Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued April 23, 2020

Massachusetts Bay Transportation Authority

For the period January 1, 2017 through March 15, 2019

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

April 23, 2020

Ms. Stephanie Pollack, Secretary and Chief Executive Officer
Massachusetts Department of Transportation
State Transportation Building
10 Park Plaza, Suite 4160
Boston, MA 02116

Dear Secretary Pollack:

I am pleased to provide this performance audit of the Massachusetts Bay Transportation Authority (MBTA). This report details the audit objectives, scope, methodology, finding, and recommendations for the audit period, January 1, 2017 through March 15, 2019. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the MBTA for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Steve Poftak, General Manager, MBTA
Jeff Gonneville, Deputy General Manager, MBTA
David Abdoo, Chief of Staff, MBTA
Todd Johnson, Chief Operating Officer, MBTA
Nick Boyd, Acting Director of Security and Emergency Management, MBTA
Kenneth Greene, Chief of Police, MBTA
Joseph Aiello, Chair, Fiscal and Management Control Board

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ID	identification
HR	Human Resources Department
HR/CMS	Human Resource / Compensation Management System
MBTA	Massachusetts Bay Transportation Authority
OSA	Office of the State Auditor

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of the Massachusetts Bay Transportation Authority (MBTA) for the period January 1, 2017 through March 15, 2019. When testing security access privileges, we extended the audit period through June 29, 2019, capturing data in the MBTA's security access control system database as of the time of our fieldwork. Some testing required physically observing the then-current status of security controls at MBTA bus and rail maintenance facilities. This included conducting unannounced inspections of these facilities between May and July 2019. Specifically, when we assessed the physical condition of perimeter fencing, our last inspection was on July 1, 2019.

The vehicles owned and used by the MBTA are stored and serviced at maintenance facilities located throughout the Commonwealth. Effective physical security controls at these facilities are essential to the MBTA's ability to protect its customers and employees and to safeguard its most critical assets.

The objective of this audit was to determine whether the MBTA had sufficient physical security measures in place to prevent unauthorized access to its vehicle maintenance and storage facilities.

Our audit of the MBTA identified information that has been omitted from this report in accordance with Exemption (n) of the Commonwealth's public records law (Section 7[26] of Chapter 4 of the General Laws), which requires the withholding of certain records, including security measures or any other records related to cybersecurity or other infrastructure, if their disclosure is likely to jeopardize public safety or cybersecurity.

In accordance with Sections 7.39 and 7.41 of the Government Accountability Office's *Government Auditing Standards*, as well as OSA policies, for reporting confidential and sensitive information, we have given a separate, full report to the MBTA, which will be responsible for acting on our recommendations.

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1a **Page 10**	The MBTA did not ensure that employee access identification (ID) cards were retrieved and destroyed when employees left the agency.
Finding 1b **Page 11**	Security access was not disabled promptly.

Recommendations Page 13	1. The MBTA should perform an immediate review of the status of all employees and deactivate security access for those who no longer require access and/or are not authorized to have it. 2. The MBTA should develop and implement an authority-wide policy and detailed procedure for the processing of terminated employees. At a minimum, it should address the frequency of exit interviews; individual department roles; the processing of required separation documentation; and the retrieval, disabling, and destruction of employee access ID cards within a defined timeframe. Supporting documentation should be kept on file for returned and destroyed cards. 3. The MBTA should develop and implement monitoring controls to ensure that security access for separated employees is promptly disabled.

Post-Audit Action

In response to this audit report, the MBTA provided the following comments related to its post-audit actions.

The draft audit report accurately captures many issues that were prevalent during the audited period. The MBTA would like to point out that since the audited period, internal audits and self-recognition of challenges have already produced substantial progress or even resolutions related to most of the recommendations suggested. These include:

- *The MBTA expects to launch . . . an identity management solution, in February 2020. [The solution] will integrate disparate systems across [the Human Resources Department], [the Information Technology Department], and Security allowing new hire, termination, and related activity to be automatically reported and in some cases acted upon across departments with shared responsibilities in this area.*

- *During the audit period, the MBTA had already independently conducted a comprehensive internal audit of its . . . electronic access control system, culminating in improved processes, documentation, and system integrity. [The system] is the technology platform the MBTA uses for electronic access control hardware and software relating to door and gate access using identification cards/badges.*

- *Since 2018, the MBTA has adopted [a] platform to streamline and improve tracking of access and badge requests. This deployment took place in two phases, beginning with a backend tracking interface in 2018 and followed by a user-facing web portal in 2019. The portal by itself has reduced the average time it takes to process a badge or access related request by 60%. . . .*

Already, the MBTA's security investments over the past decade have resulted in one of the largest and most innovative transit security systems in the country. While these deployments span most of the Authority's facilities, more work remains to be done—and is being done:

- *The MBTA has identified a prioritized list of facilities and stations and continues to actively deploy security upgrades expediently as funding and resources allow.*

- *The MBTA's security investments are further informed by a comprehensive Threat & Vulnerability Assessment that was commissioned by the MBTA and conducted by a private security consultant in 2018.*

- *The specifics of each security project are defined by the MBTA's security standard specification, which was developed in consultation with security consultants and is used to guide all deployments and configurations relating to security cameras, access control, fencing, and gates.*

OVERVIEW OF AUDITED ENTITY

The Massachusetts Bay Transportation Authority (MBTA) was created in 1964 pursuant to Chapter 161A of the Massachusetts General Laws. The agency provides services via its rapid transit system, commuter rail service, bus service, ferry routes, and transit service for people with disabilities. According to its website, the MBTA is not only the largest public transportation system in the Commonwealth but also "one of the largest public transit systems in the country, serving nearly 200 cities and towns and over 1 million daily riders on the subway, bus, ferry, and Commuter Rail."

Although the MBTA Transit Police Department has the primary responsibility for monitoring and ensuring security on the MBTA, MBTA management explained to us that physical security at the MBTA is a shared service and multiple departments have critical roles. The Security and Emergency Management Department programs and activates employee access identification (ID) cards to work on the access control system. The Automated Fare Collection Department issues MBTA employee access ID cards. The Transit Facilities Maintenance Department maintains fencing, physical doors and door hardware, and non-motorized facility gates.

Vehicle Maintenance

The MBTA operates 10 facilities that house and maintain its current fleet of buses. Employees at these facilities clean, inspect, repair, refuel, and service the MBTA's 1,002 active buses. According to MBTA management, 8 of these facilities operate 24 hours a day, seven days a week; the other 2 operate 24 hours a day, five days a week.

The MBTA performs service, inspection, and repair on its trains at 13 additional facilities. Trains return to these facilities at the end of the day and are shut down, cleaned out, and made ready for the next day's service. Essential train supplies and excess parts are also stored at these facilities.

Employee Access ID Cards

All MBTA employees are issued employee access ID cards, which must be visibly worn at all times while employees are on duty. These cards confirm employees' affiliation with the MBTA and are used by the MBTA to control access to restricted areas of facilities and buildings equipped with card readers.[1] As an

1. A card reader scans employee access identification cards to determine whether employees have the correct access privileges to physically open the door or gate controlled by the card reader.

employee benefit, each card is also embedded with an MBTA CharlieCard chip granting free, unrestricted use of the transit system. Upon collection of their employee access ID cards, retirees are issued new retiree ID cards, granting free transportation for life.

Card Reader Access Control System

At the time we initiated our audit work, seven of the MBTA's vehicle maintenance facilities used an electronic access control system to monitor and control access to secured areas within facilities. This system manages and maintains data pertaining to employee security access privileges and employee access ID cards. The MBTA has installed card readers at perimeter gates, building and perimeter entrances and exits, and other internal and external points at these facilities. This system allows authorized employees to enter through secured areas conveniently without needing to use physical keys.

In addition to controlling access, the electronic access control system can be programmed to provide door alarm monitoring to detect improper use of the system. Each door is individually evaluated during installation to determine the need for an alarm and the protocols after triggering, including who should respond.

Employee Separation Process

Several parties are involved when an employee separates from the MBTA. The Human Resources Department (HR), the Automated Fare Collection Department, the Security and Emergency Management Department, and other departments all play critical roles in the processing of exit forms and the disabling of access to vital MBTA systems.

When employees separate from the MBTA, they are to return all MBTA property, including their employee access ID cards, to their supervisors during exit interviews. Supervisors complete required separation forms, including an "Inventory Reclamation Sheet," documenting the collection of any MBTA property. Completed separation forms and any returned property are turned in to HR. HR physically delivers returned employee access ID cards to the Automated Fare Collection Department, where they are placed in secure bins and discarded.

Upon receiving separation information from department heads, HR enters it in the Commonwealth's official payroll system (the Human Resource / Compensation Management System), processing the

employee termination. At this point, the employee's name will appear on a termination report that is distributed to the appropriate parties across the MBTA, including the Automated Fare Collection Department (which is responsible for disabling individuals' free transportation benefit or issuing new ID cards to retirees) and the Security and Emergency Management Department (which is responsible for disabling terminated employees' physical access).

Perimeter Security Fencing

At the time we initiated our audit work, 20 of the MBTA's vehicle maintenance and storage facilities had perimeter security fencing systems in place. Physical barriers, such as fencing systems, are a core component of an agency's access control system. According to the American Public Transportation Association's *Recommended Practice: Fencing Systems to Control Access*, a fencing system "defines boundaries and limits . . . channels access and egress, provides visual barriers, supports security and safety, and can deter and delay intrusion and trespassing."

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Massachusetts Bay Transportation Authority (MBTA) for the period January 1, 2017 through March 15, 2019. When testing security access privileges, we extended the audit period through June 29, 2019, capturing data in the MBTA's security access control system database as of the time of our fieldwork. Some testing required physically observing the then-current status of security controls at MBTA bus and rail maintenance facilities. This included conducting unannounced inspections of these facilities between May and July 2019. Specifically, when we assessed the physical condition of perimeter fencing, our last inspection was on July 1, 2019.

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.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Does the MBTA have physical security measures to prevent unauthorized access to its vehicle maintenance and storage facilities? Specifically,	
a. Are the security access privileges of separated employees promptly disabled?	**No; see Finding 1b**
b. Are employee access identification (ID) cards retrieved and destroyed when employees leave the agency?	**No; see Finding 1a**
c. As of July 1, 2019, was perimeter security fencing in proper working condition?	**Yes**

To achieve our audit objectives, we gained an understanding of the internal controls we deemed significant to our audit objectives by reviewing agency policies and procedures, as well as conducting interviews and observations. In reviewing data pertaining to MBTA employee access ID cards, we

identified an issue regarding the timeliness with which former employees' free transportation benefit was disabled (Other Matters).

To obtain sufficient, appropriate audit evidence to address our audit objectives, we conducted further audit testing as follows:

- To determine whether the security access privileges of separated employees were promptly disabled, we performed the following procedures:
  - We were provided with a list from the Commonwealth Information Warehouse[2] of all 1,091 MBTA employees who separated from the agency (via termination or retirement) during our audit period. We also obtained a copy, as of June 29, 2019, of the MBTA's entire security access control system database. We then matched information in the database to the list of separated employees by linking each employee's unique Human Resource / Compensation Management System (HR/CMS) ID number. Of the 1,091 separated employees, 906 had corresponding HR/CMS employee IDs in the security access control system database. The HR/CMS ID numbers of the other 185 did not appear in the security database.[3]
  - We then identified all instances where an individual on the separation report had an employee access ID card that either was still active or had been deactivated more than a day after the employee's effective date of termination. We identified a total of 853 cards, assigned to 785 distinct individuals.[4] For each of the 853 cards identified, we calculated the amount of time between the individual's effective date of termination and the date the card was deactivated. Further, we reviewed access control system data to determine whether any separated employees accessed agency facilities after their effective dates of termination.
- We selected a nonstatistical random sample of 65 of the aforementioned list of 1,091 employees and reviewed supporting documentation (such as employee exit interview forms, other human resource documentation, and Automated Fare Collection Department records) to determine whether their employee access ID cards had been retrieved upon separation and ultimately destroyed. For instances where the separated employee did not return a card, we looked for evidence to determine whether the MBTA had taken any additional action to collect the card.
- We performed an unannounced visual inspection at each of the 20 vehicle maintenance and storage facilities that had perimeter security fencing systems in place at the time of our audit to

2. The Commonwealth Information Warehouse is a central data repository for the financial, budgetary, human resource, payroll, and time reporting information that is maintained in separate systems by individual agencies.
3. In its response to our audit report, the MBTA suggested that HR/CMS numbers not appearing in the security database could be caused by the individual never having had or needed physical access, or by the number not being captured or not being correct in the MBTA access control system.
4. In response to our report, the MBTA asserted that there is, and can be, only one active card per cardholder record in the system at all times. Some individuals have inactive prior cards, which could account for the larger number of cards compared to the number of individuals.

determine whether the fencing systems were in proper working condition (i.e., had no visible signs of damage).

Whenever sampling was used, we applied a nonstatistical sampling approach, and as a result, we could not project our results to the entire population.

Data Reliability

To determine the completeness and accuracy of the list of employees who separated from the agency during the audit period, supplied to us by the MBTA, we compared it to a list of current employees. We also traced the data provided to us to original source documents, such as employee exit interview forms and other human resource documentation, for accuracy. Further, we performed other electronic tests of the data and made relevant inquiries. We determined that the data were sufficiently reliable for the purposes of this audit.

To determine the completeness and accuracy of the list of vehicle maintenance and storage facilities supplied to us by the MBTA, we reconciled the list to an MBTA-commissioned maintenance efficiency study obtained from the MBTA's website. In addition, we interviewed agency officials who were knowledgeable about the facilities to obtain their assessments of the reliability of the list and conducted site visits to each location. We determined that the data were sufficiently reliable for the purposes of this audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. Physical security vulnerabilities exist at the Massachusetts Bay Transportation Authority's bus and rail maintenance facilities.

The Massachusetts Bay Transportation Authority (MBTA) did not ensure that employee access identification (ID) cards were retrieved and destroyed and that security access was disabled promptly when employees left the agency. As a result, the facilities were vulnerable to unauthorized access, placing the security and safety of MBTA property, passengers, and employees at risk.

a. The MBTA did not ensure that employee access ID cards were retrieved and destroyed when employees left the agency.

During our audit period, the MBTA did not consistently maintain documentation to substantiate that it physically retrieved and destroyed the employee access ID cards of separated employees. Specifically, of the 65 former employees' files we reviewed, only 19 (29%) contained documentation indicating that the card had been returned to the MBTA. None of the 65 employees' files contained any documentation indicating that the card had been physically destroyed.

Former MBTA employees or other unauthorized individuals in possession of MBTA employee access ID cards could have access to secured areas of the MBTA. Unauthorized individuals using these cards would significantly increase the MBTA's vulnerability to unauthorized access and potentially a wide variety of criminal acts. For instance, although a card may be deactivated (not allowing access to doors and gates), it could still be presented at security checkpoints, including at MBTA stations or on vehicles not equipped with automated fare gates, potentially allowing a person to avoid screening and/or be admitted for free.

Authoritative Guidance

MBTA's "Employment Separations" policy states,

> *Whenever practicable, employees who separate from the Authority should complete the Exit Interview Process as established by the Authority. As part of this process or otherwise, employees are required to promptly return any Authority property (e.g., vehicles, tools, electronics, badges, cards, etc.) that may be in their control, possession or custody.*

The MBTA *Employee Policy Manual* requires employees to return all property, including their employee IDs, upon leaving the agency and states that the MBTA reserves the right to withhold any

final payment due an employee until the property is returned. Through discussions with MBTA management, we determined that the MBTA had established a practice of retrieving and destroying the employee access ID cards of separating employees. Recognizing the importance of collecting cards upon separation, the MBTA has developed an "Inventory Reclamation Sheet" that is supposed to be used to document whether a separating employee's card has been collected. Although MBTA policies do not specifically require the MBTA to document the destruction of collected cards, we believe it is important that this part of the separation process be completed in every case.

Reasons for Issue

The MBTA does not have adequate policies, procedures, and monitoring controls to ensure that employee access ID cards are returned and destroyed when employees leave the agency. Although employees are encouraged to participate in an exit interview on or before their last day of employment, MBTA officials told us that this interview is not mandatory and is not consistently conducted.

Based on our discussions with MBTA officials and review of policies, there was inconsistency regarding when exit interviews are conducted. MBTA's Human Resources Department (HR) told us that exit interviews are not conducted for retirees, discharged employees, or interns. However, the MBTA's documented "Exit Interview Package Guidelines" state that the interview is "mandatory" and "must be conducted prior to or on the employee's last day." These guidelines also state that even if an employee does not show up for an exit interview, a supervisor should still fill out and process the exit interview paperwork for the employee. There is even a page of the exit interview paperwork that asks employees to specify whether their reason for separation is "resignation," "retirement," or "other," indicating that the process is in fact completed for retirees.

In addition, there is no documented guidance available to employees that specifies procedures to be followed when an employee is separated from the MBTA.

b. Security access was not disabled promptly.

The MBTA was significantly delayed in terminating former employees' security access by deactivating their employee access ID cards. The delays gave individuals continued access to MBTA facilities and properties for months and even years after separation.

Specifically, the MBTA did not disable the security access of 47 employees who left the agency during our audit period. These former employees retained unauthorized general perimeter access[5] to MBTA facilities for periods ranging from 108 to 717 days after separation.

In cases where the MBTA did disable the security access of terminated employees, we found significant lag time between employees' termination dates and the dates their security access was disabled. We reviewed security access control system data and found that it took as long as 626 days after separation for these employees' access to be disabled. On average, it took 136 days.

The table below summarizes the lag times between employees' termination dates and the dates their security access was disabled.

Security Access Removal Lag Time

Days before Security Access Was Disabled	Number of Employee Access ID Cards	Percentage of Total
2–30	220	27%
31–60	64	8%
61–100	105	13%
101–300	318	39%
301–500	93	12%
501+	6	1%
Total	806	100%

Former employees with unauthorized access to secure areas of MBTA facilities could put MBTA facilities and property, and the safety of its workers, at risk. As a result of this issue and the issue discussed in Finding 1a, we found 85 instances (involving 35 individuals) where former MBTA employees physically accessed MBTA facilities after their effective termination dates.

Authoritative Guidance

As a best practice to prevent unauthorized access, it is critical that security access be promptly disabled upon an employee's termination. Many organizations endorse such a practice; for instance, the National Institute of Standards and Technology's *Special Publication 800-53r4* states that upon

5. This is the basic security access level assigned to any authorized MBTA employee. It includes access to perimeter facility gates and non–critical infrastructure card readers.

termination of a person's employment, organizations should "[terminate/revoke] any authenticators/credentials associated with the individual."

Reasons for Issues

The MBTA has not established authority-wide policies and procedures for the processing of terminated employees.

The MBTA also has not established adequate monitoring controls to ensure that security access for separated employees is promptly disabled. Further, the MBTA has not established a specific timeframe for the revocation of security access for separating employees.

MBTA officials told us that there was a breakdown in communication between HR and the Security and Emergency Management Department. Before October 2018, notifications of employee terminations from HR to the Security and Emergency Management Department were sporadic and inconsistent. Starting in October 2018, HR began communicating employee terminations to the Security and Emergency Management Department daily.

Upon receiving separation information from department heads, HR enters it in the Human Resource / Compensation Management System, processing the employee termination. At this point, the employee's name will appear on a termination report that is distributed to the Security and Emergency Management Department, which is responsible for disabling terminated employees' physical access. However, MBTA officials also told us that separation documentation that is necessary to finalize an employee separation is not always submitted to HR promptly and that this delays the process.

Recommendations and MBTA Responses (Italicized)

1. The MBTA should perform an immediate review of the status of all employees and deactivate security access for those who no longer require access and/or are not authorized to have it.

   This has already been done via an internal audit: in addition, the in-progress . . . identity management initiative will ensure consistency going forward for employees.

2. The MBTA should develop and implement an authority-wide policy and detailed procedure for the processing of terminated employees. At a minimum, it should address the frequency of exit interviews; individual department roles; the processing of required separation documentation; and the retrieval, disabling, and destruction of employee access ID cards within a defined timeframe. Supporting documentation should be kept on file for returned and destroyed cards.

The MBTA agrees with the recommendation and will assess the best means to expediently implement a solution.

3. The MBTA should develop and implement monitoring controls to ensure that security access for separated employees is promptly disabled.

   [The identity management solution] integration with [the electronic access control system] will fully address this concern and is expected to be operational in February of 2020.

Additional Auditee Responses

In addition to the comments above, the MBTA provided specific comments about some of the issues identified.

Finding 1b

During the audited period, a separate internal audit was conducted which resulted in a large number of cardholder deactivations; this severely skews the data on average time to disable a card. The internal review period was from October 2017 to October 2018. Since that review, the MBTA has changed the request and tracking processes to an online ticketing system. . . . The audit results do not account for these changes, which occurred after October 2018.

Cardholder deactivations depend on timely flow of information between departments, which can vary due to a variety of factors.

Some of the 47 employees referenced as having not been disabled despite leaving the Authority may have transitioned from employee to contractor, or to MassDOT / Shared Service roles, which would leave their original employee ID in the system, even if their card type changed (which it typically would).

Since the MBTA's use of [an online ticketing system] for security related requests began, the turnaround time is an average of 1–2 days for access-related requests, with termination reports being a priority ticket. . . .

[The identity management solution] will automate and create a 24-hour process. High risk terminations are, and will continue to be, processed immediately by manual request.

Auditor's Reply

Finding 1b

The results of our audit testing in this area are based on information that we obtained from the MBTA and the systems that were used to administer the employee termination process during our audit period. Whether or not the average time to deactivate a card was somehow skewed, a problem exists in this area that needs to be addressed by the MBTA.

As noted in our report, the MBTA did not disable the security access of 47 employees who left the agency during our audit period. In their response, MBTA officials indicated that some of these 47 employees may have transitioned from employee to contractor or to MassDOT / Shared Service roles. However, upon identifying this issue, we provided a list of the 47 employees to HR, which confirmed that each person had been terminated and was no longer working in any capacity at the MBTA. Thus there was no indication that these individuals should have had access to MBTA facilities at the time of our audit work.

Based on its response, the MBTA is taking appropriate measures to address our concerns.

OTHER MATTERS

The free transportation privileges of separated Massachusetts Bay Transportation Authority employees were not promptly disabled.

Although this matter was not part of the audit objectives, we found that the Massachusetts Bay Transportation Authority (MBTA) did not disable the free transportation benefit of 76 former employees. These terminated employees remained active in the MBTA's automated fare collection system as of the time of our fieldwork, September 2019. They had unauthorized free transportation for periods ranging from 128 to 946 days after separation. In addition, we identified 2,594 instances (representing 51 distinct individuals) where former employees were granted free fare access after their effective dates of termination. Thus, former employees received free transportation to which they were not entitled. We estimated at least $5,517 in lost revenue for the agency. Since the MBTA's automated fare collection system only stores records for 14 months, we could not determine the extent of the problem throughout the entire audit period.