Board of Trustees

Audit Committee

October 21, 2024
3:00 p.m.
Via Zoom

A live stream of the meeting for public viewing will also take place at the following link: https://www.westfield.ma.edu/live

---

Committee Members Present: Committee Chair Theresa Jasmin, Vice Chair William Reichelt, Secretary Michael O'Rourke, Members: Melissa Alvarado, Tessa Lucey, and Dr. Gloria Williams.

Also present and participating were Westfield State University President Dr. Linda Thompson, Administration and Finance Vice President Stephen Taksar; Associate Vice President Financial Accounting Lisa Freeman; Associate Vice President Administration and Finance, Maria Feuerstein; Vice President of Institutional Advancement, Lisa MacMahon; Director of Emergency Response and Risk Management, Sam Lemanski; and Director of Dining Services, Melissa Sikes. Also present from WithumSmith & Brown PC were Ryan Sheehan and Kate Jun. From Boston Consortium were Mike Santolucito and Samantha Spezeski.

Committee Chair Theresa Jasmin called the meeting to order at 3:00 p.m., conducted a roll call of committee members, and stated the meeting was being livestreamed and recorded.

MOTION made by William Reichelt second by Gloria Williams to approve the meeting minutes of June 20, 2024 with a notable change to be made. A roll call was completed, O'Rourke and Jasmin abstained. M**otion passed with majority.**

Ryan Sheehan started off with the required communication for the auditor's responsibility under GAAS, manager's responsibility, and finding. He then moved on the financial statements where a comparison between 2023 to 2024 showed a clean audit with no findings. (See attachment FY24 Financial Statements for further information)

MOTION made by Trustee Williams and seconded by Trustee Reichelt to recommend to the full Board to approve To accept the annual report for fiscal year ending June 30, 2024, as prepared by the university's Administration and Finance Division and to authorize the submission of this report to the State Comptroller's Office, the Massachusetts Department of Higher Education, and the State Auditor's Office, as required by the Massachusetts Department of Higher Education. This annual report includes the Westfield State University FY24 Financial Statements, audited by WithumSmith and Brown, P.C. There being no further discussion, a roll call was taken, **motion passed unanimously.**

FY25 Internal Audit

Samantha Spezeski, Director of Internal Audit at the Boston Consortium, shared a list of potential internal audit projects for Westfield State University (see FY25 Internal Audits attachment). A brief history of how Westfield State came upon having a relationship with Boston Consortium was described to the Board. Samantha discussed that the University has 500 hours for the year and how they came up with the list tailored to Westfield State. Opinions were given on which internal audit would be best for the campus.

MOTION made to recommend to the full Board To approve the Internal Audit Service (Boston Consortium) area of focus for the fall semester 2024-2025 be key control & security (Building Access) and Accounts Payable in the Spring of 2025. There being no further discussion, a roll call was taken, **motion passed unanimously.**

Audit Tracker

Steve Taksar, Vice President for Administration and Finance, discussed last year's completed two audits, students accounts and the grants office. He referred to the attachment Internal Audit Recommendations Tracker and spoke about the progress made towards any findings by Boston Consortium and management's progress. This report will be provided twice per year as updated information will be included. VP Taksar asked the committee for any suggestions on the structure of the report going forward.

Enterprise Risk Management

Sam Lemanski, Director of Emergency Planning and Risk Management, was introduced to the Audit Committee and a brief work history was explained along with his job duties. A few years ago, an assessment was made to identify the top 10 risks to the university. The list was recently reevaluated by the Cabinet resulting in 8 institutional risks with a specific focus on the top three for FY24, which are enrollment management, cyber risk, and deferred maintenance. Sam Lemanski discussed naming a lead person to take charge of a specific risk to conduct an assessment, develop a plan, and a written strategy to manage the risk. Westfield State is already proactively managing these risks but does not have a formal framework. The Enterprise Risk Program will provide the model moving forward.

There being no further business, **MOTION** made by Trustee Williams and seconded by Trustee O'Rourke to adjourn the meeting. There being no discussion, **motion passed unanimously**. Meeting adjourned at 4:30 p.m.

Attachment(s):

a. Minutes 6-20-24 (Draft)
b. Motion – FY24 Financial Statements
c. FY24 Financial Statements (Required Communication)
d. FY24 Financial Statements (Draft)
e. FY25 Internal Audits
f. Audit Tracker
g. Enterprise Risk Management

Secretary's Certificate

I hereby certify that the foregoing is a true and correct copy of the approved minutes of the Westfield State University Board of Trustees, Audit Committee meeting held on October 21, 2024.

_____ _____

Michael O'Rourke, Secretary Date

Audit Committee Cybersecurity Update

Alan Blair
Chief Information Officer
Chief Information Security Officer

December 9, 2024

Statewide Collaboration

Higher Education Cybersecurity Coordinating Committee	• Mission • Leadership • Future
Cyber Dashboard	• Holistic and Individual Look • Peer Benchmarking • Self and External Assessment

Financial Investment

Future Tech Act PACE

Investment of $1.6m

- $67k for Westfield State (1/24th)
- Directed towards Assessments, Reviews & Detection

Westfield State

Investment $185k

- Directed towards Endpoint (EDR), Managed (MDR) and Extended (XDR) Detection and Response, Perimeter Defense and Education and Training

Centralized Security Training

Leading the Charge

Local & Statewide Adoption

- Westfield State was the first to implement the KnowBe4
- 23 of the 24 have now adopted KnowBe4
- Human Resources Integration
- Leveraged state collective purchasing to lower annual cost by 60%

Impact CBA

- Led by CIOs from Westfield State, Salem State and Bridgewater State, we participated in midterm bargaining (MSCA)
- Resulted in a requirement for Security Training for all faculty strengthening our cyber resilience

Shared Services Future Opportunities

Viewing the Landscape

- In collaboration with HECCC, Westfield State participated in a survey and direct meetings
- Developed a comprehensive inventory of shared services, challenges and models to address the future of cybersecurity

Future Investment

- Groundwork is now laid for expanding our collaborative efforts
- Mutually beneficial for all 24

Challenges Ahead

- Increase in data breaches, especially third party, and the institution is liable for remediation
- More frequent large area surface attacks
- Phishing/Social Engineering have increased over 1,000% since 2020
- Insider threats due to lack of training and accountability
- The increase of Bring Your Own Device (BYOD)/Internet of Things (IoT) dependency and the proliferation of Artificial Intelligence (AI)
- Resource Constraints

Mitigation Strategies

Increase in Data Breaches

- Leverage legal counsel and Procurement for stronger contract language during vendor onboarding
- Network Segmentation – The “Moat Effect”
- Vendor Risk Management Program
- Cyber Insurance and Offsite Response Repositories

Large Surface Attacks

- Map Points of Entry and Defend Accordingly
- Zero Trust Principle
- Endpoint Detection and Response (EDR), Managed Detection and Response (MDR) , Extended Detection and Response (XDR)
- Assessment and Incident Response

Mitigation Strategies

Phishing Social Engineering	• Align policies with CIS (Center for Internet Security) Critical Controls and benchmark against them with cyber dashboard • Training • Simulations and Red table
Insider Threats	• Access Management • Refresher Training • Policy development and enforcement

Mitigation Strategies

Bring Your Own Device (BYOD)/Internet of Things (IoT) Artificial Intelligence (AI)	• Developing an Enterprise Risk Management Strategy • Mobile Device Management (MDM) platform • Strong Multifactor Authentication (MFA) • Vulnerability Management
Resource Constraints	• Continue to invest in proactive cyber security initiatives • Formulate a plan to hire 3 full time employees dedicated to Cyber Security

Questions?

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued November 8, 2024

Audit of Cybersecurity Awareness Training Compliance Across Multiple State Agencies

For the period July 1, 2021 through April 30, 2023

State House Room 230 ■ Boston, MA 02133 ■ auditor@massauditor.gov ■ www.mass.gov/auditor

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

November 8, 2024

Jason Snyder, Secretary and Commonwealth Chief Information Officer
Executive Office of Technology Services and Security
1 Ashburton Place, 8th Floor
Boston, MA 02108

Dear Mr. Snyder:

I am pleased to provide to you the results of the enclosed performance audit. Pursuant to our governing statute, Section 12 of Chapter 11 of the Massachusetts General Laws, our audit covers multiple entities' compliance with the Executive Office of Technology Services and Security's cybersecurity training standards. Specifically, the following entities were included as part of this comprehensive audit:

Executive Branch Agencies	State Colleges and Universities	Regional Transit Authorities
Executive Office of Technology Services and Security	Framingham State University	Cape Ann Transportation Authority
Bureau of the State House	Holyoke Community College	Cape Cod Regional Transit Authority
Civil Service Commission	Massachusetts Bay Community College	Martha's Vineyard Regional Transit Authority
Department of Labor Standards	Massasoit Community College	Nantucket Regional Transit Authority
Department of Mental Health	North Shore Community College	
Department of Public Health	Northern Essex Community College	
Department of Revenue	Westfield State University (WSU)	
Massachusetts Department of Transportation		
Group Insurance Commission		
Massachusetts Parole Board		
Registry of Motor Vehicles		
State 911 Department		

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2021 through April 30, 2023. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Executive Office of Technology Services and Security. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team have any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

911	State 911 Department
BSH	Bureau of the State House
CATA	Cape Ann Transportation Authority
CCRTA	Cape Cod Regional Transit Authority
CSC	Civil Service Commission
DLS	Department of Labor Standards
DMH	Department of Mental Health
DOR	Department of Revenue
DPH	Department of Public Health
EOTSS	Executive Office of Technology Services and Security
FSU	Framingham State University
GIC	Group Insurance Commission
HCC	Holyoke Community College
HRD	Human Resources Division
MassDOT	Massachusetts Department of Transportation
MBCC	Massachusetts Bay Community College
MCC	Massasoit Community College
MPB	Massachusetts Parole Board
NECC	Northern Essex Community College
NRTA	Nantucket Regional Transit Authority
NSCC	North Shore Community College
RMV	Registry of Motor Vehicles
VTA	Martha's Vineyard Regional Transit Authority
WSU	Westfield State University

EXECUTIVE SUMMARY

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 the Executive Office of Technology Services and Security (EOTSS), as well as 22 other executive branch agencies, state colleges and universities, and regional transit authorities. This audit covers the period July 1, 2021 through April 30, 2023 and includes the following agencies:

Executive Branch Agencies	State Colleges and Universities	Regional Transit Authorities
Executive Office of Technology Services and Security (EOTSS)	Framingham State University (FSU)	Cape Ann Transportation Authority (CATA)
Bureau of the State House (BSH)	Holyoke Community College (HCC)	Cape Cod Regional Transit Authority (CCRTA)
Civil Service Commission (CSC)	Massachusetts Bay Community College (MBCC)	Martha's Vineyard Regional Transit Authority (VTA)
Department of Labor Standards (DLS)	Massasoit Community College (MCC)	Nantucket Regional Transit Authority (NRTA)
Department of Mental Health (DMH)	North Shore Community College (NSCC)	
Department of Public Health (DPH)	Northern Essex Community College (NECC)	
Department of Revenue (DOR)	Westfield State University (WSU)	
Massachusetts Department of Transportation (MassDOT)		
Group Insurance Commission (GIC)		
Massachusetts Parole Board (MPB)		
Registry of Motor Vehicles (RMV)		
State 911 Department (911)		

The purpose of our audit was to determine whether EOTSS and the above executive branch agencies, state colleges and universities, and regional transit authorities ensured that their employees completed cybersecurity awareness training in accordance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010.

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

Finding 1 **Page 16**	EOTSS did not ensure that all of its employees completed cybersecurity awareness training.
Effect	If EOTSS does not ensure that all of its employees complete cybersecurity awareness training, then EOTSS may expose itself to an increased risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations **Page 17**	1. EOTSS should strengthen their policy to improve oversight of executive branch state agencies, including their timely completion of cybersecurity awareness trainings. 2. EOTSS should ensure that all employee training transcripts for all employees are maintained and include records regarding cybersecurity awareness training completion. 3. EOTSS should ensure that all of its employees complete cybersecurity awareness training within 30 days of orientation and annually thereafter. 4. EOTSS should establish procedures to monitor employee cybersecurity awareness training completion rates throughout the training cycle and use historical data retained by HRD to ensure that employees meet training deadlines.
Finding 2 **Page 18**	CSC, DLS, DMH, DPH, DOR, MassDOT, GIC, MPB, and RMV did not ensure that all of their employees completed cybersecurity awareness training.
Effect	If executive branch agencies do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.
Recommendation **Page 22**	The aforementioned nine executive branch agencies should do the following: 1. provide cybersecurity awareness training (both an initial training within 30 days of orientation and an annual refresher training thereafter) to all full-time employees, contractors, and interns; 2. establish procedures to monitor employee cybersecurity awareness training completion rates throughout the training cycle and use historical data retained by HRD to ensure employees meet training deadlines; and 3. implement additional controls to ensure that the new hire onboarding process includes all relevant coursework regarding cybersecurity awareness training.
Finding 3 **Page 26**	Seven state colleges and universities did not ensure that all of their employees completed cybersecurity awareness training.
Effect	If state colleges and universities do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations **Page 29**	1. The aforementioned seven state colleges and universities should update their cybersecurity awareness training policies to require this training for all employees. 2. The aforementioned seven state colleges and universities should update their cybersecurity awareness training policies to include consequences for non-completion (e.g., restriction of access until they complete the training).

Finding 4 **Page 32**	CATA, CCRTA, and VTA did not ensure that all of their employees completed cybersecurity awareness training.
Effect	If regional transit authorities do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.
Recommendations **Page 34**	The aforementioned three regional transit authorities should do the following: 1. update their cybersecurity awareness training policies to require this training for all employees and 2. update their cybersecurity training policies to include consequences for non-completion (e.g., restriction of access until training is completed).

OVERVIEW OF AUDITED ENTITY

The Executive Office of Technology Services and Security (EOTSS), located at 1 Ashburton Place in Boston, was established in 2017 in accordance with Section 2 of Chapter 7D of the Massachusetts General Laws. According to its website, EOTSS was created to "improve data security, safeguard privacy, and promote better service delivery across the Commonwealth." EOTSS operates under the direction of the Commonwealth's chief information officer, who is appointed by the Governor.

According to its website,

> *The Executive Office of Technology Services and Security (EOTSS) seeks to provide secure and quality digital information, services, and tools to customers and constituents when and where they need them. . . . EOTSS provides responsive digital and security services that enable taxpayers, motorists, businesses, visitors, families, and other citizens to do business with the Commonwealth. . . . EOTSS also oversees and manages the enterprise technology and digital infrastructure and services for over 125 state agencies and over 43,000 state employees. . . . Since its creation, EOTSS has made critical investments in infrastructure resiliency, unifying cybersecurity operations, and deploying a Standard Operating Environment (SOE) and technology architecture across all agencies. The organization has also collaborated with agencies to improve the centralized delivery of digital services for constituents, schools, businesses, government agencies, and municipalities.*

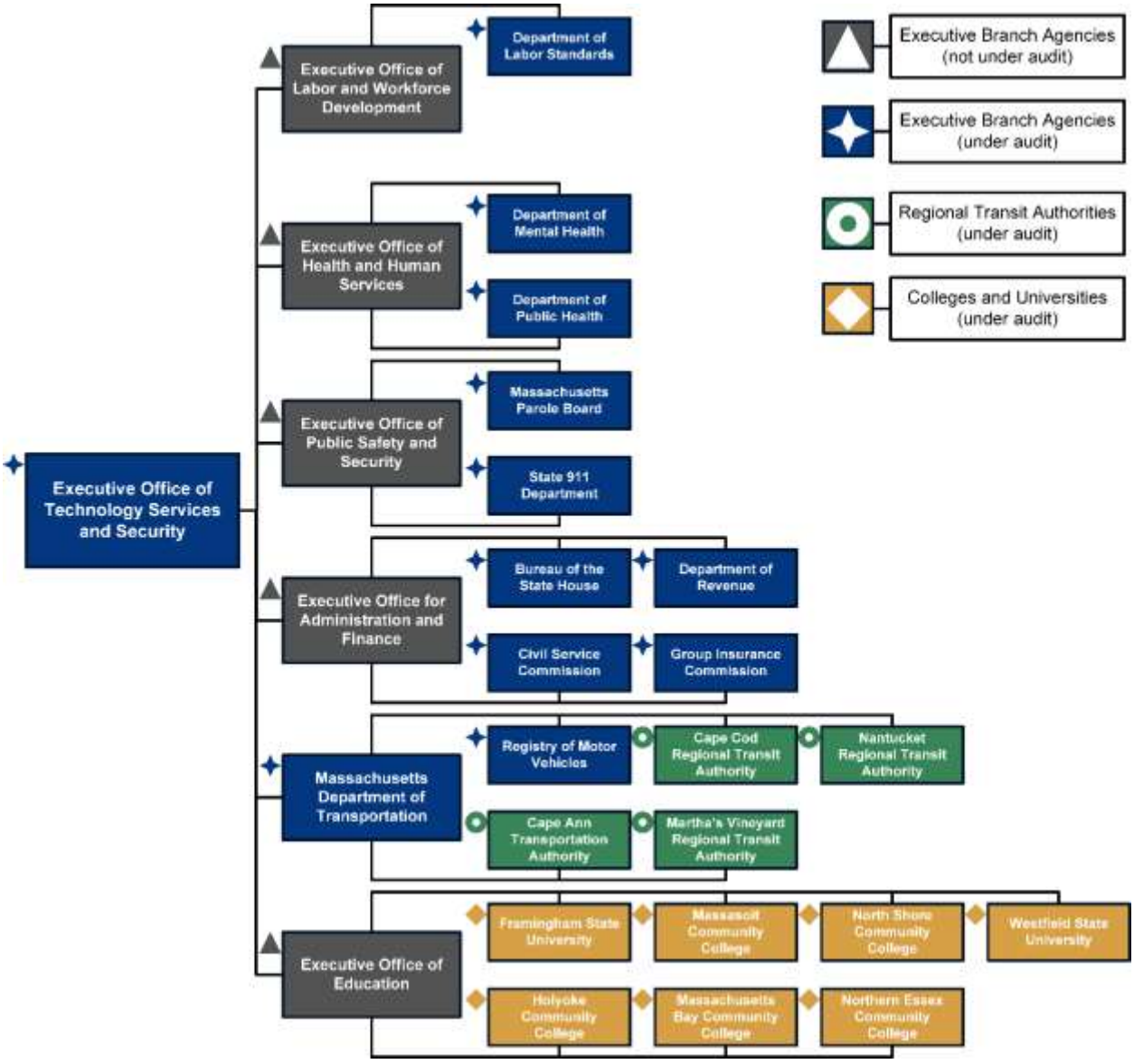
According to its website, EOTSS employed 452 full-time employees as of May 24, 2023.

Multi-Agency Approach

This report covers 22 additional agencies' compliance with EOTSS's cybersecurity awareness training standard. We separated them out into three categories (other executive branch agencies in addition to EOTSS, state colleges and universities, and regional transit authorities) for the purposes of this report.

The organization chart below shows the applicability of EOTSS guidance for the agencies in this report.

Applicability of Information Security Risk Management Standard IS.010[1]



EOTSS and Other Executive Branch Agencies

EOTSS is responsible for the development and maintenance of the Enterprise Information Security Policies and Standards, pursuant to Section 2 of Chapter 7D of the General Laws, which requires all executive branch agencies to "adhere to the policies, procedures, and objectives established by the executive office

1. Agencies marked as "not under audit" are not included in this report. Additionally, EOTSS's Information Security Risk Management Standard IS.010 states the following regarding its scope: "Executive Department agencies and offices are required to implement procedures that ensure their personnel comply with the requirements herein to safeguard information."

of technology services and security." EOTSS states in its Information Security Risk Management Standard IS.010 that this standard "applies to the Executive Department including all executive offices, and all boards, commissions, agencies, departments, divisions, councils, and bureaus." This report outlines our audit of the following executive branch agencies regarding cybersecurity awareness training:

- EOTSS itself;
- the Bureau of the State House (BSH);
- the Civil Service Commission (CSC);
- the Department of Labor Standards (DLS);
- the Department of Mental Health (DMH);
- the Department of Public Health (DPH);
- the Department of Revenue (DOR);
- the Group Insurance Commission (GIC);
- the Massachusetts Department of Transportation (MassDOT);
- the Massachusetts Parole Board (MPB);
- the Registry of Motor Vehicles (RMV); and
- the State 911 Department (911).

The table below shows the state appropriations for each of these executive branch agencies.[2] (Note that 911 does not receive state appropriations. Instead, it receives funding through an annual surcharge of $1.50 on all telephone lines capable of accessing the 911 system. These funds are kept by 911 in a trust fund account.)

2. This table shows state appropriations exclusively; however, some agencies receive additional funding from other sources. State appropriations include a variety of different spending categories, including personnel, technology, and pass-through spending. As an example, GIC (line item 1108-5100) received $4,385,239, $4,385,240, and $4,738,587 in state appropriations in fiscal years 2021, 2022, and 2023, respectively. GIC's state appropriations include group insurance premium and plan costs (line item 1108-5200), which accounted for $1,747,367,959, $1,826,778,807, and $1,921,206,747 in state appropriations in fiscal years 2021, 2022, and 2023, respectively. GIC's state appropriations also include the State Retiree Benefits Trust Fund (line item 1599-6152), which accounted for $500,000,000 in state appropriations in fiscal years 2021 and 2022 and $525,000,000 in state appropriations in fiscal year 2023. See the GIC's Historical Budget Summary for more information.

Agency	State Appropriations Fiscal Year 2021	State Appropriations Fiscal Year 2022	State Appropriations Fiscal Year 2023
EOTSS	$3,105,778	$3,105,778	$3,204,513
BSH	$3,677,814	$3,927,814	$4,569,197
CSC	$623,938	$625,406	$843,762
DLS	$3,949,551	$4,349,551	$4,628,025
DMH	$911,642,258	$951,956,760	$1,018,768,861
DPH	$769,034,718	$819,954,348	$938,273,734
DOR	$1,356,399,209	$1,399,872,660	$1,483,244,288
MassDOT	$613,006,824	$635,459,988	$752,237,634
GIC	$2,263,612,328	$2,344,120,760	$2,463,402,384
MPB	$21,908,514	$20,943,687	$21,649,317
RMV	$182,380,000	$131,573,000	$131,653,000

State Colleges and Universities

The state colleges and universities in Massachusetts work to improve higher education, support economic development and growth, and support communities across the Commonwealth. The following state colleges and universities (which were established in accordance with Section 5 of Chapter 15A of the General Laws) are a system of public institutions of higher education, and were subjects of this audit:

- Framingham State University (FSU);
- Holyoke Community College (HCC);
- Massachusetts Bay Community College (MBCC);
- Massasoit Community College (MCC);
- North Shore Community College (NSCC);
- Northern Essex Community College (NECC); and
- Westfield State University (WSU).

The table below shows the state appropriations for each of these state colleges and universities.

Agency	State Appropriations Fiscal Year 2021	State Appropriations Fiscal Year 2022	State Appropriations Fiscal Year 2023
FSU	$32,545,150	$33,193,587	$36,087,625
HCC	$22,697,040	$23,207,079	$23,851,448
MBCC	$17,779,141	$18,136,472	$18,746,043
MCC	$24,064,288	$24,474,243	$25,391,675
NSCC	$24,154,641	$24,600,186	$25,517,333
NECC	$21,986,040	$22,385,471	$23,251,578
WSU	$30,992,952	$31,621,476	$34,336,799

Regional Transit Authorities

Regional transit authorities provide public transportation services in different communities within Massachusetts, meeting the specific transit needs of each community. The following regional transit authorities were established in accordance with Section 2 of Chapter 161B of the General Laws and were subjects of this audit:

- the Cape Ann Transportation Authority (CATA);
- the Cape Cod Regional Transit Authority (CCRTA);
- the Martha's Vineyard Regional Transit Authority (VTA); and
- the Nantucket Regional Transit Authority (NRTA).

The table below shows the operating revenues for each of these regional transit authorities.

Agency	Operating Revenues Fiscal Year 2021	Operating Revenues Fiscal Year 2022	Operating Revenues Fiscal Year 2023
CATA	$13,642,963	$2,604,218	$512,110
CCRTA	$9,083,000	$1,456,000	$1,139,000
VTA	$1,289,000	$1,779,000	$1,798,000
NRTA	$389,492	$578,464	$614,688

Cybersecurity Awareness Training

EOTSS has established policies and procedures that apply to all Commonwealth agencies within the executive branch. These policies and procedures require executive branch agencies to implement procedures that ensure that their employees comply with the requirements in EOTSS's aforementioned

policies and procedures. EOTSS recommends, but does not require, non-executive branch agencies to follow its policies and procedures. Section 6.2 of EOTSS's Information Security Risk Management Standard IS.010 states,

> *The objective of the Commonwealth information security training is to educate users on their responsibility to help protect the confidentiality, availability and integrity of the Commonwealth's information assets. Commonwealth Offices and Agencies must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.*

To ensure that employees in all Commonwealth agencies within the executive branch are clear on their responsibilities, EOTSS's policies and procedures require that all newly hired employees[3] must complete an initial cybersecurity awareness training course within 30 days of their orientation, and that all existing employees[4] complete an annual refresher cybersecurity awareness course.

3. For the purposes of this audit report, we use the term newly hired employees to refer to employees who were hired during the audit period, unless stated otherwise.
4. For the purposes of this audit report, we use the term existing employees to refer to employees who were hired before the start of the audit period (July 1, 2021), unless stated otherwise.

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 cybersecurity awareness training at the Executive Office of Technology Services and Security (EOTSS). Pursuant to our governing statute, Section 12 of Chapter 11 of the General Laws, our audit covers multiple entities' compliance with EOTSS's cybersecurity training standards. Specifically, Section 12 of Chapter 11 states, "Each entity may be audited separately as a part of a larger organizational entity or as a part of an audit covering multiple entities." As such, cybersecurity awareness training testing was completed at 22 other executive branch agencies, state colleges and universities, and regional transit authorities, for the period July 1, 2021 through April 30, 2023.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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

Objective	Conclusion
1. Did EOTSS and other executive branch agencies, state colleges and universities, and regional transit authorities ensure that their employees completed cybersecurity awareness training in accordance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010?	**No; see Findings 1, 2, 3, and 4**

To accomplish our audit objective, we gained an understanding of the aspects of EOTSS's internal control environment relevant to our objective by interviewing EOTSS staff members and management and by reviewing EOTSS's Information Security Risk Management Standard IS.010.

To obtain sufficient, appropriate evidence to address our audit objective, we performed the procedures described below.

Cybersecurity Awareness Training

We separated the 23 agencies we reviewed as part of this audit into three categories based on agency type: EOTSS and other executive branch agencies, state colleges or universities, and regional transit authorities.

- The first category comprises EOTSS and 11 other executive branch agencies: the Bureau of the State House (BSH), the Civil Service Commission (CSC), the Department of Labor Standards (DLS), the Department of Mental Health (DMH), the Department of Public Health (DPH), the Department of Revenue (DOR), the Massachusetts Department of Transportation (MassDOT), the Group Insurance Commission (GIC), the Massachusetts Parole Board (MPB), the Registry of Motor Vehicles (RMV), and the State 911 Department (911).
- The second category comprises seven state colleges and universities: Framingham State University (FSU), Holyoke Community College (HCC), Massachusetts Bay Community College (MBCC), Massasoit Community College (MCC), North Shore Community College (NSCC), Northern Essex Community College (NECC), and Westfield State University (WSU).
- The third category comprises four regional transit authorities: the Cape Ann Transportation Authority (CATA), the Cape Cod Regional Transit Authority (CCRTA), the Martha's Vineyard Regional Transit Authority (VTA), and the Nantucket Regional Transit Authority (NRTA).

To determine whether EOTSS and these other executive branch agencies, state colleges and universities, and regional transit authorities ensured that their employees completed cybersecurity awareness training in accordance with Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010, we took the actions described below.

EOTSS and Other Executive Branch Agencies

To determine whether EOTSS and the 11 other executive branch agencies included in this audit ensured that their newly hired employees completed initial cybersecurity awareness training within 30 days of orientation, we analyzed the evidence for cybersecurity awareness training completion (i.e., transcript reports[5]) by comparing each employee's start date and training completion date for all 2,662 newly hired employees across these executive branch agencies.

To determine whether these executive branch agencies ensured that their existing employees completed annual refresher cybersecurity awareness training, we analyzed the evidence for cybersecurity awareness training completion (i.e., transcript reports) by comparing each employee's

5. We analyzed the cybersecurity awareness training transcript reports from EOTSS and the other executive branch agencies. These reports included fields such as the training due date and the training completion date.

training completion date and training due date for all 12,236 existing employees across these executive branch agencies.

To further substantiate the results of the above procedures, we also selected a random, statistical sample[6] of 24 employee training certificates of completion out of the population of 14,898 newly hired and existing employees, using a 90% confidence level,[7] a 0% expected error rate,[8] and a 10% tolerable error rate.[9] Our sample comprised the following:

- from EOTSS, BSH, CSC, DLS, GIC, MPB, RMV, and 911: 1 employee training certificate of completion from each agency;
- from DOR: 2 employee training certificates of completion;
- from DPH and MassDOT: 4 employee training certificates of completion from each agency; and
- from DMH: 6 employee training certificates of completion.

We selected these sample numbers based on the number of active employees each agency had during the audit period.

We did not note any exceptions in our testing corresponding to BSH and 911. Therefore, we concluded that, during the audit period, BSH and 911 met the relevant criteria regarding this matter.

For the other executive branch agencies included in this audit, we did note exceptions during our testing. See Findings 1 and 2 for issues we identified with the cybersecurity awareness training provided by EOTSS and the other executive branch agencies included in this audit.

6. Auditors use statistical sampling to select items for audit testing when a population is large and contains similar items. Auditors generally use a statistical software program to choose a random sample when sampling is used. The results of testing using statistical sampling, unlike those from judgmental sampling, can usually be used to make conclusions or projections about entire populations.
7. Confidence level is a mathematically based measure of the auditor's assurance that the sample results (statistic) are representative of the population (parameter), expressed as a percentage.
8. Expected error rate is the number of errors that are expected in the population, expressed as a percentage. It is based on the auditor's knowledge of factors such as prior year results, the understanding of controls gained in planning, or a probe sample.
9. The tolerable error rate (which is expressed as a percentage) is the maximum error in the population that is acceptable while still using the sample to conclude that the results from the sample have achieved the objective.

State Colleges and Universities

To determine whether the state colleges and universities included in this audit ensured that their employees completed cybersecurity awareness training, we took the actions described below.

We inspected the cybersecurity awareness training certificates of completion using a judgmental,[10] nonstatistical sample of 70 employee training certificates of completion out of the population of 10,094. Our sample comprised 10 employee training certificates of completion from each of the seven state colleges and universities included in this audit. Of the 10 employee training certificates of completion from each state college or university, we judgmentally selected 3 existing non-student employees, 4 newly hired non-student employees, and 3 existing student employees.

Also, we determined whether the state colleges and universities included in this audit ensured that the newly hired employees from our sample completed initial training within 30 days of orientation by comparing the dates of their orientations to the dates of their certificates of completion.

See Finding 3 for issues we identified with the cybersecurity awareness training provided by the state colleges and universities included in this audit.

Regional Transit Authorities

To determine whether the regional transit authorities included in this audit ensured that their employees completed cybersecurity awareness training, we took the actions described below.

We inspected the cybersecurity awareness training certificates of completion using a judgmental, nonstatistical sample of 23 employee training certificates of completion out of the population of 55. Our sample comprised the following:

- from CATA: 3 employee training certificates of completion (which represents its full population of employees);
- from NRTA: 4 employee training certificates of completion (which represents its full population of employees); and

10. Auditors use judgmental sampling to select items for audit testing when a population is very small, the population items are not similar enough, or there are specific items in the population that the auditors want to review. Auditors use their knowledge and judgment to select the most appropriate sample. For example, an auditor might select items from areas of high risk. The results of testing using judgmental sampling cannot be used to make conclusions or projections about entire populations; however, they can be used to identify specific issues, risks, or weaknesses.

- from CCRTA and VTA: 8 employee training certificates of completion from each agency.

Of the 8 employee training certificates of completion from CCRTA and VTA, we judgmentally selected 2 newly hired employees and 6 existing employees. Additionally, we determined whether these regional transit authorities ensured that the newly hired employees from our sample completed initial training within 30 days of orientation by comparing the dates of their orientations to the dates of their certificates of completion.

We did not note any exceptions in our testing corresponding to NRTA. Therefore, we concluded that, during the audit period, NRTA met the relevant criteria regarding this matter.

For the other regional transit authorities included in this audit, we noted exceptions during our testing. See Finding 4 for issues we identified with the cybersecurity awareness training provided by the regional transit authorities included in this audit.

We used a combination of statistical and nonstatistical sampling methods for testing, and we did not project the results of our testing to any corresponding populations.

Data Reliability Assessment

To determine the reliability of the employee lists from EOTSS and each of the 22 other executive branch agencies, state colleges and universities, and regional transit authorities included in this audit (see the list of auditees included in this report, by category), we took the actions described below.

We interviewed EOTSS management who were knowledgeable about these lists. We reviewed MassAchieve[11] system controls for access control, configuration management, contingency planning, segregation of duties, and security management. We checked that the variable formats of each agency's employee list (e.g., dates, unique identifiers, or abbreviations) were accurate. For each agency's employee list, we ensured that there was no abbreviation of data fields, no missing data (e.g., hidden rows or columns, blank cells, or incomplete records), and no duplicate records and that all values corresponded with expected values.

To determine the completeness and accuracy of each agency's employee list, we took the actions described below.

11. MassAchieve is a training platform used by executive branch agencies to administer cybersecurity awareness training.

EOTSS and Other Executive Branch Agencies

- EOTSS: We selected random samples of 20 employees from EOTSS's employee list and traced their names to CTHRU, the Commonwealth's statewide payroll open records system. We also selected random samples of 20 employees from CTHRU and traced their names back to EOTSS's employee list.

- BSH and CSC: We selected random samples of five employees from each executive branch agency's employee list and traced their names to CTHRU. We also selected random samples of five employees from each agency from CTHRU and traced their names back to each agency's employee list.

- DLS, GIC, MPB, and 911: We selected random samples of 10 employees from each executive branch agency's employee list and traced their names to CTHRU. We also selected random samples of 10 employees from each agency from CTHRU and traced their names back to each agency's employee list.

- DMH, DPH, DOR, MassDOT, and RMV: We selected random samples of 20 employees from each executive branch agency's employee list and traced their names to CTHRU. We also selected random samples of 20 employees from each agency from CTHRU and traced their names back to each agency's employee list.

State Colleges and Universities

- FSU, HCC, MBCC, MCC, NSCC, NECC, and WSU: We selected random samples of 20 employees from each state college's/university's employee list and traced their names to CTHRU. We also selected random samples of 20 employees from each state college/university from CTHRU and traced their names back to each state college/university's employee list.

Regional Transit Authorities

- CATA: We selected the total population of three employees and traced their names to CATA's open payroll webpage. We also selected the total population of three employees from CATA's open payroll webpage and traced their names back to CATA's employee list.

- CCRTA and VTA: We selected random samples of five employees from each regional transit authority's employee list and traced their names to each agency's open payroll webpage. We also selected random samples of five employees from each regional transit authority's open payroll webpage and traced their names back to each agency's employee list.

- NRTA: We selected the total population of four employees and traced their names to NRTA's open payroll webpage. We also selected the total population of four employees from NRTA's open payroll webpage and traced their names back to NRTA's employee list.

Based on the results of the data reliability assessment procedures described above, we determined that the information we obtained for the audit period was sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. EOTSS did not ensure that all of its employees completed cybersecurity awareness training.

The Executive Office of Technology Services and Security (EOTSS) did not ensure that all of its employees who were active during the audit period completed initial and annual refresher cybersecurity awareness training.

The original due date for the training was August 31, 2022, but EOTSS executive management requested and received an extension from the Human Resources Division (HRD), which extended the due date for all executive branch agencies to October 14, 2022. HRD communicated this new deadline to executive branch managers through its *Managers' Corner Newsletter*.

The table below shows our findings for EOTSS. Note that this table reflects the extended October 14, 2022 due date.

Cybersecurity Awareness Training Type	On-Time Training Completion Percentage	Total Number of Employees Tested	Number of Employees Who Completed Training Late	Number of Employees Who Did Not Complete Training
Initial	67.8%	115	28	9
Annual Refresher	99.8%	411	—	1

If EOTSS does not ensure that all of its employees complete cybersecurity awareness training, then EOTSS may expose itself to an increased risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

EOTSS's Information Security Risk Management Standard IS.010 states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course shall be conducted via web-based learning or in class training and shall be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*
>
> *6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.*

Reasons for Issue

EOTSS management explained that contract employees undergo a different onboarding process compared to non-contact employees. EOTSS processes contract employees' training assignments in batches and must create training accounts manually. This process is time-consuming and typically occurs only once or twice per month. Additionally, EOTSS management noted that they do not have access to training transcripts for former employees.

Recommendations

1. EOTSS should strengthen their policy to improve oversight of executive branch state agencies, including their timely completion of cybersecurity awareness trainings.
2. EOTSS should ensure that all employee training transcript for all employees are maintained and include records regarding cybersecurity awareness training completion.
3. EOTSS should ensure that all of its employees complete cybersecurity awareness training within 30 days of orientation and annually thereafter.
4. EOTSS should establish procedures to monitor employee cybersecurity awareness training completion rates throughout the training cycle and use historical data retained by HRD to ensure that employees meet training deadlines.

Auditee's Response

Security awareness training is a critical component of the Commonwealth's security compliance strategy. Mandatory cybersecurity training must be completed within 30 days of employee orientation. The new hire 30-day training completion requirement is tied to employee orientation, rather than date of hire, to accommodate business processes related to onboarding and credentialing into the training system. Further, the process for onboarding and credentialing contract employees is different than the process for non-contract employees. Contractors are assigned training in "batches" once or twice per month. The new hire 30-day training completion requirement is purposefully tied to orientation date, as opposed to new hire date to accommodate for such business processes. [The Office of the State Auditor] relied on hire date, rather than employee orientation/onboarding date to calculate the 30-day deadline.

Moving forward, EOTSS will evaluate its internal processes to identify areas for improvement related to new hire orientation and contractor onboarding.

Additionally, EOTSS will work with necessary partners to explore whether there is a technical solution to accessing transcript data of former agency employees.

Auditor's Reply

We agree with EOTSS's statement that "security awareness training is a critical component of the Commonwealth's security compliance strategy," and for this reason, we believe that all employees, regardless of classification, should complete their initial training within 30 days. The data provided by EOTSS in response to our data requests in this audit did not include new hire orientation dates, it included new hire start dates.

Additionally, while we acknowledge that EOTSS has established policies and procedures applicable to all Commonwealth agencies within the executive branch, based on the findings below respective to those executive branch agencies, we believe there is a need for EOTSS to enhance its oversight of these agencies to ensure greater compliance with the Enterprise Information Security Policies and Standards.[12]

Based on its response, EOTSS has indicated that it will take steps to address our concerns on this matter. We will follow up on this during our post-audit review process in approximately six months.

2. CSC, DLS, DMH, DPH, DOR, MassDOT, GIC, MPB, and RMV did not ensure that all of their employees completed cybersecurity awareness training.

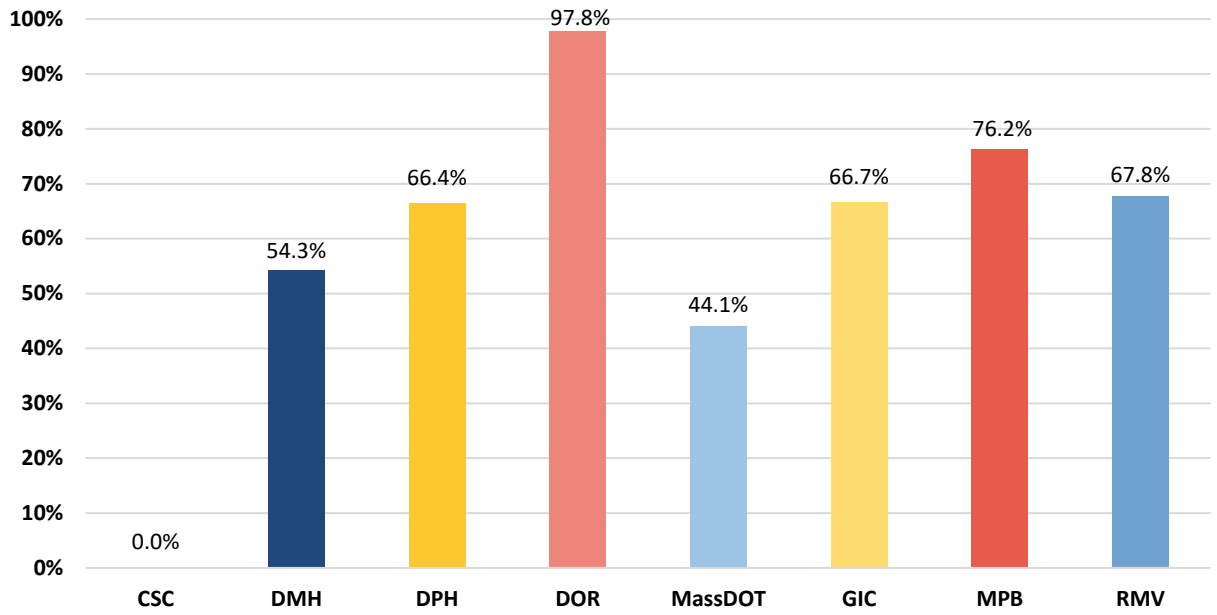
The following executive branch agencies did not ensure that all of their employees completed cybersecurity awareness training during the audit period: the Civil Service Commission (CSC), the Department of Labor Standards (DLS), the Department of Mental Health (DMH), the Department of Public Health (DPH), the Department of Revenue (DOR), the Massachusetts Department of Transportation (MassDOT), the Group Insurance Commission (GIC), the Massachusetts Parole Board (MPB), and the Registry of Motor Vehicles (RMV).

Regarding the completion rates for the initial cybersecurity awareness training, we observed that 445 newly hired employees completed training late, while 601 did not complete training at all. Regarding the completion rates for the annual refresher cybersecurity awareness training, we observed that 156 existing employees completed training late, while 951 did not complete training at all.

12. The Enterprise Information Security Policies and Standards is the compilation of policies and standards that all executive branch agencies are required to follow. Information Security Risk Management Standard IS.010 is just one of these policies.

The table and graph below show our findings for these agencies regarding initial cybersecurity awareness training.

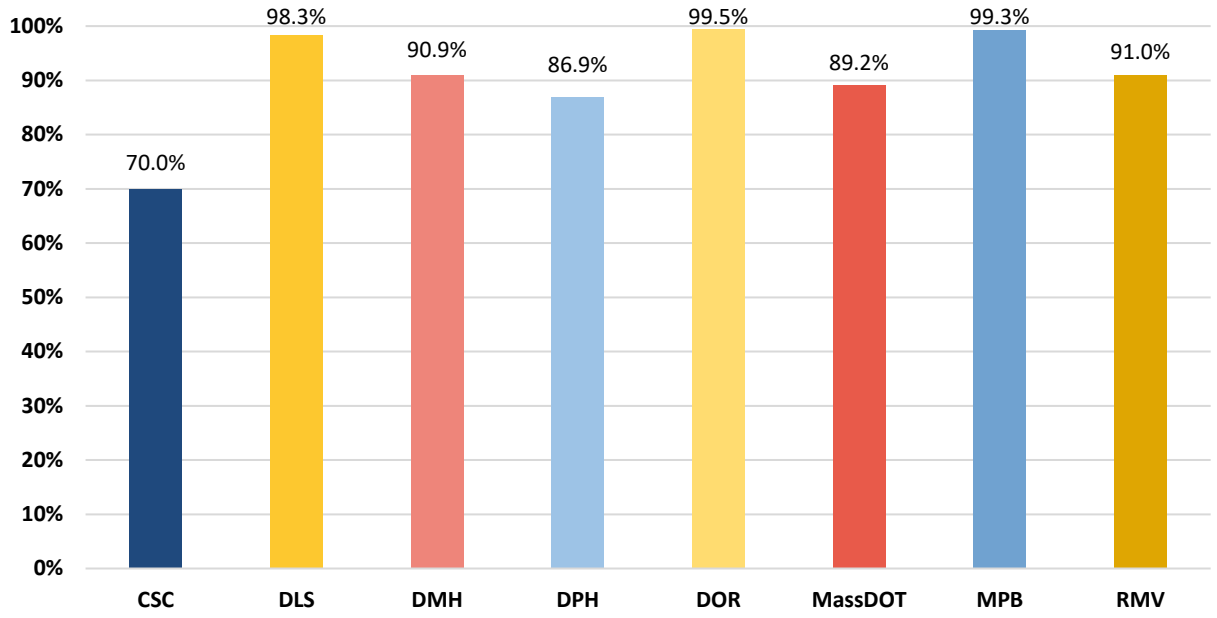
On-Time Cybersecurity Awareness Training Completion Rates for Executive Branch Agencies: Newly Hired Employees



Agency	On-Time Initial Training Completion Percentage	Total Number of Employees Tested	Number of Tested Employees Who Completed Training Late	Number of Tested Employees Who Did Not Complete Training
CSC	00.0%	1	—	1
DMH	54.3%	905	148	266
DPH	66.4%	524	83	93
DOR	97.8%	229	—	5
MassDOT	44.1%	742	185	230
GIC	66.7%	3	1	—
MPB	76.2%	21	5	—
RMV	67.8%	90	23	6

The table and graph below show our findings for these agencies regarding annual refresher cybersecurity awareness training.

On-Time Cybersecurity Awareness Training Completion Rates for Executive Branch Agencies: Existing Employees



Agency	On-Time Annual Refresher Training Completion Percentage	Total Number of Employees Tested	Number of Tested Employees Who Completed Training Late	Number of Tested Employees Who Did Not Complete Training
CSC	70.0%	10	—	3
DLS	98.3%	58	1	—
DMH	90.9%	3246	30	265
DPH	86.9%	2911	26	355
DOR	99.5%	1356	—	7
MassDOT	89.2%	3455	91	284
MPB	99.3%	151	—	1
RMV	91.0%	488	8	36

If executive branch agencies do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

EOTSS's Information Security Risk Management Standard IS.010 states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course shall be conducted via web-based learning or in class training and shall be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*
>
> *6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.*

Reasons for Issue

Management from each of the following executive branch agencies provided us with the following reasons for noncompliance:

- CSC management stated that contracted attorneys and interns were not on the list of employees required to complete the cybersecurity awareness training.
- DLS management stated that they are not sure what the reason was for the late training completion of the employee from our finding, other than the employee overlooked the training due date. DLS management noted that this employee is no longer with DLS.
- DMH management sent us an email on February 16, 2024 regarding the employees from our finding, stating that these are "Employees who do not have [computer] Network Access—these staff are exempt."
- DPH management stated that the staff members from our finding started their cybersecurity awareness training but did not complete the full training.
- DOR management stated that some of the employees from our finding had job duties that did not require them to have computer network access, while others separated from DOR shortly after their training due date had passed, leaving no time for DOR to enforce training completion.
- MassDOT management and RMV management stated that employees missed the training deadline and that interns did not receive cybersecurity awareness training because MassAchieve did not assign them training.
- GIC management stated that the employee from our finding left the agency shortly after starting and did not complete the training before their departure.
- MPB management stated that newly hired employees have assigned joint orientation/training days which may have been scheduled past the 30 days from hire dates for some staff. Regarding

refresher training, it appears that one employee found not to have completed the training, completed only 2 out of the 5 required sections of the cybersecurity training.

Recommendations

The aforementioned nine executive branch agencies should do the following:

1. provide cybersecurity awareness training (both an initial training within 30 days of orientation and an annual refresher training thereafter) to all full-time employees, contractors, and interns;
2. establish procedures to monitor employee cybersecurity awareness training completion rates throughout the training cycle and use historical data retained by HRD to ensure employees meet training deadlines; and
3. implement additional controls to ensure that the new hire onboarding process includes all required coursework regarding cybersecurity awareness training.

We appreciate the following responses provided by the executive branch agencies:

Auditee's Response: CSC

CSC appreciates receiving clarification from the Office of the State Auditor that seasonal interns and contract employees are required to complete the cybersecurity awareness training. In response, CSC had the seasonal interns and contract employee at the time immediately complete the required cybersecurity training. Going forward, any CSC interns and contract employees will be required to complete the same initial and refresher cybersecurity training as all regular CSC employees, ensuring 100% compliance with this requirement.

Auditor's Reply: CSC

Based on its response, CSC has taken measures to address our concerns regarding this matter.

Auditee's Response: DLS

[DLS] management agrees with the finding. As [the Office of the State Auditor] has affirmed, we now have a program to ensure employees are trained in a timely manner. This is demonstrated by the 100% completion for new hires and near completion for existing employees. Of the two existing employees whose training was not completed by the deadline, one staff was one (1) day late due to her supervisor leaving and the new supervisor not receiving the alerts, while the other staff is no longer an [Executive Office of Labor and Workforce Development] employee. Regardless, we will continue to reinforce timely completion by sending email reminders.

Auditor's Reply: DLS

Based on its response, DLS will take measures to address our concerns regarding this matter.

Auditee's Response: DMH

As DMH indicated to the [Office of the State Auditor] during the audit, 417 of the newly hired individuals are contract employees who do not have any network access. Consequently, they do not need cybersecurity training. In fact, providing this training would unnecessarily expend resources and increase security risk, as DMH would need to create network access solely to provide the training.

DMH recognizes that the [Office of the State Auditor] assesses compliance with the policy or standard as written, and that it reads Section 6.2 of EOTSS's Information Security Risk Management Standards as requiring cybersecurity training for "all personnel." Indeed, Section 6.2 states that "all personnel" must be trained. The immediately preceding sentence, however, states that the objective of the cybersecurity training is to educate "users" on their cybersecurity responsibilities. Respectfully, DMH views the word "personnel" in the second sentence as referring to the "users" referred to in the first sentence. Thus, per DMH's reading, only "users" must be trained. . . .

The data used for this finding had some limitations, as indicated during the audit. Some employees were hired after the end date that the 2021 annual cybersecurity training was due; some left state service and then returned after the due date for the 2021 cybersecurity training; and, on account of system limitations, DMH was unable to determine dates that some staff left DMH. DMH understands that data of the sort required and assessed here typically has limitations, and that the Auditor's Office needs to utilize data as provided, but the number here likely is not accurate.

Auditor's Reply: DMH

Section 2 of Chapter 7D of the Massachusetts General Laws mandates that all executive branch state agencies, including DMH, "adhere to the policies, procedures and objectives established by the executive office of technology services and security." DMH must ensure that contractors are trained in compliance with EOTSS's Information Security Risk Management Standard IS.010.

Regarding the definition of "personnel," we maintain that EOTSS's Information Security Risk Management Standard IS.010 states, "All new personnel must complete an Initial Security Awareness Training course," and that EOTSS does not provide an exemption to this policy for employees who lack access to computers.

We urge DMH to implement an alternative method for employees without system access to complete their training, such as offering a paper-based training option. We recognize that some agencies may disagree with EOTSS standards, but nonetheless, these standards exist. Cybersecurity awareness policies are not just guidelines; they are essential safeguards in today's digital landscape. Comprehensive employee training and shared responsibility are critical to mitigating potential cyber threats. It is important to consistently assess and reinforce cybersecurity measures to ensure that policies are effective, compliance is maintained, and public trust in the agency's ability to safely manage data is

upheld. These policies exist to protect both individuals and organization, fostering a secure and safe digital environment.

Regarding the data's limitations, we conducted a data reliability assessment on the information DMH provided to us, ensuring the completeness and accuracy of DMH's employee list. As we have recommended, we believe that DMH should establish procedures to (1) monitor employee cybersecurity awareness training completion rates throughout the training cycle, (2) accurately track the dates when employees leave the agency, and (3) use historical data retained by HRD to ensure that employees meet training deadlines.

Auditee's Response: DPH

1. *Provide cybersecurity awareness training (both an initial training within 30 days of orientation and an annual refresher training thereafter) to all full-time employees, contractors, and interns.*
    a. *The training is offered through MassAchieve within 30 days of start and annually.*
    b. *DPH has increased staffing in this area and developed and implemented a robust system of reminders for all staff who are incompliant starting in December of each year.*
    c. *We promote completion of this training by alerting staff to the consequence of shut-off by EOTSS.*
    d. *This past fiscal year we achieved near perfect completion with less than 10 shut offs.*
2. *Establish procedures to monitor employee completion throughout the training cycle to ensure that staff are meeting the training deadlines.*
    a. *Our staff run reports monthly and have empowered each bureau, office and hospital to run their own custom-built reports.*
    b. *We established standard communications to go out to supervisors and incompliant staff.*

We appreciate the insights provided by the audit and are addressing these findings promptly.

Auditor's Reply: DPH

Based on its response, DPH has taken measures to address our concerns regarding this matter.

Auditee's Response: DOR

DOR agrees with the results of the audit. The employees who did not complete the training during the audit period were employees with no access to computers or were separated from DOR shortly after hire.

DOR will continue to utilize MassAchieve to track employee completion throughout the training cycle.

In [fiscal year 2024], DOR implemented the process of "paper training," where Employees with no access to computers and/or systems will take the training in person, in a class organized by their managers, and sign an acknowledgement that they have received, taken and understand the training. Information will be uploaded to MassAchieve.

DOR will incorporate cybersecurity awareness training into the new hire process, where the course is added to DOR's Learning Management System (LMS—DOR's internal training system). LMS system also will be used to track completion and follow up with new hires that have not completed the training. Information will be uploaded to MassAchieve.

Auditor's Reply: DOR

Based on its response, DOR has taken, and will continue to take, measures to address our concerns regarding this matter.

Auditee's Response: MassDOT and RMV

As of 2024, MassDOT has transitioned to using only the MassAchieve LMS, eliminating confusion for employees regarding where to find and complete assigned training. Furthermore, statewide improvements, such as increased frequency of reminders from HRD, have helped improve performance. Additionally, EOTSS has followed through on removing access to those who do not complete cybersecurity training on time. MassDOT has used this consequence to effect in our messaging to further incentivize timely completion of cybersecurity training and has collaborated with EOTSS as needed to reinstate access for individuals who had their access removed due to non-compliance. . . .

In the 2023–24 training cycle MassDOT implemented procedures to continue to support the agency's efforts in meeting its compliance obligation. This includes earlier distribution of targeted activity reports, making it easier for managers to identify those yet to complete training. Reports are shared on an increasing cadence as the training deadline approaches.

Auditor's Reply: MassDOT and RMV

Based on their response, MassDOT and RMV have taken measures to address our concerns regarding this matter.

Auditee Response: GIC

GIC was given the opportunity to respond to a draft version of this audit report and did not provide a written response.

Auditee's Response: MPB

MPB concurs with [the Office of the State Auditor's] recommendations to (1) provide cybersecurity awareness training (both an initial training within 30 days of orientation and an annual refresher training thereafter) to all full-time employees, contractors, and interns; and (2) establish procedures to monitor employee completion throughout the training cycle to ensure that staff are meeting the training deadlines.

To improve timely completion of cybersecurity training for new hires, MPB will modify its existing "Checklist for Employee Orientation" form to specify due dates for completion of cybersecurity training and include an acknowledgement receipt upon completion.

Bi-weekly Managers' Meetings will be utilized to further monitor adherence to the training deadlines.

Auditor's Reply: MPB

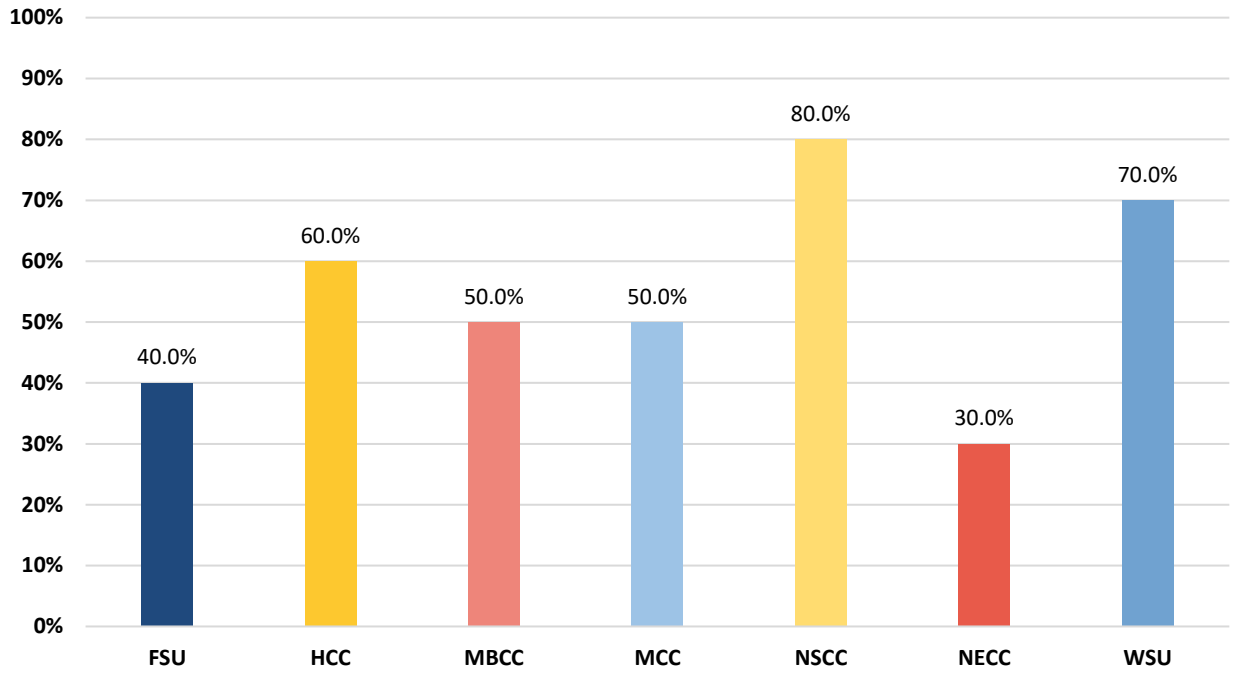
Based on its response, MPB will take measures to address our concerns regarding this matter.

3. Seven state colleges and universities did not ensure that all of their employees completed cybersecurity awareness training.

The following state colleges and universities did not ensure that all of their employees completed cybersecurity awareness training during the audit period: Framingham State University (FSU), Holyoke Community College (HCC), Massachusetts Bay Community College (MBCC), Massasoit Community College (MCC), North Shore Community College (NSCC), Northern Essex Community College (NECC), and Westfield State University (WSU).

The table and graph below show our findings for these state colleges and universities.

On-Time Cybersecurity Awareness Training Completion Rates for State Colleges and Universities: Sample of All Employees



State College or University	On-Time Training Completion Percentage*	Total Number of Employees Tested	Number of Tested Employees Who Completed Training Late	Number of Tested Employees Who Did Not Complete Training
FSU	40.0%	10	—	6
HCC	60.0%	10	—	4
MBCC	50.0%	10	—	5
MCC	50.0%	10	—	5
NSCC	80.0%	10	—	2
NECC	30.0%	10	—	7
WSU	70.0%	10	—	3

* Note that this table is based on the sample of employees from each state college or university, not the population of employees.

If state colleges and universities do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

EOTSS's Information Security Risk Management Standard IS.010 states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course shall be conducted via web-based learning or in class training and shall be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*
>
> *6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.*

Reasons for Issue

Management from each of the following state colleges and universities provided us with the following reasons for noncompliance:

- FSU management stated that its internal policy only recommended cybersecurity awareness training for its employees, instead of requiring it.
- HCC management stated that student employees did not have access to HCC's computer network (which is only accessible with staff member accounts), so therefore, providing them with cybersecurity awareness training would not be required.
- MBCC management stated the following:
  - Two student employees from our finding "never received student [employee] accounts, so they were missed in getting training assigned as part of the onboarding" (from an email MBCC sent to us on February 15, 2024);
  - Two employees from our finding "did not elect to complete their training. . . . As a result, their employment with [MBCC] was discontinued" (from an email MBCC sent to us on February 15, 2024);
  - One newly hired employee from our finding "started before the training program was in place, so [they] would not have had the option for [initial] training" (from an email MBCC sent to us on February 15, 2024); and
  - One newly hired employee from our finding joined MBCC while the college was conducting annual refresher cybersecurity awareness training, so MBCC enrolled this employee in the annual refresher training rather than being trained on the same content twice in a short period of time by first being enrolled in the initial cybersecurity awareness training.
- MCC management stated that its internal policy only recommended cybersecurity awareness training for its employees, instead of requiring it.

- NSCC management stated that two newly hired employees did not complete the cybersecurity awareness training because its auto-enrollment process failed briefly in September 2022, leading to NSCC's inability to enroll newly hired employees into the training during this period.

- NECC management stated that it has a written cybersecurity awareness training policy, but that the policy is not enforced. Management also stated that they are not allowed to limit user access for employees who do not complete cybersecurity awareness training.

- WSU management stated that they were not aware that contractors, part-time employees, or seasonal employees were required to complete the cybersecurity awareness training.

Recommendations

1. The aforementioned seven state colleges and universities should update their cybersecurity awareness training policies to require this training for all employees.

2. The aforementioned seven state colleges and universities should update their cybersecurity awareness training policies to include consequences for non-completion (e.g., restriction of access until they complete the training).

Auditees' Responses

FSU

We are in agreement with the merits of the [EOTSS] Standard and the University is now aligned with the goals of the cybersecurity awareness training. To that end, since the completion of the field work associated with this audit, but prior to the receipt of this draft report, FSU developed and formally adopted campus policy consistent with the Information Security Risk Management Standard. Appendix A contains the text of this Policy on Cybersecurity Training for Employees established on July 17, 2024. The policy is currently in effect and will begin full implementation in October 2024 pursuant to the establishment of a bargained labor agreement that permits initial onboarding cybersecurity training and then subsequent annual training, including prescriptive penalties or remediations for noncompliance.

This local policy will achieve the same goals and mitigate the risks identified in the recommendations associated with Finding 3. We remain committed to the protection of the information technology assets and information retained by the University and share the mutual desire to remain vigilant to new and emerging threats to these digital assets and networks.

HCC

*Upon learning that **all** HCC work study students, regardless of their need to access the network, must complete the cybersecurity training within 30 days of their assignment, HCC implemented the following policies and procedures:*

***Policy**: HCC's policy now mandates that all work study students will be notified they need to complete mandatory cybersecurity training within 30 days of starting their work assignment.*

***Consequences**: Failure to complete the required training within 30 days of their work assignment will result in revoking their work study assignment/job until the training is completed.*

MBCC

[MBCC writes] in response to your email of July 19, 2024, regarding the recent audit of cybersecurity training at [MBCC]. Thank you for sharing the audit results and providing us with the opportunity to respond.

The two student employees mentioned did not receive student employee accounts and thus were not assigned training during onboarding. As part of our employee onboarding process, all MBCC employees receive an account and are enrolled in the new hire cybersecurity training program. This issue was identified in November 2023 due to this audit, and since then, MBCC has taken steps to ensure the enforcement of this process.

Two employees chose not to complete their training, leading to the termination of their employment with MBCC, underscoring the institution's commitment to mandatory training.

One employee joined before the training program was established. The program is now fully operational, requiring all employees to complete it within 30 days of starting. If not, they are granted an additional 30 days then this [is] escalated to senior management and their access is restricted until it is completed.

Lastly, one newly hired employee started with MBCC during the annual cybersecurity awareness training. As the on boarding training is identical, they were not enrolled twice. Going forward we will ensure that they are enrolled in both.

Thank you again for the audit. Our policy states that all employees must complete the cybersecurity training, but this audit helped us identify areas for improvement. We have taken the necessary steps to remediate areas of concern. Going forward we anticipate we will be in full compliance with the State requirements.

MCC

The college fully acknowledges the need for, and importance of, cybersecurity training for all employees.

Massasoit Community College's leadership is currently developing language to amend the existing Written Information Security Program (WISP) with the recommendations of the recent Executive Office of Technology Services and Security performance audit.

The college will be collaborating with the Unions, through impact bargaining, to ensure proper checks and balances are in place, that new hire training and annual re-training are

conducted in a timely manner, and that, if necessary, reasonable gradated consequences for non-compliance are in place.

NSCC

The College agrees that cybersecurity training is critical and important. The College management and especially the [information technology] department has put a great deal of effort into a collaborative process ensuring that cybersecurity training is ongoing and annual, as demonstrated in our highest completion rate (80%) of those tested in the [Office of the State Auditor] draft report. Since that audit the College has gone further with tighter process improvements which now disables employee accounts that have not completed either the new employee training or annual training within the allotted time frames. Disabled accounts are reenabled upon request and employees are granted an additional week to complete the required training. Our training completion rate now stands at 97%.

NECC

At NECC we specifically value and understand the importance of Cybersecurity training. Recently we experienced a cyber incident caused by user error. Had it not been for the systems we have in place; this threat would have had significant impact on our operation. We also worked with EOTSS after the incident to discuss lessons learned from the attack, working with vendors and the Commonwealth.

In order to better comply with EOTSS's Information Security Risk Management Standard IS.010, and industry's best practices, we have developed a revised Cybersecurity Training Process. . . . NECC is implementing the process starting in the Fall. This process may be subject to impact bargaining with our [Massachusetts Community College Council] and [American Federation of State, County and Municipal Employees] union members.

Thank you again for the opportunity to respond to this audit and please do not hesitate to contact me should you have any additional questions.

WSU

Westfield State's current Security Education Training and Awareness (SETA Program) already requires training as part of the campus onboarding program. . . . For the faculty collective bargaining unit, [Massachusetts State College Association], training was impact bargained and the final agreement was completed on March 21, 2024. As a result, beginning in the fall 2024, cyber security training will be required for faculty. . . .

The University's Access Control Guidelines already allows for the suspension of access to information technology resources for non-compliance. Efforts are currently underway to formalize the consequences with Office of Information and Instructional Technology and the Human Resources Office. Progressive discipline actions may require further impact bargaining.

Auditor's Reply

We appreciate the responses provided by the seven state colleges and universities we audited. The issue we identified is that these state colleges and universities did not consistently provide cybersecurity training to their employees. We regard EOTSS's Information Security Risk Management Standard IS.010 as the baseline for best practices in cybersecurity awareness training across the Commonwealth's agencies, and therefore, we used this as our audit criteria. According to Section 8.18 of the US Government Accountability Office's Generally Accepted Government Auditing Standards, "Examples of criteria include: . . . (c) technically developed standards or norms; . . . (f) defined business practices; . . . and (h) benchmarks against which performance is compared, including performance of other entities or sectors."

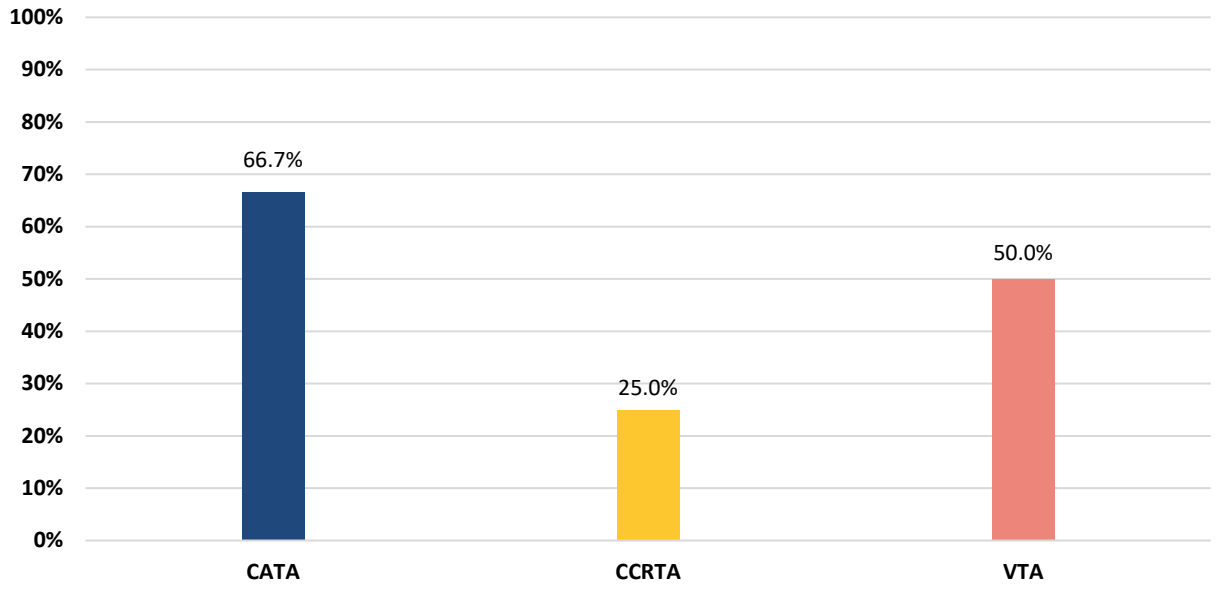
As noted above within the auditees' responses, many colleges and universities have already started addressing our concerns in this area.

4. CATA, CCRTA, and VTA did not ensure that all of their employees completed cybersecurity awareness training.

The following regional transit authorities did not ensure that all of their employees completed cybersecurity awareness training during the audit period: the Cape Ann Transportation Authority (CATA), the Cape Cod Regional Transit Authority (CCRTA), and the Martha's Vineyard Regional Transit Authority (VTA).

The table and graph below show our findings for these regional transit authorities.

On-Time Cybersecurity Awareness Training Completion Rates for Regional Transit Authorities: Sample of All Employees



Regional Transit Authority	On-Time Training Completion Percentage*	Total Number of Employees Tested	Number of Tested Employees Who Completed Training Late	Number of Tested Employees Who Did Not Complete Training
CATA	66.7%	3	—	1
CCRTA	25.0%	8	—	6
VTA	50.0%	8	—	4

* Note that this table is based on the sample of employees from each regional transit authority, not the population of employees.

If regional transit authorities do not ensure that all of their employees complete cybersecurity awareness training, then they may expose themselves to an increased risk of cybersecurity attacks and financial and/or reputational losses.

Authoritative Guidance

EOTSS's Information Security Risk Management Standard IS.010 states,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. This course shall be conducted via web-based learning or in class training and shall be included in the new hire orientation checklist. The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*

6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training. Once implemented, automatic email reminders will be sent to personnel 12 months after course completion, alerting personnel to annual refresher training completion deadlines.

Reasons for Issue

Management from each of the following regional transit authorities provided us with the following reasons for noncompliance:

- CATA management stated that the employee from our finding overlooked the email reminders for the cybersecurity awareness training and did not know they could complete training after the due date.
- CCRTA management stated that not all employees participated in the cybersecurity awareness training, as it was given only to staff members with access to sensitive customer or agency data.
- VTA management stated that some employees did not have computer network access, and therefore, VTA did not require them to take cybersecurity awareness training.

Recommendations

The aforementioned three regional transit authorities should do the following:

1. update their cybersecurity awareness training policies to require this training for all employees and
2. update their cybersecurity training policies to include consequences for non-completion (e.g., restriction of access until training is completed).

Auditees' Responses

CATA

The Cape Ann Transportation Authority agrees with the recommendations.

CCRTA

*The [Office of the State Auditor] audit findings are based on a limited compliance review conducted in accordance with the EOTSS IS.010 cybersecurity policy, which the CCRTA did not opt to adopt as permitted under the policy (**AUTHORITY Section 2, 2.1**: "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.").*

VTA

VTA stated that 4 of the 8 employees selected did not have computer network access as part of their job duties.

Auditor's Reply

We appreciate the responses provided by the regional transit authorities we audited. The issue we identified is that these regional transit authorities did not consistently provide cybersecurity training to their employees. We regard EOTSS's Information Security Risk Management Standard (IS.010) as the baseline for best practices in cybersecurity awareness training across the Commonwealth's agencies, and therefore we used this as our audit criteria. Per Generally Accepted Government Auditing Standards 8.18, examples of criteria include: (C) technically developed standards or norms, (f) defined business practices, and (h) benchmarks for performance comparison, including those of other entities or sectors.

We also note here that EOTSS's Information Security Risk Management Standard IS.010 is applicable to the use of information systems and resources by all Commonwealth agencies within the executive branch, encompassing, as it states, "all executive offices, and all boards, commissions, agencies, [and] departments." This EOTSS standard is designed to safeguard information and serves as a minimum requirement for cybersecurity awareness training.

Regarding training employees who do not have computer network access, we maintain that EOTSS's Information Security Risk Management Standard IS.010 states, "All new personnel must complete an Initial Security Awareness Training course" and that EOTSS does not provide an exemption to this policy for employees who lack access to computer systems. We urge the regional transit authorities to implement an alternative method to complete training for employees without system access, such as offering a paper-based training option.

As noted above within the auditees' responses, many RTAs have already started addressing our concerns in this area.

Westfield STATE UNIVERSITY

OFFICE OF INFORMATION AND INSTRUCTIONAL TECHNOLOGY

To: Audit Committee, Board of Trustees

From: Alan R. Blair,
Chief Information Officer
Chief Information Security Officer

Office of Information and Instructional Technology

Date: November 4, 2023

RE: PCI Assessment Overview

Over the past several years, the Office of Information and Instructional Technology (OIT) has been working diligently to remain Payment Card Industry Data Security Standard (PCI-DSS) compliant. The most significant challenge in this endeavor is the ever changing and evolving requirements of the PCI Security Standards Council.

In 2015, we found ourselves in a position where the new standards were published but not effective until 2016. ITS requested to be held to the 2016 standard during our assessment. This led to 38 sub requirement failures and 5 major requirement failures. After the final report was published, ITS put in place an action plan to mitigate the risks associated with the failures. Because of that action plan, we were able to reduce the sub requirement failures to 3 and major requirement failures to 2 during the 2016 assessment. Prioritization of other projects, funding and time constraints were the major contributing factors to ITS not being able to mitigate the remaining failures. Again, in 2016, we put an action plan in place to mitigate the remaining risks. As a result of the remainder of the that action plan and gaining a head start on the new requirements published by the PCI Security Standards Council in 2016, we were able to mitigate all risks and pass all requirements for the first time in 2017 and successfully adhere to that standard again in 2018 -2023. The new PCI-DSS standards were released in Q1 2023 and take full effect in 2025. OIT requested to be assessed in alignment with the new standards. We are pleased to report that we are 100% compliant with those new standards. Additionally, because of our efforts to provide a more secure and scalable billing system, we have been able to eliminate all of the risks associated with our older billing system.

The challenges we face in the next year are an ever-increasing threat landscape, the lack of human resources on our information security team and the new PCI-DSS standards that we will need to review and adapt our process and procedures to so that we can remain compliant. As we have matured greatly in our PCI-DSS posture we will be focusing our efforts on updating our Cyber Security program to meet the standards of the CIS Critical Controls, version 8. We have begun this process by mapping our policies and conducting both internal and external reviews of our current environment.

PCI Requirement		2015 Result	2016 Result	2017 - 2024 Result
1	Install and Maintain a Firewall Configuration	PASS	PASS	PASS
2	Do Not Use Vendor Supplied Defaults for System passwords and other Security Parameters	PASS	PASS	PASS
3	Protect Stored Data (Electronic)	PASS	PASS	PASS
4	Encrypt Transmission of Cardholder and Sensitive Information across Public Networks	PASS	PASS	PASS
5	Use and Regularly Update Anti-Virus Software	PASS	PASS	PASS
6	Develop and Maintain Secure Systems and Applications	PASS	PASS	PASS
7	Restrict Access to Data by Business Need-To-Know	PASS	PASS	PASS
8	Assign Unique ID to Each Person with Computer Access	FAIL	PASS	PASS
9	Restrict Physical Access to Cardholder Data	FAIL	PASS	PASS
10	Track and Monitor All Access to Network Resources and Cardholder Data	FAIL	PASS	PASS
11	Regularly Test Security Systems and Processes	FAIL	FAIL	PASS
12	Maintain a Policy that Addresses Information Security for Employees and Contractors	FAIL	FAIL	PASS