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

Official Audit Report – Issued November 24, 2020

Executive Office of Housing and Economic Development—Review of Cybersecurity Awareness Training

For the period May 14, 2018 through June 30, 2019

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

November 24, 2020

Mr. Michael Kennealy, Secretary
Executive Office of Housing and Economic Development
1 Ashburton Place, Room 2101
Boston, MA 02108

Dear Secretary Kennealy:

I am pleased to provide this performance audit of the Executive Office of Housing and Economic Development. This report details the audit objective, scope, methodology, finding, and recommendations for the audit period, May 14, 2018 through June 30, 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 Executive Office of Housing and Economic Development for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Curtis Woods, Secretary of the Executive Office of Technology Services and Security

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

EOHED	Executive Office of Housing and Economic Development
EOTSS	Executive Office of Technology Services and Security
HR/CMS	Human Resources Compensation Management System
HRD	Human Resources Division
IT	information technology
MMP	Massachusetts Marketing Partnership
NIST	National Institute of Standards and Technology
PACE	Performance and Career Enhancement

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted an audit of the Executive Office of Housing and Economic Development (EOHED) covering the period May 14, 2018 through June 30, 2019. The purpose of this audit was to determine whether, during our audit period, EOHED ensured that all its information system users[1] in the Human Resources Compensation Management System (HR/CMS) managed by the state Human Resources Division completed the required cybersecurity awareness training.

Below is a summary of our finding and recommendation, with links to each page listed.

Finding 1 **Page 6**	EOHED did not ensure that all information system users in HR/CMS completed the required cybersecurity awareness training.
Recommendation **Page 7**	EOHED should establish effective monitoring controls over its cybersecurity awareness training to ensure that all its information system users complete it in accordance with the standards of the Executive Office of Technology Services and Security and that EOHED maintains documentation of the completion of this training.

1. These users include full-time, part-time, and temporary employees, interns, and contractors with access to EOHED information systems.

OVERVIEW OF AUDITED ENTITY

The Executive Office of Housing and Economic Development (EOHED) was established by Section 16G of Chapter 6A of the Massachusetts General Laws. At the time of our audit, EOHED consisted of 10 agencies.

According to its website,

> *[EOHED] prioritizes economic opportunity for residents, collaborative leadership in communities, and an environment that supports job creation and business growth. EOHED also supports new housing for residents through targeted investments.*

The website also states that EOHED has several programs and grants that offer "information and funding for everything from infrastructure to creative work spaces." During fiscal years 2018 and 2019, EOHED received appropriations of $524 million and $570 million, respectively.

EOHED uses the state's Performance and Career Enhancement (PACE) Learning Management System to administer training and the state's Human Resources Compensation Management System (HR/CMS) to administer payroll and other human resources functions. PACE and HR/CMS are managed by the Commonwealth's Human Resources Division.

EOHED initiated its cybersecurity awareness training on May 14, 2018 and required all of its information system users to complete their initial training by June 15, 2018, and complete training annually thereafter. It also required all new employees to complete cybersecurity awareness training within 30 days of being hired and annually thereafter.

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 the Executive Office of Housing and Economic Development (EOHED) for the period May 14, 2018 through June 30, 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 our audit objective, indicating the question we intended our audit to answer, the conclusion we reached regarding the objective, and where the objective is discussed in the audit findings.

In addition to our finding, we identified an issue we believe warrants EOHED's attention, which we have disclosed in the "Other Matters" section of this report.

Objective	Conclusion
1. Did EOHED ensure that all its information system users in the Human Resources Compensation Management System (HR/CMS) completed required cybersecurity awareness training that was in accordance with Section AT-2 of Revision 4 of the National Institute of Standards and Technology (NIST) Special Publication 800-53; Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security (EOTSS) Information Security Standard IS.010, "Information Security Risk Management Standard"; and Section E04-09, "Intern and Volunteer Records," of the Massachusetts Statewide Records Retention Schedule 06-18?	**No; see Finding 1**

We conducted this performance audit using policies, procedures, and standards issued by EOHED, enterprise security policies and standards issued by EOTSS, and the Massachusetts Statewide Records Retention Schedule 06-18 as criteria. A preliminary version of the EOTSS enterprise security policies and standards was available to agencies in October 2017, and agencies were required to comply with a finalized version on October 15, 2018. Although compliance with these policies was not required for the whole audit period, they were available for agencies to view on EOTSS's website and represented best practices that state agencies such as EOHED should have followed.

We also used Revision 4 of NIST's Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Although EOHED is not required to follow this industry standard, it represents best practices for information system security.

To achieve our audit objective, we first gained an understanding of the internal controls related to the objective by conducting interviews with EOHED management and other staff members involved in administering the agency's cybersecurity awareness training, as well as performing observations of certain management activities related to this training.

Scope Limitation

During the performance of our data reliability assessment, EOHED could not provide evidence of cybersecurity awareness training documentation for all the non–HR/CMS users within its Massachusetts Marketing Partnership agency (MMP). Because MMP did not maintain this training documentation, we modified our audit objective to limit the scope to HR/CMS users.

Next, to assess whether the EOHED information system users on a list obtained from HR/CMS had completed the required cybersecurity awareness training, we performed the following procedures:

- We obtained EOHED's cybersecurity awareness training records through the Performance and Career Enhancement (PACE) Learning Management System and compared this information to a list of users provided by EOHED to determine which information system users completed the training.
- We reviewed PACE training records to determine whether the records for all users were retained.
- We conducted follow-up meetings with EOHED management to discuss the users who did not complete this training according to PACE.

To assess the reliability of the list of HR/CMS users provided by EOHED, we tested for missing data, duplicate data, and data outside the audit period. We also interviewed the EOHED human resources officer who was involved in maintaining the user list. Based on the results of these data reliability assessment procedures, we determined that the data obtained from HR/CMS for audit testing were sufficiently reliable for the purpose of the audit.

To assess the reliability of EOHED's cybersecurity awareness training records in PACE, we tested for missing data, duplicate data, and data outside the audit period. We also interviewed EOHED's human

resources training director and the PACE administrator and observed the PACE administrator exporting the training records from PACE. Based on the results of these data reliability assessment procedures, we determined that the data obtained from PACE for our audit were sufficiently reliable for the purpose of the audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Executive Office of Housing and Economic Development did not ensure that all its information system users in the Human Resources Compensation Management System completed the required cybersecurity awareness training.

Of the 1,101 information system users listed in the Human Resources Compensation Management System as employed by agencies within the Executive Office of Housing and Economic Development (EOHED) during our audit period, at least 45[2] did not complete the required cybersecurity awareness training. The 45 included new hires and existing users. Additionally, three interns who worked for EOHED's Massachusetts Marketing Partnership agency (MMP) were information system users during the audit period but may not have completed this training; MMP did not maintain cybersecurity awareness training documentation for these interns. By not ensuring that all users completed the required training, EOHED exposed itself to an increased risk of cybersecurity attacks and financial and/or reputation losses.

Authoritative Guidance

Section AT-2 of Revision 4 of the National Institute of Standards and Technology Special Publication 800-53 establishes the following best practices:

> *The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):*
>
> *a. As part of initial training for new users;*
>
> *b. When required by information system changes; and*
>
> *c. [Annually] thereafter.*

Additionally, Section 6.2 of the Executive Office of Technology Services and Security (EOTSS) Information Security Standard IS.010, "Information Security Risk Management," effective October 15, 2018, requires the following:

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. . . .*

2. During the audit period, an additional 51 EOHED agency employees terminated their employment without completing the training. However, EOHED management could not provide us with human resources records for these 51 employees so that we could determine whether they would have been required to take the training.

6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training.

Additionally, Section E04-09, "Intern and Volunteer Records," of the Massachusetts Statewide Records Retention Schedule 06-18 establishes the following requirement:

Retain 6 years after separation.

Documents individual volunteer and intern involvement with agency. Includes resumes, applications, agreements, work plans, and related correspondence.

Reasons for Noncompliance

EOHED officials stated that they believed the three MMP interns might have completed the required cybersecurity awareness training, but that because of miscommunication among MMP and EOHED human resources personnel, any such training was not documented. In addition, although EOHED agencies conducted some periodic reviews of training records, the reviews were not consistently performed by each agency; therefore, this monitoring control was ineffective at ensuring compliance with the training requirements.

Recommendation

EOHED should establish effective monitoring controls over its cybersecurity awareness training to ensure that all information system users complete it in accordance with EOTSS standards and that EOHED maintains documentation of the completion of this training.

Auditee's Response

Agency records provided to your staff do show that a relatively small number of employees and volunteer board members did not complete a cybersecurity training during the audit period. We would like to note that 13 of the 45 persons identified by your staff as not having completed a cybersecurity training were volunteer board members who do not have (and never had) access to the EOHED network.

As of May, 2018, EOHED and all agencies within the executive office have been utilizing updated, standardized cybersecurity training materials developed by the Executive Office of Technology Services and Security (EOTSS). This training program is administered by the Commonwealth Human Resources Department, and is provided to new employees through the statewide Performance and Career Enhancement (PACE) Learning Management System. The training program is required for all new employees, and must be completed within 30 days of the employee's start date. In addition, all existing employees were required to complete a cybersecurity training program developed by EOTSS and provided through a third party vendor. It is our expectation that EOTSS will make additional training sessions available in the future. We

currently are working with EOTSS and [the state's Human Resources Division, or HRD] to establish a tracking system so that EOHED can confirm whether and when employees within the executive office have completed cybersecurity training.

Although not technically within the scope of the audit or related to the audit finding, I would like to note that EOHED agencies do not rely solely on HRD/EOTSS cybersecurity training to keep employees informed of good cybersecurity practices. For example, the onboarding process for new employees includes a mandatory review and acknowledgement of the Acceptable Use of Information Technology Policy. Additionally, each EOHED agency lists its IT policies on an intranet site accessible to all employees. Further, all employees regularly receive email from EOTSS regarding best practices for avoiding cybersecurity threats and regular notification of phishing frauds and other known cybersecurity threats. The EOHED IT team routinely reissues these EOTSS notifications to ensure employees are aware of current threats. Agencies also regularly post notices in areas where employees congregate (e.g., copy machines and lunch areas) to remind employees of cybersecurity threats and ways to avoid them.

Auditor's Reply

As noted above, at least 45 of the information system users employed by agencies within EOHED during our audit period did not complete the required cybersecurity awareness training.

EOHED notes that there were 13 volunteer board members who did not have access to EOHED's network and would not have been required to complete the cybersecurity awareness training. We confirmed that the 45 employees did not include 13 volunteer board members but were regular employees who had access to EOHED's network.

In its response, EOHED asserts that these 45 employees represent a "relatively small number of employees"; however, even a single employee can be vulnerable to a cybersecurity attack. All system users should receive this training to effectively reduce the risk of such an attack.

Based on its response, EOHED is taking measures to ensure that its system users are properly trained in cybersecurity in accordance with EOTSS standards and is also working with EOTSS and HRD to establish a tracking system to monitor staff compliance with this training requirement. We again urge EOHED to maintain documentation of this training's completion.

OTHER MATTERS

Documented Evidence to Test System Access Controls

In performing our evaluation of the Executive Office of Housing and Economic Development's (EOHED's) internal controls, we intended to review and assess certain system access controls related to EOHED's network (specifically, whether information system users signed access agreements before accessing EOHED's network and whether EOHED revoked the access rights of terminated users in a timely manner). We selected samples of users who were hired by EOHED agencies during our audit period, as well as samples of users who terminated their employment at EOHED agencies during this period, to test these controls. We asked EOHED for the necessary information, which included supporting documentation to verify the dates of each employee's first access to the network and of each employee's termination of user access rights within the network. EOHED management responded in a letter that this information was not available because it "is not captured nor logged in a manner that depicts an accurate history of this activity."

As a best practice, Section PS-6 of Revision 4 of the National Institute of Standards and Technology Special Publication 800-53 states that users who need access to organizational information and information systems should sign appropriate access agreements before being granted access. Additionally, Section 6.1.6.2.1 of the Executive Office of Technology Services and Security (EOTSS) Information Security Standard IS.003, "Access Management," states that upon termination, users' access to information systems must be "removed within 24 business hours."

EOHED should implement procedures to provide supporting evidence that its controls are working as designed in compliance with EOTSS standards and industry best practices.

Auditee's Response

As of now, new employees are provided user access to the EOHED network when they are credentialed and start employment, though neither EOHED nor EOTSS has in place a system to track the date and time of a new employee's first use of the EOHED network. Similarly, EOTSS does not record the date and time when user access rights are terminated. In response to your office's recommendation, EOHED will consult with EOTSS to determine if steps can be taken to document this information.

Auditor's Reply

As previously noted, during our audit, we identified areas in EOHED's information technology (IT) environment that we thought could be improved. We decided that these issues were significant enough to present in the "Other Matters" section of this report for management's consideration. Although we are confident that the IT control enhancements we suggest would strengthen EOHED's control environment and improve its IT security, we acknowledge that it is ultimately up to EOHED management to determine what measures to take to address these issues given the agency's work environment and available resources. We are encouraged by EOHED's acknowledgement that improvements can be made in the areas identified and by its willingness to take the measures it deems feasible to enhance IT controls over these areas.