U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

FISMA 2017: The Surface Transportation Board's Information Security Program Is Not Effective

Report No. FI2018002

October 26, 2017

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

FISMA 2017: The Surface Transportation Board's Information Security Program Is Not Effective

Requested by the Surface Transportation Board

Surface Transportation Board | FI2018002 | October 26, 2017

What We Looked At

The Federal Information Security Management Act of 2002, requires agencies to implement information security programs, conduct annual effectiveness reviews, and report the results to OMB. For 2017's review, OMB required determination of programs' maturity levels—(lowest to highest) Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized. Our objective was to determine the program's effectiveness for the 12 months prior to June 30, 2017, in five control areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

STB's program is at the Ad Hoc maturity level.

STB's **Identify** controls—risk management, weakness remediation, and security authorization—were inadequate. STB did not have a risk management program and its process to reauthorize systems was inadequate.

STB's **Protect** controls—configuration management, user identity management, and security training—were inadequate. Policy and procedures did not cover software patch installation or parts of user identity management. Only 66 percent of STB employees completed 2017 security awareness training.

STB did not have policy for **Detect** controls—to identify cybersecurity incidents in an information security continuous monitoring program—and lacked a monitoring strategy.

STB's **Respond** controls—incident handling and reporting—were inadequate. The policy did not cover incident response planning and analysis. STB had not collaborated with DHS on incident response.

STB had not implemented **Recover** controls for contingency planning. STB lacked a plan for system recovery after emergency shutdowns, impact analysis, alternative sites, or data back-up.

Our Recommendations

We made several recommendations to serve as a roadmap for STB to develop an effective information security program. STB concurred with all of our recommendations.

All OIG reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Legal, Legislative, and External Affairs at (202) 366-8751.

U.S. Department of Transportation

Office of Inspector General
Washington, D.C. 20590

October 26, 2017

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

Dear Ms. Begeman:

The Federal Information Security Management Act of 2002 (FISMA),[1] as amended,[2] requires agencies to implement information security programs. FISMA also requires agencies to have an annual independent evaluation performed to determine the effectiveness of their programs and report the results of these reviews to OMB. This report presents the results of our review of the Surface Transportation Board's (STB) program. We performed this review at STB's request.[3]

For the 2017 review, OMB required independent auditors to assess 54 metrics in 5 security function areas to determine the maturity level[4] of their agencies' information security programs. Program maturity can be at one of five levels defined by OMB (from lowest to highest)—Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized. OMB defines effective as meeting all metrics in the first four levels.

[1] Public Law No. 107-347 (2002).

[2] The Federal Information Security Modernization Act of 2014 (Public Law No. 113-283) amended FISMA to, among other things, (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) for agency information security policies and practices and (2) set authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of policies and practices for information systems.

[3] Agencies that do not have inspectors general are required to engage external independent auditors to evaluate their information security programs. Accordingly, we, the Department of Transportation (DOT) Office of Inspector General (OIG), entered into a memorandum of understanding with STB to perform STB's 2017 FISMA evaluation. Under 49 U.S.C. § 1326, we have the authority to review STB's financial management, property management, and business operations, including internal accounting and administrative control systems, to determine the Agency's compliance with applicable Federal laws, rules, and regulations. While we have limited authority to review STB's operations, our office is not the Inspector General for STB and is not legally obligated to perform the independent evaluation that FISMA requires.

[4] OMB's *FY 2017 Inspector General FISMA Act of 2014 Reporting Metrics* (April 2017) prescribes the metrics and represents a continuation of work begun in fiscal year 2016, when the metrics were aligned with the five function areas in the National Institute for Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover* (2014).

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of STB's information security program and practices for the 12-month period ended June 30, 2017.[5] Specifically, we assessed STB's performance in the following function areas: (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover.

We conducted our work in accordance with generally accepted Government auditing standards. To address OMB's 2017 FISMA reporting metrics, we assessed STB's three systems, interviewed STB officials, and analyzed data pertaining to its information security practices. For more details on our scope and methodology, see exhibit A. As required, we provided our results to OMB via its web portal.[6]

RESULTS IN BRIEF

STB's information security program is not effective, based on OMB's methodology. STB officials noted that when it separated from DOT in December 2015,[7] the Agency focused on implementing what it deemed the most critical activities required to separate STB's IT systems from DOT's, such as improving operational security and performing regular maintenance operations. However, STB did not issue any policies needed to create a cybersecurity program until May 2017—after we commenced our audit and 15 months after it separated from DOT. STB also noted that because it did not have an Information Systems Security Manager (ISSM), it was difficult to develop a cybersecurity program. The lack of policies and related procedures for an extended period of time contributed to deficiencies that increased STB's susceptibility to external threats and to non-compliance with Federal requirements and guidelines. Specifically:

1. **Identify.** STB's Identify controls, which include risk management and weakness remediation, and security authorization,[8] were inadequate. STB does not have an adequate risk management program, and plans to implement one by March 2018. STB's process to reauthorize systems was not adequate. For example, STB's local area network (LAN) was operating without reauthorization.

[5] Per OMB's *Annual Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, agencies should set cut-off dates for data collection and report preparation that allow adequate time for meaningful internal reviews, comments, and resolution of disputes before reports' finalization.

[6] Because OMB designates this information "For Official Use Only," our submission to OMB is not contained in this report.

[7] Public Law No. 114-110 (2015).

[8] NIST defines system authorization as the official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to organizational operations—including mission, functions, image, or reputation—organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

2. **Protect.** STB's Protect controls, which include configuration management, identity and access management and security training, were not adequate. Its recently issued policy and procedures were insufficient because they did not address controls such as software patch installation, or the reviews and transition plans needed to support the identity and access management process. Based on STB statistics, only 66 percent of employees actually took security awareness training during fiscal year 2017.

3. **Detect**. STB has not issued policy for its Detect controls—used to identify cybersecurity incidents as part of an information security continuous monitoring[9] (ISCM) program. STB also lacks an ISCM strategy.

4. **Respond.** STB's Respond controls, which encompass incident handling and reporting, are not adequate. For example, STB's policy does not adequately address a number of areas, including strategies for incident response planning, and incident analysis. STB also did not provide evidence that it collaborated with the Department of Homeland Security (DHS) on quick incident response.

5. **Recover.** STB has not implemented its Recover controls, which address contingency planning. The Agency lacked contingency plans, business impact analysis, alternate processing sites, and a process to back up data.

These deficiencies place STB's information security program at the lowest (ad hoc) program maturity level overall as well as in each of the five cyber security function areas. We are making a series of recommendations to serve as a roadmap for STB to develop an effective information security program.

BACKGROUND

STB is an independent, adjudicatory body that, until passage of the Surface Transportation Board Reauthorization Act in December 2015, was housed within DOT. STB retains jurisdiction over certain surface transportation economic regulatory matters. While part of DOT, STB shared many information security controls, such as policy and procedures, with DOT and its Operating Administrations. As a stand-alone Agency, STB became responsible for maintaining its own information security program and independently meeting FISMA's requirements.

Under FISMA,[10] each Federal agency must make secure the information and information systems that support its operations, including those provided or

[9] On-going awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
[10] 44 U.S.C. Chapter 35, Sub Chapter II, Information Security.

managed by other agencies, entities, or contractors. Furthermore, OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*,[11] requires Federal agencies to ensure that appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. FISMA also 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.[12]

For the 2017 review, OMB and DHS, in consultation with the Council of the Inspectors General on Integrity and Efficiency and the Federal Chief Information Officer Council, revised the metrics[13] for inspectors general reviews and independent auditors' annual information security evaluations. The metrics are organized around the five security functions—Identify, Protect, Detect, Respond, and Recover—outlined in NIST's cybersecurity framework.[14] See table 1 for definitions of these functions and the number of metrics in each function.

[11] The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 Fed. Reg. 52730, December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (Pub. Law No. 100-235).

[12] For 2016, STB did not meet these reporting requirements nor did it hire an independent auditor to perform the evaluation of its information security program.

[13] DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* April 2017.

[14] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, 2014.

Table 1. Cybersecurity Framework Functions and Definitions

Cybersecurity Framework Function	Definition	No. of metrics for FISMA 2017
Identify	Requires agencies to develop the understanding needed to manage security risks to systems, assets, data, and capabilities. Includes metrics for risk management, weakness remediation, and security authorization.	12
Protect	Requires agencies to develop and implement appropriate safeguards to ensure delivery of infrastructure services. Includes metrics for configuration management, identity and access management, and security training.	23
Detect	Requires agencies to develop and implement processes to identify incidents that may include security breaches. Includes metrics for information security continuous monitoring.	5
Respond	Requires agencies to develop and implement processes for remediating detected cybersecurity incidents. Includes metrics for incident handling and reporting.	7
Recover	Requires agencies to develop, implement, and maintain up-to-date plans for restoration of capabilities and services impaired during a security event or emergency shut down. Includes metrics for contingency planning.	7

Source: DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

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 2. Cybersecurity Maturity Levels and Definitions

Maturity Level (from lowest to highest)	Definition
Ad Hoc	Policies, procedures, and strategy are not formalized; activities are performed in a reactive manner.
Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable	Quantitative and qualitative measures are collected across the organization, and used to assess the effectiveness of policies, procedures, and strategy and make necessary changes.
Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business and mission needs.

Source: DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

IDENTIFY FUNCTION CONTROLS ARE INADEQUATE

STB’s Identify function controls, which include risk management, weakness remediation, and security authorization, are inadequate. STB has not implemented its risk management policies and procedures, and does not conduct adequate system security reauthorization. Furthermore, the Agency’s security weakness remediation does not comply with requirements. STB also lacks two other elements of a risk management program—automated solutions and a security architecture. Based on OMB’s metrics, STB’s Identify function is at the Ad Hoc maturity level.

STB Has Not Implemented Its Risk Management Policies and Procedures

FISMA requires agencies to implement policies and procedures to cost-effectively reduce risks to an acceptable level. OMB requires[15] agencies to implement risk management programs that include structures for managing and monitoring risk at the organization, business process, and system levels. STB issued its risk management policy and procedures in May 2017—after we started our audit and 15 months after it became an independent Agency—but had not fully implemented or communicated them to personnel. For example, STB had not completed a risk assessment or risk management plan. STB plans to complete implementation by March 2018. This lack of a complete risk management plan inhibits STB’s ability to identify risks, design system controls to address risks, and ensure officials make decisions based on correct understandings of the risks the Agency is exposed to.

[15] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*, July 2016.

STB Does Not Conduct Adequate System Security Reauthorization

STB had not conducted the required security reauthorization and control testing or established continuous monitoring for its three systems—the STB LAN, the AWS US Public, and the Microsoft Office 365 Multi-Tenant & Supporting Services System. The latter two systems are cloud systems. OMB[16] states that system reauthorizations should occur in response to significant changes. STB's departure from DOT represented such a change. Since it is no longer part of DOT's infrastructure, STB's LAN does not fall within DOT's security perimeter or use the Department's internet access connections. However, STB last authorized the LAN in 2014, when it was still part of DOT, and officials incorrectly assumed that system authorization was still valid. After we began our audit, an STB official signed a document to accept the risk for the LAN to operate through December 6, 2017, without re-authorization. In October 2017, STB signed an inter-agency agreement with Department of Interior to complete the security assessment and authorization. STB informed us that it has issued policy on system authorization but would not complete the policy's implementation until March 2018.

STB officials also informed us that the Agency ensures that all cloud services contractors comply with Federal Risk and Authorization Management Program's (FedRAMP) security requirements. However, STB could not provide evidence—such as service level agreements[17]—to support this compliance. As a result, we could not verify whether STB's two cloud systems met NIST's reauthorization requirements for cloud systems.[18] STB officials stated that the Agency plans to complete formal documentation of this reauthorization process no later than March 2018. This lack of up-to-date system authorizations prevents STB's verification that its systems' security controls are properly designed and operating effectively and address the appropriate levels of risk tolerance.

Security Weakness Remediation Does Not Comply With Requirements

An agency's plans of action and milestones (POA&M) program—required by OMB[19]—sets up the correction and elimination of identified system weaknesses. STB had not implemented an effective POA&M program. STB informed us that for years 2012 to 2017, it had 45 POA&Ms. However, this information is not consistent with information from STB when it was still a part of DOT. For

[16] OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, July 2016.

[17] A service level agreement defines levels of service and performance that the agency expects the contractor to meet and the agency uses the information to measure the effectiveness of its cloud services.

[18] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[19] OMB M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act,* August 23, 2004.

example, for our fiscal year 2015 FISMA report, DOT informed us that STB had 59 open POA&Ms. According to STB officials, the Agency plans to complete the implementation of its POA&M program by March 2018. Incomplete POA&M information inhibits STB's assessment of risk and funding requirements, analysis of weakness trends, prioritization of remediation, and implementation of corrective actions.

STB Also Lacks Two Other Elements of a Risk Management Program—Automated Solutions and a Security Architecture

OMB's reporting metrics for fiscal year 2017 require inspectors general to assess two other characteristics of their agencies' risk management programs—the use of automated solutions and security architecture.

STB informed us that it has not defined requirements for an automated solution. An automated solution provides a centralized view of an agency's risks and controls and a management dashboard. STB stated further that it will acquire and implement solutions to meet this requirement by March 2018.

STB has also not defined an information security architecture and the processes for ensuring that new hardware and software are consistent with the architecture prior to use. According to STB officials, the Agency plans to develop the appropriate policies for its security architecture by June 2018. The lack of an automated solution and a security architecture increases the difficulty of managing risks, including those introduced by acquisition of new technology.

PROTECT FUNCTION CONTROLS ARE INADEQUATE

STB's Protect function controls, which include configuration management, user identity and access management, and security awareness training, are not adequate. The Agency has not fully implemented its configuration management program. Its user identity and access management program is also inadequate, and its security awareness training program does not meet requirements. Based on OMB metrics, STB's Protect function is at an Ad Hoc maturity level.

STB Has Not Fully Implemented Its Configuration Management Program

Configuration management describes the practices, processes, and responsibilities that support the secure design and implementation of information systems. According to NIST,[20] a configuration management plan should describe an agency's configuration management policy and how it will implement the policy. STB has not fully implemented a configuration management program, and lacks comprehensive configuration management policies, procedures, plans, and strategies. Specifically, we found that:

- STB acknowledges that it has not developed and disseminated comprehensive policies and procedures for information system configuration management. For example, existing procedures do not fully address identification, reporting, and resolution of information system flaws, including timely patch installation.

- Although STB recently defined roles and responsibilities for personnel involved in configuration management, the Agency has not fully implemented them. According to STB officials, the Agency will complete these activities by March 2018.

- STB has not developed an organizationwide configuration management plan with all necessary components. For example, while STB informed us that it has a change management policy, it acknowledges that it has not developed charters for its two change control boards.[21] These boards approve proposed changes to system configuration while considering the changes' security impact. STB is developing charters with a target completion date in the first quarter fiscal year 2018.

The lack of full implementation of configuration management processes and procedures makes it difficult for STB to be sure that it is protecting its information systems from known, exploitable software weaknesses.

STB's User Identity and Access Management Program Is Not Adequate

An agency's identity, credential, and access management (ICAM) program establishes policy and procedures for user identity and secure access to systems and facilities. Federal agencies use the Federal Identity, Credential, and Access

[20] NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011.

[21] A change control board charter describes the process by which the board operates, including how to handle configuration changes, the range of dispositions (approved, not approved, on hold, etc.), evaluation criteria, and the quorum required to make configuration change control-related decisions.

Management Roadmap and Implementation Guidance (FICAM)[22] to develop ICAM programs. STB lacks comprehensive ICAM policies, procedures, and strategies. Specifically, we found that:

- STB's ICAM program does not include reviews of current practices (as-is assessment), identification of gaps (from a desired or to-be state), and a transition plan. These reviews help determine to what degree an agency needs a strategy to guide its ICAM processes and activities.

- STB has not fully defined its processes for assigning personnel risk designations prior to granting access to its systems. STB did not provide us with adequate evidence that it has appropriate personnel screening processes in place. Personnel screening ensures that each individual that accesses an information system, or processes, stores, or transmits classified information is cleared to the highest classification level of the accessed information.

- STB has not fully defined its processes for developing, documenting, and maintaining access agreements for individuals with system access. OMB requires[23] that each individual with access sign an agreement to acknowledge that he or she has read, understands, and will abide by the constraints associated with organizational information systems to which access is authorized.

- STB also has not fully defined its configuration and connection requirements for remote access connections, including system time-outs, and how it monitors and controls remote access sessions. STB did not provide enough documentation on remote access connections for us to determine whether it continuously monitors these sessions.

The lack of procedures and processes for implementing security controls over user identity and access management puts STB's systems at risk for unauthorized access by individuals who no longer have authorized access. STB stated that the majority of both its privileged and non-privileged users[24] use personal identity verification (PIV) cards for access, but PIV access to STB's facility is not possible due to outdated equipment.

[22] Federal Chief Information Officers Council, FICAM, v. 2 (2011).

[23] OMB Circular A-130, Appendix III (2016).

[24] A privileged user is authorized and trusted to perform security-relevant functions that ordinary, or unprivileged, users are not authorized to perform. A non- privileged user has an account for everyday access to applications such as email and data processing.

STB's Security Awareness Training Program Does Not Meet Federal Requirements

FISMA requires agencies to develop and maintain security training programs to ensure that all computer users are adequately trained in their security responsibilities before they are allowed access to information systems. Furthermore, both FISMA and OMB[25] require agencies to provide security awareness training to all employees and contractors, even those that never access computer systems.

STB issued a security awareness training plan in May 2017, during our audit. We found the following deficiencies in the plan:

- It defines roles and responsibilities for STB staff, but it is not clear that these roles and responsibilities have been appropriately resourced. NIST[26] recommends that agencies conduct needs assessments to help them determine security awareness training needs and ensure that they allocate appropriate resources. According to STB officials, the Agency's process to evaluate the skills of personnel with significant security and privacy responsibilities is informal.

- It does not include the following components in NIST's guidelines—funding, goals, use of technologies for training, methods for training deployment, and a process for training evaluation and feedback and use of the information for training improvements.

- It does not provide metrics indicating how STB would measure the completion of security awareness training. For example, Agency officials informed us of training dates for 137 individuals but did not provide the target security awareness training completion rate.

STB did not ensure that sufficient staff took security awareness training. The Agency informed us that 47 (34 percent of 137) individuals took training in fiscal year 2016 and 90 (66 percent of 137) in fiscal year 2017.

STB's lack of a policy for security awareness training over an extended period of time created the risk that the Agency could not protect the confidentiality, integrity, and availability of its information. The lack of a needs assessment makes it difficult for STB to be sure that the personnel that manage its IT infrastructure have the skills necessary to carry out their duties effectively.

[25] OMB Memorandum M-16-04 (October 2015).

[26] NIST SP 800-50 (October 2003).

DETECT FUNCTION CONTROLS ARE NOT SUFFICIENT

STB is in the process of implementing and finalizing its Detect function controls. These controls, for an information security continuous monitoring (ISCM) program, are used to identify cybersecurity incidents. According to NIST guidelines,[27] ISCM provides (1) awareness of relevant threats and vulnerabilities; (2) visibility into organizational assets; and (3) evaluation of the effectiveness of deployed security controls. Based on OMB's metrics, STB's Detect function is at the Ad Hoc maturity level.

STB—which has been operating without an ISCM policy since its separation from DOT—acknowledges that it has not completed implementation of an ISCM program. According to STB officials, the Agency's ISCM policies, procedures, and strategies are currently in draft with a target completion date March 2018. STB's lack of a finalized ISCM program creates a risk that the Agency cannot protect the confidentiality, integrity, and availability of information.

STB'S RESPOND FUNCTION CONTROLS ARE INSUFFICIENT

STB's Respond controls, which include incident handling and reporting, are not sufficient, and based on OMB's metrics, are at the Ad-Hoc maturity level. Under FISMA, OMB policy, and NIST guidelines, Federal agencies must establish incident response and reporting programs for their information systems. Such a program includes monitoring of information systems for possible security breaches, analysis of each breach, and a process for resolution of the weakness that allowed the breach. In addition, STB has not defined the unit that receives incident reports and to what extent, if any, incidents should be reported to the United States Computer Emergency Readiness Team, which provides respond capabilities across the Government.

STB's incident response and reporting program does not comply with Federal requirements. Specifically, STB's policy does not adequately address the following areas: strategies for incident response planning; incident detection and analysis; incident containment, eradication, and recovery; training; special considerations for major incidents; and incident coordination, information sharing, and reporting.

STB did not provide evidence of how it collaborates with DHS for quick incident response or how it plans to use DHS's Einstein[28] technology for intrusion

[27] NIST SP 800-137 (September 2011).

[28] Einstein is a technology that DHS uses to detect and block cyberattacks from compromising Federal agencies, provides situational awareness to use threat information detected in one agency to protect the rest of the Government, and help the private sector protect itself.

detection and prevention. STB informed us that it uses a set of incident response standard operating procedures (SOP), but acknowledges that it has not integrated these SOPs into its incident response policy though intends to do so by June 2018.

STB's lack of an adequate incident response program makes it difficult for the Agency to be sure that it identifies, reports, and mitigates all incidents. As a result, STB's information systems are at risk that compromises will occur and will remain undetected.

RECOVER FUNCTION CONTROLS ARE INADEQUATE

STB's Recover function controls, which address contingency planning, are not developed and are at an Ad Hoc level of maturity. OMB and NIST guidelines[29] require agencies to establish contingency plans to enable the recovery of information systems, operations, and data after a disruption. These plans can include system restoration using alternate equipment, manual processing, alternate locations, or other strategies based on the system's characteristics. STB issued contingency planning policy in June 2017, during our audit, but we found no evidence that the Agency had implemented the policy. STB also did not:

- Provide us a business impact analysis.[30]

- Perform contingency plan testing.

- Have alternate processing sites.

- Perform necessary backups of system information.

This lack of a properly implemented contingency planning process increases the risk that STB will not be able to restore its information systems in the event of disruption.

CONCLUSION

As a result of its separation from DOT in December 2015, STB gained full ownership of its cybersecurity program. With that ownership has come the need to replace the security controls that were once available while STB resided within the DOT cybersecurity perimeter. These controls ranged from basic building blocks such as policies and procedures to an implemented and regularly updated

[29] NIST 800-53, rev. 4 (January 2015); NIST 800-34, rev. 1 (May 2010); OMB M-17-09 (December 2016).

[30] An analysis—important for the development of system-specific contingency plans—of an information system's requirements functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

information security program based on a changing threat and technology landscape and business and mission needs. Although it has taken a major step by issuing policy in May 2017, STB has not completed implementation. In the meantime, STB is encumbered by a number of weaknesses in all five cybersecurity function areas, and its program, based on OMB metrics, has a low level of maturity. Until STB addresses these deficiencies, the Agency's information systems will be at increased risk of attack or compromise.

RECOMMENDATIONS

To assist STB address the challenges in developing a mature and effective information security program, we recommend that the Chairman of the STB or designee:

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.

2. Complete the system reauthorization of the STB LAN.

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.

4. Define specifications and acquire an automated solution to assist with the risk management program.

5. Develop policies and procedures for the implementation of an information security architecture.

6. Modify existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation.

7. Incorporate missing elements into its enterprise-wide configuration management plan such as a change control board charter.

8. Modify identity and access management policies and procedures to adequately 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.

   d. Requirements for remote access.

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.

10. Develop and implement a formal process for measuring the effectiveness of its security awareness and training program.

11. Modify the training plan to include missing elements such as funding, goals and use of technology.

12. Develop and implement an ISCM program that, at a minimum provides awareness of threats and vulnerabilities.

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.

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.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided STB with our draft report on September 26, 2017, and received its response on October 10, 2017, which is included as an appendix to this report. STB concurred with all 14 of our recommendations. STB’s response did not include estimated dates for completing planned actions, which we have requested. We will track and evaluate the completion of these planned recommendations until they are resolved or until STB engages an independent auditor to perform its 2018 FISMA audit.

We appreciate the courtesies and cooperation of the STB’s representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Kevin Dorsey, Program Director, at (202) 366-1518.

Sincerely,

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

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our audit between April and September 2017, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FISMA requires agencies to have an annual independent evaluation performed to determine the effectiveness of their information security program. Agencies that do not have an inspector general, such as STB, are required to engage an external independent auditor to evaluate their information security programs. Accordingly, in April 2017, STB entered into a memorandum of understanding with us to be reimbursed for performing its 2017 FISMA evaluation. We have limited authority to review STB operations under 49 U.S.C. § 1326, but our office is not the STB's Inspector General. As part of this evaluation, we were required to test a representative subset of systems.

As required by FISMA, our objective was to determine the effectiveness of STB's information security program and practices. Our testing covered the 12-month period ending June 30, 2017 and was performed in Washington, D.C. We obtained and reviewed relevant NIST, OMB, and other Federal requirements. We requested data to test STB's performance in the five cyber function areas described in NIST's Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover. We also interviewed personnel, including the Managing Director. We reviewed all the audit evidence gathered and evaluated against Federal requirements. We determined that STB had only three systems, so we reviewed the cybersecurity documentation of all three instead of selecting a subset.

As part of our efforts to assess effectiveness, we evaluated STB's data according to OMB's FISMA metrics for OIGs, as described in OMB's *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* to determine the maturity level of STB's information security program. The results of the metrics review were used to populate the Cyberscope database, as required by OMB.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Kevin Dorsey	Program Director
Martha Morrobel	Senior Information Technology Specialist
Tracy Colligan	Senior Information Technology Specialist
Jenelle Morris	Senior Information Technology Specialist
Jo’Shena Jamison	Information Technology Specialist
Petra Swartzlander	Senior Statistician
Makesi Ormond	Statistician
Susan Neill	Writer-Editor

APPENDIX. AGENCY COMMENTS

Surface Transportation Board
Washington, D.C. 20423-0001

October 10, 2017

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

Re: Surface Transportation Board FISMA Audit FY2017

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Federal Information Security Modernization Act Audit for the Surface Transportation Board (STB). The OIG comments are valuable to STB. They afford STB an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to STB by the Federal workforce, the Federal agencies, our private industry partners, and the public. STB welcomes a collaborative dialogue to help ensure we fully understand the OIG's recommendations as we plan and execute our remediation efforts, prioritizing the most critical deficiencies. STB also looks forward to continued discussions during future reviews to help ensure we remain aligned. STB concurs with all fourteen recommendations, and STB understands it has a lot of work to do to address the underlying issues.

STB is reaching out to similarly-sized entities to draw lessons from other Federal agencies in order to implement several of the recommendations such as implementing policies and procedures for risk management; developing and adopting procedures to implement an information security architecture; modifying existing procedures to fully address identification, reporting, and resolution of information system flaws, including timely patch installation; and developing and implementing a functional ISCM program. STB is also ensuring that it can demonstrate that cloud systems are properly authorized to operate.

STB procured a provider to complete its system reauthorization of the STB LAN, and STB is researching market options to obtain an automated solution to assist with the risk management program.

Internally, STB is incorporating the missing elements into its enterprise-wide configuration management plan. STB is modifying its identity and access management policies and procedures to address: a) reviews of as-is states, desired states and a transition plan; b) processes for assigning personnel risk designations prior to granting access to its systems; c) processes for developing, documenting, and maintaining access agreements for individuals with system access; and d) requirements for remote access. STB is researching the elements to design and conduct a needs assessment so it can formally determine STB'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.

With respect to training, STB is developing a formal process to measure the effectiveness of its security awareness and training program, and STB is scrutinizing its training plan to buttress it and include missing elements such as funding, goals and use of technology.

Finally, concerning incident and contingency planning, STB will 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. In addition, STB will perform business impact analyses, update and complete its system contingency plans, test contingency plans, perform necessary backups and obtain an adequate alternate processing site in order to implement its contingency plan.

Sincerely,

/s/ Rachel D. Campbell

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