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

Official Audit Report – Issued November 5, 2021

Office of the Inspector General—Review of Cybersecurity Awareness Training

For the period January 1, 2019 through December 31, 2020

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

November 5, 2021

Mr. Glenn Cunha, Inspector General
Office of the Inspector General
1 Ashburton Place, 13th Floor
Boston, MA 02108

Dear Inspector General Cunha:

I am pleased to provide this performance audit of the Office of the Inspector General. This report details the audit objective, scope, methodology, and conclusion for the audit period, January 1, 2019 through December 31, 2020. 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 Office of the Inspector General 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

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 Office of the Inspector General (OIG)[1] for the period January 1, 2019 through December 31, 2020. In this performance audit, we determined whether OIG administered a cybersecurity awareness training program that complied with the Executive Office of Technology Services and Security's (EOTSS's) requirements and industry best practices.

Our audit revealed no significant instances of noncompliance by OIG that must be reported under generally accepted government auditing standards. However, in performing our audit testing, we found an internal control issue: OIG had not established a written policy regarding its cybersecurity awareness training. This written policy would include establishing a requirement for all employees to receive cybersecurity awareness training upon hire and annually thereafter as required by EOTSS standards. We brought this matter to the attention of OIG officials who established a formal, written cybersecurity awareness training policy after our audit.

1. Generally accepted government auditing standards require that organizations be free from organizational impairments to independence with respect to the entities they audit. In accordance with Section 2 of Chapter 12A of the General Laws, the Inspector General is appointed by a majority vote of the Attorney General, State Auditor, and Governor. Additionally, pursuant to Section 3 of Chapter 12A of the General Laws, State Auditor Suzanne M. Bump serves on the eight-member Inspector General Council along with the Attorney General; the Secretary of Public Safety; the State Comptroller; and four other members appointed separately by the Attorney General, State Auditor, and Governor. This disclosure is made for informational purposes only, and this circumstance did not interfere with our ability to perform our audit work and report its results impartially.

OVERVIEW OF AUDITED ENTITY

The Office of the Inspector General (OIG) was established in 1981 by Section 2 of Chapter 12A of the Massachusetts General Laws. The Inspector General is appointed by the Governor, Attorney General, and State Auditor for a maximum of two five-year terms.

According to OIG's website,

> *[OIG] is an independent agency that prevents and detects fraud, waste and abuse of public funds and public property and promotes transparency in government.*

To allow OIG to meet its mandated responsibilities, Chapter 12A gives OIG subpoena power and the authority to investigate both criminal and civil violations of the law.

OIG is composed of the following divisions: the Audit, Oversight and Investigations Division; the Bureau of Program Integrity; the Division of State Police Oversight; the Internal Special Audit Unit for the Massachusetts Department of Transportation; the Policy and Government Division; the Regulatory and Compliance Division; the Administration and Finance Division; and the Legal Division.

During fiscal years 2020 and 2021, OIG received state appropriations of $5,685,654 and $5,916,287, respectively. It had approximately 87 and 83 full-time employees in 2019 and 2020, respectively. OIG is located at 1 Ashburton Place in Boston.

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 Office of the Inspector General (OIG) for the period January 1, 2019 through December 31, 2020.

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 and the conclusion we reached regarding the objective.

Objective	Conclusion
1. Did OIG administer a security awareness training program in accordance with Sections 6.2.3, 6.2.4, 6.2.1.3, 6.2.7, and 6.2.8 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010 and Control AT-1 of the National Institute of Standards and Technology's Special Publication 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*?	**Yes**

To achieve our audit objective, we first gained an understanding of the internal controls related to the objective by conducting interviews with OIG management and other staff members involved in administering the agency's cybersecurity awareness training. We observed certain management activities related to the administration of this training. We also requested and reviewed OIG's *Personnel Policies and Procedures Manual* to determine OIG's cybersecurity awareness training program requirements. While reviewing the manual, we found that during the audit period, OIG had not established a formal written cybersecurity awareness training policy. We brought this matter to the attention of OIG officials, and in March 2021, after our audit, OIG incorporated a cybersecurity awareness training policy into the 2021 edition of its *Personnel Policies and Procedures Manual*.

Additionally, we performed the following procedures to address our audit objective.

To determine whether all OIG system users completed their cybersecurity awareness training (using a training system called KnowBe4), we obtained from OIG a list of all OIG employees during the audit period. We reviewed all OIG's cybersecurity awareness training records and determined which OIG system users received the training during the audit period and whether they completed the training within the timeframe established by EOTSS standards.

To determine whether all new OIG employees received the cybersecurity awareness training in accordance with EOTSS requirements, we obtained from OIG a list of the 55 employees it hired during the audit period. From this list, we selected a nonstatistical, random sample of 20 individuals for testing. For each individual in our sample, we examined the orientation date and onboarding training records to determine whether s/he completed initial cybersecurity awareness training during orientation in his/her onboarding period. In addition, we requested from OIG's Human Resources Department copies of signed Employee Acknowledgment of Receipt forms, which include the acknowledgment of OIG's "Acceptable Use of IT Resources" policy, for all of the 20 users. We verified that there was a signature on the Employee Acknowledgment of Receipt form for each user in the sample to ensure that all users had signed the form and acknowledged the policy.

Because we used a nonstatistical approach for our audit sample, we could not project our results to the entire population of system users.

Data Reliability

OIG gave us a list of all its employees from the audit period, which it extracted from the Commonwealth's Human Resources Compensation Management System. To assess the reliability of the data on this list, we tested for duplicate data, missing data, and data outside the audit period. We also compared the list to the list of OIG employees in the Commonwealth Information Warehouse.[2]

To assess the reliability of OIG's cybersecurity awareness training records, we tested for missing and duplicate data. We also interviewed EOTSS's director of governance, risk, and compliance and observed her exporting the training records from the system.

2. According to the Office of the Comptroller of the Commonwealth's website, the Commonwealth Information Warehouse is a system that "brings together a subset of the financial, budgetary, human resources, payroll and time reporting information maintained in dedicated and separate systems by individual agencies."

Based on the results of these data reliability assessment procedures, we determined that the data obtained from OIG were sufficiently reliable for the purpose of the audit.

Conclusion

Our audit revealed no significant instances of noncompliance that must be reported under generally accepted government auditing standards.