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

Official Audit Report – Issued October 29, 2021

Attorney General's Office—Review of Cybersecurity Awareness Training

For the period July 1, 2018 through July 31, 2020

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

October 29, 2021

Attorney General Maura Healey
Attorney General's Office
1 Ashburton Place, 20th Floor
Boston, MA 02108

Dear Attorney General Healey:

I am pleased to provide this performance audit of the Attorney General's Office. This report details the audit objective, scope, methodology, finding, and recommendations for the audit period, July 1, 2018 through July 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 Attorney General's Office 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

AGO	Attorney General's Office
EOTSS	Executive Office of Technology Services and Security
HR/CMS	Human Resources Compensation Management System
IT	information technology
NIST	National Institute of Standards and Technology
SANS	SysAdmin, Audit, Network, and Security

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 Attorney General's Office (AGO) for the period July 1, 2018 through July 31, 2020. In this performance audit, we reviewed AGO's cybersecurity awareness training and practices to determine whether all employees had completed cybersecurity awareness training and signed information technology policies.

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

Finding 1 **Page 6**	AGO did not offer cybersecurity awareness training during a portion of the audit period.
Recommendations **Page 7**	1. AGO should ensure that initial cybersecurity awareness training for new hires and annual training thereafter for existing employees are always available. 2. If a new vendor or training program is selected, an interim training plan should always be in place to ensure continuity in cybersecurity awareness training during the transition to the new vendor or program.

Post-Audit Action

During the audit, AGO management provided the audit team with the agency's then-current draft of its cybersecurity awareness training policy. Our review of this draft policy indicated that AGO had addressed the concern discussed in the audit report regarding the lack of training for employees, such as student interns, who were compensated outside the Human Resources Compensation Management System during the audit period. It did so by including these employees in future trainings.

OVERVIEW OF AUDITED ENTITY

The Attorney General's Office (AGO) was established by Section 1A of Chapter 12 of the Massachusetts General Laws. AGO is composed of six bureaus: the Executive Bureau, the Criminal Bureau, the Government Bureau, the Public Protection and Advocacy Bureau, the Health Care and Fair Competition Bureau, and the Energy and Environmental Bureau. According to its website,

> *The Massachusetts Attorney General's Office is an advocate and resource for the people of Massachusetts in many ways, including protecting consumers, combating fraud and corruption, investigating and prosecuting crime, and protecting the environment, workers, and civil rights.*

During the audit period, AGO distributed and monitored its cybersecurity awareness training through the SysAdmin, Audit, Network, and Security system and the KnowBe4 system.

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 activities of the Attorney General's Office (AGO) for the period July 1, 2018 through July 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, the conclusion we reached regarding the objective, and where the objective is discussed in the audit findings.

Objective	Conclusion
1. Did AGO administer a security awareness training program in accordance with Sections 6.2.1.3, 6.2.3, 6.2.4, 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 Controls AT-1(a)(1) and AT-2(a) of the National Institute of Standards and Technology's (NIST's) Special Publication 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*?	**Partially; see Finding 1**

We conducted this performance audit using policies, procedures, and standards issued by AGO. We also used NIST's Special Publication 800-53r4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Although AGO is not required to follow this industry standard, it represents best practices for information system security. Additionally, we used criteria from enterprise security policies and standards issued by EOTSS. A preliminary version of the EOTSS enterprise security policies was available to agencies in October 2017, and agencies were required to comply with a final version starting October 15, 2018. Although AGO is an independent agency,[1] agencies that use EOTSS resources are required to comply with these policies and standards.

1. According to mass.gov, "Independent agencies and commissions are part of the Executive Branch. However, they are not subject to oversight or control by the Executive Branch."

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

To determine whether all personnel completed the annual cybersecurity awareness training, we obtained a list of all personnel at AGO during the audit period. For employees who were in the Human Resources Compensation Management System (HR/CMS),[2] we reviewed the electronic training records in the SysAdmin, Audit, Network, and Security (SANS) and KnowBe4 training systems. We also reviewed the training records in SANS and KnowBe4 to determine whether all employees completed the training within the timeframe set by AGO. For personnel, such as interns and volunteers, who were not in HR/CMS because they were not paid through that system and whose access to the network was more restricted than that of full-time employees, AGO provided us with documentation indicating that it did not provide the same training outside HR/CMS during the audit period because of cost considerations.

We also examined and reviewed the SANS and KnowBe4 programs, including their training content and training procedures, to ensure that they were in accordance with EOTSS's Information Security Risk Management Standard IS.010.

We selected a nonstatistical, random sample of 35 of 243 newly hired users whom the agency required to take the training. For each user in our sample, we reviewed and compared the electronic records with the new hire orientation date to determine whether the user completed the initial cybersecurity awareness training within 30 days of new hire orientation. In addition, we requested from AGO's Human Resources Department the signed Employee Manual Acknowledgment Statement that included the acknowledgment of AGO's information technology (IT) policy for each newly hired user in our sample. We performed an observation to verify the signature on the Employee Manual Acknowledgment Statement for each user in the sample to ensure that all users had signed and acknowledged AGO's IT policy. Because we used a nonstatistical approach for our audit sample, we could not project our results to the entire population of employees.

2. This is the Commonwealth's official payroll system.

Data Reliability

AGO provided a list of users in HR/CMS. To assess the reliability of the list, we tested for duplicate data, missing data, and data outside the audit period. We also compared the list to the list of users in the Commonwealth Information Warehouse.[3]

To assess the reliability of AGO's cybersecurity awareness training records from SANS and KnowBe4, we tested for missing and duplicate data. We also interviewed AGO's chief information officer and observed him exporting the training records from both systems. Based on the results of these data reliability assessment procedures, we determined that the data obtained from HR/CMS, SANS, and KnowBe4 for our audit were sufficiently reliable for the purpose of the audit.

3. 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."

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Attorney General's Office did not offer cybersecurity awareness training during a portion of the audit period.

The Attorney General's Office (AGO) only offered its SysAdmin, Audit, Network, and Security (SANS) cybersecurity awareness training to current and new employees through September 28, 2018. Any employees hired after that date were not offered, or required to take, cybersecurity awareness training until June 30, 2020, when AGO finalized the implementation of its KnowBe4 training. Employees who received training in 2018 did not receive refresher training until they were required to take the new KnowBe4 training. Additionally, AGO management did not require users who were not compensated through the Human Resources Compensation Management System (HR/CMS), such as student interns, to take the SANS training. Lack of training for new employees and lack of refresher training for existing employees create a greater risk that employees and the agency may be vulnerable to a cyberattack.

Authoritative Guidance

Section 6.2 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010, 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. . . .*
>
> *6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training.*

Reasons for Issue

AGO management told us in an email,

> *As we've previously discussed, unlike our current protocol, the SANS training was available on a one-time basis and therefore did not capture everyone who worked at the Office during the audit period. This was a function of the tools then available, cost considerations, and adherence to EOTSS procedures at the time.*

Consequently, the transition from SANS to KnowBe4 resulted in a period when there was no cybersecurity awareness training in place at AGO.

Recommendations

1. AGO should ensure that initial cybersecurity awareness training for new hires and annual training thereafter for existing employees are always available.

2. If a new vendor or training program is selected, an interim training plan should always be in place to ensure continuity in cybersecurity awareness training during the transition to the new vendor or program.

Auditee's Response

In addition to specific comments about the audit finding, AGO also provided the following general comments:

In addition to keeping our large staff productive through provision and constant support of IT resources, the [IT] team continuously monitors cybersecurity risks and implements state-of-the-art defense mechanisms, both technological and behavioral. They do all of this seamlessly while laboring under the tight budgetary restrictions of the AGO's annual appropriation. The IT team's philosophy with respect to system vulnerabilities is proactive, not reactive, as evidenced by the sophisticated and multi-layered approach toward technological risk management that they promote.

Among the numerous security precautions the AGO's IT team has adopted in accordance with [National Institute of Standards and Technology] guidelines are:

- *robust endpoint security features, including up-to-date anti-virus software; firewall protection; next-generation cloud-native [artificial intelligence]–driven endpoint protection; and full disk encryption*
- *routine and urgent patch management, implemented remotely*
- *firewall redundancy*
- *industry-leading intrusion prevention software*
- *multiple approaches to web filtering, including daily updates of known security risks*
- *continuous network monitoring*
- *[uniform resource locator, or URL] defense software*
- *outside email warning flags (implemented by the Commonwealth's Executive Office of Technology Services and Security [EOTSS])*
- *standardized image on all AGO-issued devices, standard user accounts, and locked administrator privileges to prevent unauthorized software installations.*
- *restriction of personal devices to secure remote work*
- *multi-factor authentication requirements and [virtual private network] for remote work*

- *a multi-pronged cybersecurity awareness and training (CSAT) program, enforced through mandatory office policy, which includes*
  - *required annual training for all holders of AGO information system user accounts*
  - *required training for all new account holders as they on-board*
  - *optional monthly training for all users*
  - *phishing tests several times a year*
  - *a phish alert button to report suspected phishing emails to IT*
  - *additional mandatory training for all who click a phishing test link*

Implementation of these and other security tools are sponsored and supported by AGO leadership at the highest levels. Coupled with the constant focus of our IT team on system security, these strategies have protected the integrity of the AGO's network, which has never experienced a breach. We are proud of our record and committed to continuing to ensure strong security protection for the AGO's information system.

Regarding the audit finding, AGO stated,

The AGO implemented two [Cybersecurity Awareness and Training, or CSAT] campaigns during the audit period and one since, which is ongoing. These three campaigns are described below.

SANS July–September 2018

The AGO selected SANS as its CSAT provider in 2018. . . . At the time, EOTSS had chosen SANS, a reputable leader in CSAT, as a vendor and was offering discounted pricing, so the AGO purchased the program for all employees through a chargeback mechanism. Based on comparative risk analysis and pecuniary considerations, the AGO made the determination to require the training of all employees compensated through the HR/CMS system, but not temporary staff, interns, co-op students, or volunteers, whose access to sensitive data is more limited. Unlike the AGO's current CSAT protocol, discussed below, the SANS training was available on a one-time basis and not offered to everyone who worked at the AGO during the audit period. The structure of the campaign was a function of the tools then available, cost considerations, and adherence to contemporary EOTSS protocols.

The AGO's IT team ran the SANS CSAT campaign from July to September 2018 and achieved greater than 95% compliance from 573 enrolled users. The First Assistant Attorney General, the General Counsel, and the [chief information officer] acted as executive-level sponsors and promoters. The SANS tool tracked user completion, allowing for follow-up with users who did not timely complete the training module.

KnowBe4 June 2020

By late 2019, CSAT had jumped in popularity and more varied program options were becoming available. At that time, AGO IT staff started evaluating KnowBe4, an industry leader, to provide a

comprehensive ongoing CSAT program. . . . The AGO ultimately selected KnowBe4 and subsequently learned that EOTSS had done so as well. After exploring the possibility of securing a volume pricing discount by licensing the KnowBe4 program through EOTSS, the AGO decided to contract with KnowBe4 directly to enable us to tailor administration of the program to our needs by controlling such factors as the frequency and content of phishing tests. The AGO's KnowBe4 purchase and implementation was delayed for several months due to the unprecedented and rapid shift to remote work in the first quarter of 2020 necessitated by Covid-19.

The AGO ran the KnowBe4 campaign for three weeks in June 2020 and required its completion by 632 holders of AGO information system user accounts. Compliance was secured by 99.8% of the enrolled users (631 out of 632). Following completion of the mandatory training program in June, the AGO continued providing KnowBe4 CSAT modules throughout the year, including multiple phishing tests, required additional training for those that failed the phishing test, sent supplemental dramatized content monthly, and regular emails cautioning users against particular cybersecurity vulnerabilities.

KnowBe4 June 2021

On June 1, 2021, the AGO commenced a new required CSAT program, with expanded content from the 2020 program. The campaign was sent to 625 current employees and is delivered to all new employees on an ongoing basis. All new users are assigned the KnowBe4 CSAT on their first day of employment and are required to complete it within one week. As of the date of this letter, we have secured a 100% compliance level. As in 2020, we are supplementing this required training regularly by pushing out additional content, conducting periodic phishing tests, and required remedial training for those who fail those tests. Consequently, the AGO has satisfied the . . . recommendations . . . of the Draft Audit Report.

As outlined herein, the AGO is, and has been, diligent, proactive, and resourceful in its implementation of CSAT and attention to matters of cybersecurity.

Auditor's Reply

Based on its response and the information provided to the Office of the State Auditor during the audit regarding AGO's new cybersecurity awareness training policy, AGO has taken measures to address our concerns on this matter.