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

Official Audit Report – Issued October 10, 2018

Executive Office for Administration and Finance

For the period October 1, 2017 through March 31, 2018

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

October 10, 2018

Mr. Michael J. Heffernan, Secretary
Executive Office for Administration and Finance
24 Beacon Street, State House, Room 373
Boston, MA 02133

Dear Mr. Heffernan:

I am pleased to provide this performance audit of the Executive Office for Administration and Finance. This report details the audit objectives, scope, and methodology for the audit period, October 1, 2017 through March 31, 2018. My audit staff discussed the contents of this report with management of the agency, whose comments we considered when drafting this report.

I would also like to express my appreciation to the Executive Office for Administration and Finance for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CIS Control	Center for Internet Security Critical Security Control
EAMS	Employee Access Management System
EOAF	Executive Office for Administration and Finance
EOTSS	Executive Office of Technology Services and Security
IT	information technology
NIST	National Institute of Standards and Technology

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 for Administration and Finance (EOAF). The purpose of this audit was to review and evaluate controls over selected information technology (IT) operations and activities for the period October 1, 2017 through March 31, 2018.

In this performance audit, we examined EOAF's processes for managing the IT hardware connected to its network and determined whether EOAF had a program in place to detect, manage, and patch potential system and software vulnerabilities.

Based on our audit, we have concluded that EOAF has established adequate controls and practices in the areas we reviewed that were related to our audit objectives. We did not identify any significant deficiencies in those areas.

OVERVIEW OF AUDITED ENTITY

The Executive Office for Administration and Finance (EOAF), established by Chapter 7 of the Massachusetts General Laws, oversees fiscal planning and budgeting for the Commonwealth. It is headed by the Secretary of Administration and Finance, who reports directly to the Governor as a member of the Governor's cabinet.

Section 3 of Chapter 7 of the General Laws identifies EOAF's responsibilities, which include the following:

1. *Developing, co-ordinating, administering and controlling the financial policies and programs of the commonwealth;*
2. *Supervising the organization and conduct of the business affairs of the departments, commissions, offices, boards, divisions, institutions and other agencies within the executive department of the government of the commonwealth;*
3. *Developing new policies and programs which will improve the organization, structure, functions, economy, efficiency, procedures, services and administrative practices of all such departments, commissions, offices, boards, divisions, institutions and other agencies.*

Through its various entities, EOAF is responsible for maintaining Commonwealth assets, collecting taxes, performing human-resource functions, and supervising other state fiscal and/or administrative matters. EOAF administers the following entities:

Appellate Tax Board
Bureau of the State House
Civil Service Commission
Department of Revenue
Division of Administrative Law Appeals
Division of Capital Asset Management and Maintenance
Group Insurance Commission
Human Resources Division
Massachusetts Developmental Disabilities Council
Massachusetts Office on Disability
Operational Services Division
State Library of Massachusetts
Massachusetts Teachers' Retirement System
Public Employee Retirement Administration Commission

Chapter 64 of the Acts of 2017 established the Executive Office of Technology Services and Security (EOTSS) as a cabinet-level executive office with a mandate to consolidate and centralize all of the state's information technology (IT) functions, including its network and procurement. All secretariats, including EOAF, are required to appoint chief information officers to coordinate their organizations' IT activities with EOTSS.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain information technology (IT) activities of the Executive Office for Administration and Finance (EOAF) for the period October 1, 2017 through March 31, 2018.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer and the conclusion we reached regarding each objective.

Objective	Conclusion
1. Does EOAF actively manage the inventory of hardware devices connected to its network?	**Yes**
2. Does EOAF have a program in place to detect, manage, and patch[1] potential system and software vulnerabilities?	**Yes**

We conducted this performance audit using criteria from policies issued by the Executive Office of Technology Services and Security (EOTSS) as well as industry standards established in the Center for Internet Security Critical Security Controls (CIS Controls) 1 and 3, which are based on the National Institute of Standards and Technology's (NIST's) Special Publication 800-53r4. Although EOTSS is not required to follow these industry standards, we believe they represent IT industry best practices for cybersecurity. The EOTSS policies we used as criteria are also derived from NIST Special Publication 800-53r4.

1. According to the National Institute of Standards and Technology's Special Publication 800-40r3, patches are software packages deployed by a manufacturer to "correct security and functionality problems in software and firmware."

CIS Control 1 states that IT organizations should do the following:

> *Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.*

CIS Control 3 states that IT organizations should do the following:

> *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.*

Systems and Applications Relevant to the Audit

EOAF and its agencies use a variety of systems and applications to carry out day-to-day tasks. Our audit focused primarily on the following applications that were relevant to our audit objectives:

1. ServiceNow, a cloud-based Web application that is used to manage and administer computing devices such as laptops, desktops, and servers from a central application interface
2. Employee Access Management System (EAMS), an application that is used to keep track of the Commonwealth's IT hardware inventory
3. Nessus, an application that scans all computers and devices connected to a common network for known software vulnerabilities
4. ZENworks, an application that is used to keep all software (such as Adobe Flash and Adobe Acrobat Reader) that is installed on laptops and desktops up to date from one point of management through a central application interface

Audit Procedures

To achieve our audit objectives, we gained an understanding of the internal control environment related to our audit objectives by reviewing applicable EOAF and EOTSS policies and procedures, reviewing relevant laws and regulations, and interviewing various EOAF staff members and outside contractors. Additionally, we performed the following procedures:

- We surveyed EOAF regarding the activities it performs to adhere to the various subcontrols[2] outlined in CIS Controls 1 and 3 to determine whether EOAF adhered to these CIS Controls.
- We performed a walkthrough of ServiceNow and EAMS and obtained screenshots of the process undertaken to keep track of EOAF's IT hardware inventory to confirm that this process existed.

2. CIS subcontrols are questions intended to evaluate whether the guidelines set forth in the CIS Controls are in place.

- We requested and examined a list of all EOAF IT hardware listed in ServiceNow and EAMS to determine whether EOAF had a clear understanding of what devices were connected to its network.

- We performed a walkthrough of the patching process for Windows and Linux servers and obtained screenshots from our observation of the process to confirm that EOAF had a process to keep its vital systems up to date.

- We performed a walkthrough of the ZENworks patching process and obtained screenshots from our observation thereof to confirm that EOAF had a process to keep the applications on its systems up to date.

- We observed a walkthrough of Nessus conducted by EOAF and EOTSS staff members. We observed scans of the network for system vulnerabilities and obtained screenshots of the process to confirm that EOAF had a process in place to scan its network regularly for known vulnerabilities.