SURFACE TRANSPORTATION BOARD
Washington, DC 20423

April 24, 2020

The Honorable Roger Wicker Chairman Senate Committee on Commerce, Science, and Transportation 512 Dirksen Senate Office Building Washington, DC 20510	The Honorable Maria Cantwell Ranking Member Senate Committee on Commerce, Science, and Transportation 425 Hart Senate Office Building Washington, DC 20510
The Honorable Deb Fischer Chairman Subcommittee on Transportation and and Safety 454 Russell Senate Office Building Washington, DC 20510	The Honorable Tammy Duckworth Ranking Member Subcommittee on Transportation and and Safety 524 Hart Senate Office Building Washington, DC 20510

Re: STB Information Security Improvement Act

Dear Chairman Wicker, Ranking Member Cantwell, Subcommittee Chairman Fischer, and Subcommittee Ranking Member Duckworth:

I am writing in further reference to my April 10, 2020 letter submitted to you pursuant to Section 2(b)(2) of the STB Information Security Improvement Act, P.L. 115-269. In that letter, I reported on the progress of the Surface Transportation Board (STB or Board) towards implementing the fiscal year (FY) 2017 recommendations outlined by the Department of Transportation Office of Inspector General (DOT OIG) in Report No. FI2018002, an audit conducted in accordance with the Federal Information Security Modernization Act of 2014 (FISMA Audit). Specifically, I noted that 11 of the 14 recommendations had been closed (i.e., deemed complete) by the DOT OIG and three were under its review for closure.

I am pleased to report that the DOT OIG has now closed the final three recommendations, resulting in completion of all 14 FY 2017 FISMA Audit recommendations. The Board greatly appreciates the work of the DOT OIG, particularly Joseph Come, Louis King, Barry DeWeese, Nilesh Patel, and Jenelle Morris, which has enabled the STB to fulfill the FISMA Audit directives and advance the security of our information technology systems.

Attached for your information is a final chart with the detail of each recommendation and its closure status. This letter completes the Board's reporting obligations under the STB Information Security Improvement Act.

Once again, thank you for your continued interest in the Board's work and its efforts to fully address the FY 2017 FISMA Audit recommendations. If you have any questions, please contact me or Rachel Campbell, the Board's Managing Director, at 202-245-0357.

Sincerely,

Ann Begeman

Ann Begeman
Chairman

Surface Transportation Board
FY 2017 FISMA Audit Recommendations

#	Description of Recommendation	Status
2017-1	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.	Parts *b* and *c* closed in FY 2018, part *a* closed in FY 2019.
2017-2	Complete the system reauthorization of the STB LAN.	Closed in FY 2018.
2017-3	Complete service level agreements or similar documents that permit STB or its auditor to perform tests and/or obtain supporting documentation to demonstrate that cloud systems are properly authorized to operate.	Closed in FY 2018.
2017-4	Define specifications and acquire an automated solution to assist with the risk management program.	Closed in FY 2019.
2017-5	Develop policies and procedures for the implementation of an information security architecture.	Closed in FY 2019.
2017-6	Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.	Closed in FY 2019.
2017-7	Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.	Closed in FY 2018.
2017-8	Modify 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.	Part *a* closed FY 2018. Part *b*, *c*, and *d* closed in FY 2019.
2017-9	Conduct a needs assessment to formally determine the organization's awareness and training needs, including but not limited to developing and implementing a formal process for assessing the skills, knowledge, and abilities of its workforce.	Closed in FY 2020.

#	Description of Recommendation	Status
2017-10	Develop and implement a formal process for measuring the effectiveness of its security awareness and training program.	Closed in FY 2020.
2017-11	Modify the training plan to include missing elements such as funding, goals and use of technology.	Closed in FY 2020.
2017-12	Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.	Closed in FY 2020.
2017-13	Modify its policies and procedures to address missing components such as incident detection and analysis; incident prioritization, containment, eradication, and recovery; coordination, information sharing, and reporting; incident response training and testing, and considerations for major incidents.	Closed in FY 2019.
2017-14	Implement its contingency planning policy by performing business impact analyses, updating or completing system contingency plans, testing contingency plans, performing necessary backups and obtaining an adequate alternate processing site, it needed.	Closed in FY 2020.