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

Official Audit Report – Issued June 2, 2022

Massachusetts District Attorneys Association

For the period July 1, 2019 through June 30, 2021

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

June 2, 2022

District Attorney Thomas Quinn III, President
Massachusetts District Attorneys Association
1 Bulfinch Place, Suite 202
Boston, MA 02114

Dear District Attorney Quinn:

I am pleased to provide this performance audit of the Massachusetts District Attorneys Association. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2019 through June 30, 2021. My audit staff discussed the contents of this report with management of the association, whose comments are reflected in this report.

I would also like to express my appreciation to the Massachusetts District Attorneys Association 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

CIO	chief information officer
EOTSS	Executive Office of Technology Services and Security
HR/CMS	Human Resources Compensation Management System
IT	information technology
MDAA	Massachusetts District Attorneys Association

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 Massachusetts District Attorneys Association (MDAA) for the period July 1, 2019 through June 30, 2021. In this performance audit, we examined whether MDAA ensured that its employees completed initial and annual cybersecurity awareness training and signed an acceptable use policy as required by the state's Executive Office of Technology Services and Security.

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

Finding 1 **Page 5**	MDAA did not ensure that employees received cybersecurity awareness training.
Recommendations **Page 5**	1. MDAA should develop and implement policies and procedures that require newly hired employees to receive initial cybersecurity awareness training within 30 days of their hire dates. 2. MDAA should develop and implement policies and procedures that require all employees to receive annual cybersecurity awareness training. 3. MDAA should retain records of training completion for each employee.

OVERVIEW OF AUDITED ENTITY

The Massachusetts District Attorneys Association (MDAA) was created by Section 20D of Chapter 12 of the Massachusetts General Laws. Its executive director is appointed by the 11 elected Massachusetts district attorneys. Each year, by majority, the district attorneys choose a president from among themselves. As of June 30, 2021, MDAA employed 10 people. Its office is at 1 Bulfinch Place, Suite 202, in Boston.

According to its most recent internal control plan, dated June 2021,

> *The MDAA's mission is to promote public safety, the fair and effective administration of justice, the education of prosecutors and the safeguarding of the rights of victims.*

According to its website and internal control plan, MDAA supports the 11 elected district attorneys and their staffs, including 785 prosecutors and 260 victim-witness advocates.

According to its website,

> *MDAA supports the District Attorneys by managing statewide business technology services and administering grants in the area of Violence Against Women and Motor Vehicle Crimes. MDAA also produces publications for prosecutors and victim-witness advocates, hosts dozens of prosecutor trainings annually, and provides information on budgetary, criminal justice, and public safety issues to the executive and legislative branches.*

In fiscal year 2020, the state Legislature provided $3,995,443 to MDAA. In fiscal year 2021, it provided $4,083,450.

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 Massachusetts District Attorneys Association (MDAA) for the period July 1, 2019 through June 30, 2021.

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; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Do MDAA employees complete initial and annual cybersecurity awareness training as required by Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010?	**No; see Finding 1**
2. Do MDAA employees sign an acceptable use policy as required by Section 6.2.8 of EOTSS's Information Security Risk Management Standard IS.010?	**Yes**

We also identified a record retention issue we believe warrants MDAA's attention, which we have disclosed in the "Other Matters" section of this report.

To achieve our objectives, we gained an understanding of MDAA's internal control environment related to the objectives by reviewing applicable MDAA policies and procedures, as well as conducting inquires with MDAA management.

Cybersecurity Awareness Training

To determine whether MDAA employees received initial and annual cybersecurity awareness training in accordance with EOTSS requirements, we inspected employee files, which should contain training certificates and/or transcripts, for all 13 employees who worked at MDAA during the audit period.

Acceptable Use Policy Signoffs

To determine whether MDAA employees had signed an acceptable use policy in accordance with EOTSS requirements, we inspected the "MDAA Information Technology User Responsibility Agreement" and "MDAA Policy on the Use of Information Technology Resources" for each of the 13 employees who worked at MDAA during the audit period to determine whether each employee had signed them.

Data Reliability Assessment

To determine the completeness and accuracy of the hardcopy list of 13 MDAA employees that we received from MDAA's legal counsel, we performed a query in the Human Resources Compensation Management System (HR/CMS), the Commonwealth's human resources and payroll system, to determine the total number of employees who worked at MDAA during the audit period and compared the HR/CMS query results to MDAA's list of employees. We also matched the 13 employee names, hire dates, and termination dates (where applicable) to hardcopy MDAA employee files.

Based on the results of these procedures, we determined that the MDAA employee list was sufficiently reliable for the purposes of this audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts District Attorneys Association did not ensure that employees received cybersecurity awareness training.

The Massachusetts District Attorneys Association (MDAA) did not ensure that employees received cybersecurity awareness training: none of the 13 employees who worked at MDAA during the audit period received either initial training (if they were new hires) or annual training (if they were not new hires). Insufficient cybersecurity awareness training may lead to user error and compromise the integrity and security of the district attorneys' computer network, which MDAA manages.

Authoritative Guidance

According to the Executive Office of Technology Services and Security's Information Security Risk Management Standard IS.010,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course. . . . The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*
>
> *6.2.4 Annual Security Awareness Training: All personnel will be required to complete Annual Security Awareness Training.*

Reasons for Issue

MDAA does not have policies and procedures that require new employees to receive cybersecurity awareness training within 30 days of their hire dates or that require employees to receive annual cybersecurity awareness training.

Recommendations

1. MDAA should develop and implement policies and procedures that require newly hired employees to receive initial cybersecurity awareness training within 30 days of their hire dates.
2. MDAA should develop and implement policies and procedures that require all employees to receive annual cybersecurity awareness training.
3. MDAA should retain records of training completion for each employee.

Auditee's Response

> *MDAA has implemented policies and procedures and a security awareness training program to enhance its security awareness practices for its employees. MDAA will require that newly hired*

employees receive initial cybersecurity awareness training within 30 days of their hire date as part of its onboarding process. MDAA will require that all employees receive annual cybersecurity awareness training. MDAA will retain records of training completion for all cybersecurity awareness trainings.

During the audit process, MDAA engaged a cybersecurity training vendor to provide an automated security awareness system and to create both an initial training and ongoing training program. MDAA staff have completed the first phase of cybersecurity awareness training. MDAA has drafted policies that outline the responsibilities and procedures for reporting phishing and suspicious emails, as well as the responsibilities and procedures for the [information technology] department to respond to these events.

Auditor's Reply

Based on its response, MDAA has taken measures to address our concerns on this matter.

OTHER MATTERS

The Massachusetts District Attorneys Association (MDAA) does not retain information technology (IT) records, such as reports or audit log history, as required by its own policy and the Executive Office of Technology Services and Security's (EOTSS's) Logging and Event Monitoring Standard IS.011.

Specifically, during the audit period, MDAA did not keep 101 of 104 antivirus reports, 24 of 24 Internet event monitoring reports, 5 of 730 firewall reports, 706 of 730 network monitoring reports, and 706 of 730 network compliance reports.

IT Reports

Type	Frequency	Total Reports from Audit Period	Reports Kept	Reports Not Kept
Antivirus	Weekly	104	3	101
Internet Event Monitoring	Every 30 days	24	0	24
Firewall	Daily	730	725	5
Network Monitoring	Daily	730	24	706
Network Compliance	Daily	730	24	706

Because MDAA does not retain IT reports or audit log history, it cannot effectively audit to identify cybersecurity threats or to ensure that its network has been effectively and efficiently protected.

According to MDAA's "Media and Records Policy,"

> *All correspondence, phone logs, emails, work-product and other files maintained in the normal course of business shall be retained for a minimum of three years after the last activity pertaining to the document, except that documents related to policy development shall be retained for a minimum of five years.*

According to Section 6.1.6.4 of EOTSS's Logging and Event Monitoring Standard IS.011, MDAA should do the following:

> *Retain audit trails for the required retention periods per business, legal or regulatory need. Audit* ***log*** *history must be retained for at least one (1) year, with a minimum of three (3) months immediately available for analysis.*

From our interviews and observations of MDAA's IT processes, it appears that MDAA did not fully understand the requirements of its "Media and Records Policy" or Section 6.1.6.4 of EOTSS's Logging and

Event Monitoring Standard IS.011. In addition, according to MDAA's chief information officer (CIO), reports were not retained because the alerts recorded in them had been mitigated or identified as incorrect (the alerts were in response to false threats) in real time and compiling them in a database would be cost and resource prohibitive. According to both MDAA's CIO and its chief information security officer, MDAA retained emails and documents only when an employee determined that there would be a need in the future (if there was a specific business requirement, another documented requirement, or an event requiring retention).

MDAA should follow the record retention requirements in its policy and retain an audit log history in accordance with Section 6.1.6.4 of EOTSS's Logging and Event Monitoring Standard IS.011.

Auditee's Response

MDAA will review its record retention policy and ensure that all staff receive and follow the updated policy. MDAA is working to comply with Section 6.1.6.4 of EOTSS's Logging and Event Monitoring Standard IS.011.

Auditor's Reply

Based on its response, MDAA is taking measures to address our concerns on this matter.