improve its information security posture. Please see the STB response to each FISMA domain and the established estimated completion dates for the work on the FY 2021 audit recommendations below.

STB Response to the FISMA Risk Management Domain

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

- **Recommendation 2021-1**: December 31, 2022
- **Recommendation 2021-2**: December 31, 2021
- **Recommendation 2021-3**: April 30, 2022
- **Recommendation 2021-4**: December 31, 2021

**STB Response to the FISMA Supply Chain Risk Management Domain**

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

- **Recommendation 2021-05**: March 31, 2022

**STB Response to the FISMA Configuration Management Domain**

The STB continues to mature processes related to Configuration Management and has recently developed and incorporated security impact analysis into its existing Configuration Management process that allows the STB to better understand the security risk associated with proposed configuration changes. The Board will implement the proposed recommendations to help improve its Configuration Management processes. The STB estimated completion dates for recommendations associated with the Configuration Management domain are:

- **Recommendation 2021-6**: December 31, 2021
- **Recommendation 2021-7**: March 31, 2022
- **Recommendation 2021-8**: March 31, 2022
- **Recommendation 2021-9**: December 31, 2021

**STB Response to the FISMA Identity and Access Management Domain**

The STB has taken steps to improve to its Identity and Access Management plans and procedures. These plans and procedures add clarity to the organizational management of the request, modification, and revocation of access entitlements for both privileged and non-privileged accounts, ensuring that the right people are gaining the right access, at the right time.
The Board will implement the proposed recommendations to help improve its Identity and Access Management processes. The estimated completion dates for recommendations associated with the Identity and Access Management domain are:

- **Recommendation 2021-10**: October 31, 2021
- **Recommendation 2021-11**: December 31, 2021
- **Recommendation 2021-12**: December 31, 2021

**STB Response to the FISMA Data Protection and Privacy Domain**

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

- **Recommendation 2021-13**: December 31, 2021
- **Recommendation 2021-14**: December 31, 2021
- **Recommendation 2021-15**: September 30, 2022

**STB Response to the FISMA Security Training Domain**

The STB has increased its ability to develop, host, and manage training requirements within its designated learning management system. The STB has also established additional procedures to ensure all users complete mandatory security awareness training as well as improvements to the security training validation process, ensuring that STB personnel are sufficiently trained. The Board will implement the proposed recommendations to help improve its capability within this domain. The STB estimated completion date for the recommendation associated with the Security Training domain is:

- **Recommendation 2021-16**: March 31, 2022

**STB Response to the FISMA Information Security Continuous Monitoring Domain**

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

- **Recommendation 2021-17**: September 30, 2023
- **Recommendation 2021-18**: September 30, 2022
- **Recommendation 2021-19**: September 30, 2022

**STB Response to the FISMA Incident Response Domain**

The STB continues to make improvements to its Incident Response capability, including modifications of its Incident Response process to align with NIST SP 800-61. This realignment has allowed the STB to categorize incidents efficiently and consistently. Additionally, the STB has developed a more robust Incident Response prioritization matrix that helps prioritize incidents based on type and severity. Implementation of these changes has improved the management of security incidents within the organization. The Board will implement the proposed recommendations to help improve its capability within this domain. The estimated completion dates for recommendations associated with the Incident Response domain are:

- **Recommendation 2021-20**: September 30, 2021
- **Recommendation 2021-21**: September 30, 2021
- **Recommendation 2021-22**: September 30, 2021
- **Recommendation 2021-23**: September 30, 2021
- **Recommendation 2021-24**: September 30, 2021

**STB Response to the FISMA Contingency Planning Domain**

The STB continues to make progress on its Contingency Planning processes including modernizing its backup processes and capabilities. Additionally, the Board continues to migrate data and business processes to federally approved cloud services providers. These modernization and migration activities to the cloud increase availability and redundancy of STB data and information systems. The Board will implement the proposed recommendations to help improve its capability within this domain. The estimated completion dates for recommendations associated with the Contingency Planning domain are:

- **Recommendation 2021-25**: May 30, 2022
- **Recommendation 2021-26**: May 30, 2022
• **Recommendation 2021-27: September 30, 2022**

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

Rachel D. Campbell
Managing Director
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.