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

Official Audit Report – Issued September 27, 2018

Executive Office of Public Safety and Security

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

September 27, 2018

Mr. Daniel Bennett, Secretary
Executive Office of Public Safety and Security
1 Ashburton Place, Suite 2133
Boston, MA 02108

Dear Mr. Bennett:

I am pleased to provide this performance audit of the Executive Office of Public Safety and Security. 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 of Public Safety and Security 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
EOPSS	Executive Office of Public Safety and Security
EOTSS	Executive Office of Technology Services and Security
IT	information technology
NIST	National Institute of Standards and Technology
OTIS	Office of Technology Information Services

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 Public Safety and Security (EOPSS). 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 EOPSS's processes for managing the IT hardware connected to its network and determined whether EOPSS had a program in place to detect, manage, and patch potential system and software vulnerabilities.

Based on our audit, we have concluded that EOPSS 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 of Public Safety and Security (EOPSS) is a secretariat that oversees the state's public safety agencies, boards, and commissions, which include the following:

Department of Criminal Justice Information Services
Department of Fire Services
EOPSS Information and Technology Department
Homeland Security Division
Massachusetts Department of Correction
Massachusetts Emergency Management Agency
Massachusetts National Guard
Massachusetts Parole Board
Massachusetts Public Safety Broadband Office
Massachusetts State Police
Massachusetts State Police Crime Laboratory
Municipal Police Training Committee
Office of the Chief Medical Examiner
Office of Grants and Research
Sex Offender Registry Board
State 911 Department

According to its website,

> *EOPSS is responsible for the policy development and budgetary oversight of its secretariat agencies, independent programs, and several boards which aid in crime prevention, homeland security preparedness, and ensuring the safety of residents and visitors in the Commonwealth.*

The Office of Technology Information Services (OTIS) within EOPSS provides consolidated information technology services and support to the agencies and personnel it oversees. Additionally, OTIS operates and manages a public safety data center that is open 24 hours a day, seven days a week, and a Criminal Justice Information Systems network to support the Commonwealth's justice and law enforcement personnel.

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 of Public Safety and Security (EOPSS) 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 EOPSS actively manage the inventory of hardware devices connected to its network?	**Yes**
2. Does EOPSS have a program in place to detect, manage, and patch[1] potential system and software vulnerabilities?	**Yes**

We conducted this performance audit by 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's 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

EOPSS and its entities use a variety of systems and applications to carry out day-to-day tasks. Our audit focused primarily on examining 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. Nessus, an application that scans all computers and devices connected to a common network for known software vulnerabilities.

Audit Procedures

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

- We conducted a survey of EOPSS regarding what activities it performed to adhere to the various subcontrols[2] outlined in CIS Controls 1 and 3 to ensure that the devices on the network were monitored and that a vulnerability scan process was in place.
- We performed an overall walkthrough of the patching process to ensure that software patches were actively updated. We focused on the patch frequency and triage patches[3] being deployed.
- We performed a walkthrough of ServiceNow to determine whether EOPSS had an automated process to track what devices were connected to its network.
- We obtained and verified a list of all EOPSS IT hardware recorded in ServiceNow to ensure that EOPSS had accurate information on what devices were connected to its network.

2. CIS subcontrols are questions intended to evaluate whether the guidelines set forth in the CIS Controls are in place.
3. Triage patches are done in order of greatest risk to least risk.

- We performed a walkthrough of Nessus to ensure that EOPSS kept up to date with software releases to mitigate security vulnerabilities.

- We requested and reviewed an example of a vulnerability scan report from Nessus to determine whether EOPSS knew that vulnerabilities existed on its network.