Internal Audit of Information Security, Cybersecurity Controls, and Payment Card Industry Data Security Standards (PCI DSS) Compliance

Internal Audit Report

September 17, 2018

Main audit categories

- Payment Card Industry Data Security Standards (PCI DSS)
- Cybersecurity Controls
- Information Security / Physical Security

Prepared by MassDOT Internal Audit

massDOT
Massachusetts Department of Transportation

Payment Card Industry Data Security Standards

1) Issues:

1) MassDOT was not in compliance with PCI DSS in 2016. Findings were not remedied.

2) MassDOT Security flaws were identified during 2017 PCI testing, which were not remedied. The 2017 Report of Compliance (ROC) was not finalized.

Management Response:
MassDOT has completed the PCI DSS 3.2 compliance audit. MassDOT has addressed previously identified PCI DSS compliance issues and has received a PASS rating. (Gary Foster, Chief Information Officer)

Implementation Date: Completed 06/30/2018

Payment Card Industry Data Security Standards

2) Issues:

1) Vulnerability scanning and penetration testing are performed on MassDOT systems that are within PCI DSS scope, however, these tests are not performed on all IT systems.

2) In FY 2015 – 2017, there have been multiple MassDOT and MBTA vulnerability scan and penetration test results that were rated as 'FAIL' or as a 'HIGH' risk.

Management Response:

MassDOT: Penetration test was performed on external network, internal network and applications, results of which are stated in the report dated 5/17/18. No External network vulnerabilities were identified. The application vulnerabilities were addressed on 7/11/18. Internal network vulnerabilities continue to be addressed according to the MassDOT's risk management process, all HIGH risk issues have been addressed.

MassDOT has achieved a PCI PASSing grade on four (4) successive Quarterly External vulnerability scans, performed by a Qualified Security Vendor (QSV, Coalfire) to comply with PCI.

Internal vulnerability scans are being performed on PCI assets and are being addressed according to MassDOT's risk-based remediation process.

A vulnerability management program is in CIP FY 19 to operationalize and expand with additional related security practices and capabilities.

Further expansion for vulnerability scanning of the Non-PCI assets is also being coordinated with EOTSS to be addressed in FY 19.

EOTSS will be working to expand their vulnerability management and scanning program to the MassDOT network in FY 19. MassDOT will evaluate whether implementation of total penetration testing outside of the PCI environment is feasible during FY 19. (Gary Foster, Chief Information Officer)

MBTA: A Vulnerability Management Assessment has been performed by E&Y in FY 2018. The report of recommendations and program operations is planned to be addressed in CIP FY 19. (Gary Foster, Chief Information Officer)

Implementation Dates:

Please see above.

Cybersecurity Controls

3) Issue:
Employees at the RMV, TransCore, and Edenred who process credit card transactions, have internet access, as well as access to personal e-mail.

Management Response:
MassDOT is updating its Acceptable Use Policy and will consider and address these matters as part of that policy update. (Stephanie Pollack, Secretary & CEO / Executive Office)

Implementation Date: FY 19

4) Issue:
USB flash drives are allowed to be used throughout MassDOT, however, there is no established formal policy describing proper usage.

Management Response:
MassDOT will look at similar organizations, consult with EOTSS and work with IT and HR to develop an appropriate policy on use of USBs that aligns with Commonwealth-wide policy and addresses the concerns identified. (Stephanie Pollack, Secretary & CEO / Executive Office)

Implementation Date: FY 19

Cybersecurity Controls

5) Issue:
Unused USB ports are not disabled on computers used to process customer RMV transactions.

Management Response:
Although RMV computers do not have any credit card data on them, which meets the PCI requirement, there are other cyber security issues. To disable unused ports would be too cumbersome and hard to support. One option is to implement blank USB port adaptors for those ports that are unused. Plan is to order and test a couple of options. If this is a viable solution, we will phase into the Service Centers. (Harri Rosenberg, Director of IT Operations)

Implementation Date: 12/31/2018

---

6) Issue:
RMV credit card terminals are not being inspected for tampering (with the exception of AAA Service Centers).

Management Response:
RMV will work with MassDOT CISO to develop and distribute SOPs for inspecting credit card terminals for tampering. RMV will develop a departmental process to train personnel on inspecting terminals as part of start of day operations. (Sarah Zaphiris, RMV Chief Administrative Officer)

Chief Information Security Officer (CISO) will provide support as requested by the RMV business unit. (Kendall Silva, Chief Information Security Officer)

Implementation Date: 10/30/2018

Cybersecurity Controls

7) Issue:
A MassDOT IT Incident Response plan has been written, however, it has not been distributed and deployed.

Management Response:
The Executive Incident Response Plan was distributed to those identified as part of the core and secondary response teams. A table top exercise was also run previously. Additional tactical procedures need to be developed within business departments. (Kendall Silva, Chief Information Security Officer)

Implementation Date:
MassDOT will leverage the documented output of the E&Y Incident Response program executed for MBTA in FY18. The recommended policies, process and planning will be aligned with EOTSS Incident response plans in FY 19.

---

8) Issues:

(a) There is no Data Loss Prevention program in place at MassDOT.

(b) There is no non-PCI Data Loss Prevention program in place at the MBTA.

Management Response:
Given ongoing evaluation in FY19, an initial data loss prevention program is being evaluated in the FY19 CIP planning as part of the Vulnerability Management program budgeted activities.

An initial DLP capability will also be assessed and requirements defined for incorporation into the Mobile Device Management (MDM) security configuration controls assessment that is in the FY 19 CIP. (Gary Foster, Chief Information Officer)

Implementation Date: FY 19

Cybersecurity Controls

9) Issue:

MassDOT and MBTA do not have a formal Data Classification policy.

Management Response:

This is a large project extending beyond the Information Security team and MassDOT and MBTA IT departments. This requires a thorough data classification assessment and data flow analysis to identify the types of data, data storage and data processing performed by the business applications. (MassDOT: Dennis McDermitt, Chief Information Officer (EOTSS) / MassDOT & MBTA: Gary Foster, Chief Information Officer)

Implementation Date:

MassDOT:

An initial Data Classification program is being planned in FY19 as part of the Vulnerability Management CIP budgeted activities. Data Flow analysis will be initiated to identify and document the PII and sensitive information being processed and stored by the MassDOT applications. The EOTSS Data Classification standard will be utilized and aligned with during this process.

MBTA:

MBTA will utilize the E&Y Vulnerability Management program recommendations (which include a Data Classification capability), to initially address this as part of the FY 19 CIP.

Cybersecurity Controls

10) Issue:
MassDOT and MBTA do not have formal Disaster Recovery Plans in place to address disruptive events.

Management Response:
MBTA:
For MBTA, we have established a 18 month Cyber Security Modernization Program and expect it to be funded in the MBTA Capital Improvement Plan (CIP). This plan includes a $3M investment in Disaster Recovery. It does not include any funds for a holistic Business Continuity Plan (BCP) / Continuity of Operations Plan (COOP) for the MBTA. Disaster Recovery is a component of an organizations BCP. Many risks will not be resolved by a Disaster Recovery plan alone. (Gary Foster, Chief Information Officer)

MassDOT:
MassDOT is transforming infrastructure as part of the Commonwealth's Executive Office of Technology Services and Security (EOTSS) plans. The expectation is that MassDOT Disaster Recovery will be part of a greater program managed and designed by EOTSS. (Gary Foster, Chief Information Officer)

Implementation Date:
MBTA: FY 19 - 20
MassDOT: TBD with EOTSS

Cybersecurity Controls

11) Issue:
Critical security updates (i.e., Microsoft and third party) should be installed within one month of release, however, this is not always being done at MassDOT.

Management Response:
Monthly patching is in place for Microsoft and 3rd party applications. We are following a risk-based approach to addressing the security patches on a monthly basis. There are months when we are able to address all security patches, and there are other months that we may not address all security patches due to: (1) volume of patches that vary from month to month, and (2) other security and business priorities. Per our policies, we follow and comply with our risk-based remediation best practices. (Harri Rosenberg, Director of IT Operations)

Implementation Date:
Ongoing as part of the Vulnerability Management program being operationalized in FY 19 CIP. It will leverage the E&Y Vulnerability Management Assessment recommendations from FY 18.

Information Security / Physical Security

12) <u>Issues</u>:

1) Physical security access (door lock access) for MassDOT and MBTA terminated employees is not always disabled in a timely manner.

2) The RMV branch alarm system access code is not always disabled upon (or shortly after) employee termination.

3) At various RMV locations, an alarm system access code is assigned to a group, rather than to an individual employee. Furthermore, if an employee who uses a group alarm system access code is terminated, the alarm system access code is not changed.

4) When an MBTA employee is terminated, procedures for notifying applicable business units exist, however, they can be enhanced to strengthen controls.

5) There are no Standard Operating Procedures (SOPs) in place at MassDOT regarding disabling all access for terminated employees (including physical, system, and car pool access).

Information Security / Physical Security

Management Responses (Continued):

- The MBTA – working across all business units - is clarifying procedures related to the need for immediate disabling of access to key systems for terminated employees. In addition to the weekly report distribution, notifications will be distributed to HR, operations workforce coordinators, Finance and payroll and security as necessary. (Gina Spaziani, Director of Financial Planning and Analysis)

- General Services Unit to immediately cancel the 10 Park Plaza motor pool vehicle account of the terminated employee's effective termination date from the HR distribution list. General Services Unit will work with other departments involved in the employee termination process to ensure the terminated employee car pool vehicle account is disabled in a timely manner, as well as establish a formal written SOP addressing disabling terminated employees car pool vehicle account. (Roland Francois Jr., Director of General Services)

- In the time since the audit was conducted, notification has improved and internal processes have been adapted to prioritize these requests. Furthermore, Security and Emergency Management Unit (S&EM) will work with other departments involved in the employee termination process to ensure the terminated employee physical access is disabled in a timely manner, and to assist in the process of SOP's development / modifications. S&EM will develop written dedicated SOPs for the process of disabling physical security access for MassDOT and MBTA terminated employees, as well as a dedicated SOPs for alarm system access policies. RMV needs to request disabling of alarm code for terminated employees that have access. (Nick Boyd, Acting Director Security and Emergency Management)

- Someone must take responsibility for this control. IT is a small part of this process and we are open to changes and improvements. There are many other people with access similar to employees and they should also be considered in a holistic solution. (Gary Foster, Chief Information Officer)

- There is a policy in place since September 26, 2007, entitled Employment Separations. While this policy addresses some of the procedures for separating an employee from the MBTA, the policy needs to be updated and standard operating procedures (SOPs) must be established to reflect current practices in terminations of (affiliated and unaffiliated) employees. (Vincent Reina, Director of Employee Availability) / (Juan Concepcion, Director of Policy and HR Communications)

Information Security / Physical Security

Management Responses (Continued):

- The HR Terminated Employees (MassDOT) report has been moved to twice weekly to limit potential gaps. The report is also prospective, and identifies employees in advance of their date of separation. With HR moving to a service center model, supervisors will also have a single point of contact to identify separating employees to, limiting potential communication gaps. With this change, HR will document a standard operating procedure for terminated employee notification and distribute to impacted business units. This process is scheduled for additional review as a component of the HR Strategic Plan's focus on Process Simplification. At present, the plan is to share a revised (as needed) process as part of the HR Navigator tool or as a component of the planned HR Self-Service Platform, during FY 2019 (Matthew Knosp, Assistant Director of Human Resources /Juan Concepcion, Director of Policy and HR Communications)

- Our current process is documented in the MBTA Help Desk Run Book. We will work with applicable business units to modify / improve the employee termination process. The process written SOPs will be updated accordingly. (Christine McCarthy, Deputy Director, IT Infrastructure and Operations)

- The MBTA has identified the root cause of the access control issues as related to both process and technology. We are now working to prioritize and address the most pressing issues, while aligning our strategy to the longer-term vision of identity access management. (Nick Easley, Chief Transformation Officer, MBTA)

Implementation Dates:

Completed (GS)
Completed 05/2018 (RF)
11/2018 (NB)
06/2018 – FY 19 (VR)(MK)(JC)
Completed 05/17/18 (C.McCarthy)
12/01/2018 (NE)

Information Security / Physical Security

13) Issues:

1) When a MassDOT or MBTA employee is temporary suspended, the following access occasionally is not disabled:
   - a) Security Alarm System
   - b) Physical security access (access control panels on doors)
   - c) Local Area Network (LAN) access
   - d) Car pool access

2) There is no formal, consistent process in place to disable all access for suspended employees (including physical, system, and car pool access).

Management Responses:

- Determination to remove access during a suspension should be handled on a case by case basis, including a review of situation-specific factors. MassDOT Labor Relations and Human Resources will work together to develop a risk assessment matrix, and a communications process to notify impacted departments (e.g., IT, Security, Facilities) when suspended employees should have access disabled based upon the results of the risk assessment. This process will be documented in standard operating procedures and distributed to impacted business units. (Matthew Knosp, Assistant Director of Human Resources / Maria Rota, Deputy Director Labor Relations (MassDOT) / Juan Concepcion, Director of Policy and HR Communications)

- Facility alarm codes (a) are reviewed and removed for management-level employee terminations and suspensions upon notification being made to the Security Department. For all other employees, the assumption is that there is no alarm code and we request notification, if this is not the case, so it can be addressed. For the purpose of this report, we recommend RMV Branch Operations conduct an audit of alarm codes at each location; if they are amenable to this proposal, we can provide the necessary reports/information for this purpose. Any code that has not been used for more than 45 days could be removed and a new code will need to be formally requested, should one be needed. For suspensions (b), we process disabling of access for all suspensions that are reported to us. However, in practice, few departments report them.

Information Security / Physical Security

Management Responses (Continued):

- (Continued) A related concern is barring of any facility access for any employees that have been suspended or terminated with cause for concern for safety/violence. When such suspension or termination situations are reported to us, we complete a form and provide it with a photo of the employee to 10PP for posting at the Security Desk and visitor station. In addition, we are working on a new process to roll out similar notifications to HWY District Offices and RMV Service Centers / Offices and will develop an SOP to this end. (Nick Boyd, Acting Director Security and Emergency Management)

- The Progressive Discipline Policy will be reviewed by MBTA Labor Relations and Policy, within the next 6-12 months, to consider corrective steps. (Ahmad Barnes, Director of Labor Relations (MBTA))

- HR needs to define suspension guidelines and set process/procedure for IT to follow. Once done, we will follow guidelines. (Harri Rosenberg, Director of IT Operations)

- General Services Unit to immediately cancel the 10 Park Plaza motor pool vehicle account of the suspended employee's effective suspension date (if the General Services Unit is notified of the employee suspension). General Services Unit will work with other departments involved in the employee suspension process to ensure the suspended employee car pool vehicle account is disabled in a timely manner, as well as establish a formal written SOP addressing disabling suspended employees car pool vehicle account. (Roland Francois Jr., Director of General Services)

Implementation Dates:

09/2018 (MK)(MR)(JC)
12/2018 (NB)
11/2018 – 05/2019 (AB)
Completed 05/2018 (RF)

Information Security / Physical Security

14) Issues:

1) Due to space limitations, there are multiple RMV branch locations where servers used for software distribution of vital security software (such as anti-virus and patch updates) are not stored in a room specifically designated for server storage.

2) Furthermore, there are instances where the servers that are located in these rooms are not stored in locked security server cabinets. Since these rooms are used for purposes other than to store IT servers, various non-IT personnel have access to these rooms.

Management Responses:

- See action note already in document. (Sarah Zaphiris, RMV Chief Administrative Officer)

- IT Network equipment in the following service centers is not installed in locked cabinets or in a separate designated location for IT equipment due to space limitations within each of these Service Centers:
  - Roslindale - cash room/ manager office
  - Nantucket - manager office
  - Pittsfield - lunch room

  Unless additional space or a designated room is provided to IT, we will not be able to meet this requirement. IT will work with the General Services group to determine the feasibility of gaining additional space for this purpose. (Frank Spada, Director, Intelligent Transportation Systems)

- The RMV service center servers are no longer needed for start of day support. We plan to remove the servers in the Service Center offices by the end of the year. A PC for software distribution/patch management will replace them. These are a much smaller form factor. To create locked areas for these is a General Services task. IT will work with General Services to coordinate implementation. (Harri Rosenberg, Director of IT Operations)

- General Services will work with IT to coordinate implementation. In locations with space limitations and/or restrictions the IT Dept. will be required, at times, to purchase a locked cabinet (Roland Francois Jr., Director of General Services).

Implementation Dates:

12/31/18 (HR)
12/31/18 (RF)