



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. QC2022001

October 4, 2021



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

Required by the Federal Information Security Modernization Act of 2014

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.



U.S. Department of
Transportation

Office of Inspector General
Washington, DC

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.

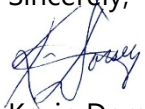
¹ Pub. L. No. 113-283.

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,

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

Kevin Dorsey

Assistant Inspector General for
Information Technology Audits

cc: STB Audit Liaison

Attachment

Quality Control Review

We performed a quality control review (QCR) of Williams Adley's report, dated August 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

BIA	Business Impact Analysis
CIS	Center for Internet Security
FISMA	Federal Information Security Modernization Act
GSS	General Support System
ICAM	Identity, Credential, and Access Management
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
LAN	Local Area Network
OMB	Office of Management and Budget
PII	Personally Identifiable Information
POA&M	Plan of Actions and Milestones
PTA	Privacy Threshold Analysis
QCR	Quality Control Review
SCRM	Supply Chain Risk Management
STB	Surface Transportation Board
VDP	Vulnerability Disclosure Policy

Attachment. Independent Auditor's Report

U.S. DOT IG Fraud & Safety Hotline

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

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

Our Mission

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

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



www.oig.dot.gov