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

Official Audit Report – Issued December 13, 2019

Department of Revenue—Information Security

For the period July 1, 2016 through December 31, 2018

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

December 13, 2019

Mr. Christopher C. Harding, Commissioner
Department of Revenue
100 Cambridge Street
Boston, MA 02114

Dear Mr. Harding:

I am pleased to provide this performance audit of the Department of Revenue. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2016 through December 31, 2018. 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 Department of Revenue 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

DLS	Division of Local Services
DOR	Department of Revenue
EOAF	Executive Office for Administration and Finance
EOTSS	Executive Office of Technology Services and Security
ISA	interdepartmental service agreement
ISACA	Information Systems Audit and Control Association
IT	information technology
LMS	Learning Management System
MassIT	Massachusetts Office of Information Technology
NIST	National Institute of Standards and Technology
OSA	Office of the State Auditor
PII	personally identifiable information
UST	underground storage tank

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 Department of Revenue (DOR) covering the period July 1, 2016 through December 31, 2018. For our review of DOR's training programs, we used attendance records from April 19, 2018 through June 4, 2019. The purpose of this audit was to assess DOR's information security governance, information security training programs, information technology (IT) policies, incident response procedures, and management of third-party risks.

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

Finding 1 **Page 6**	DOR did not establish an IT strategy committee.
Recommendation **Page 7**	DOR should work with the Executive Office of Technology Services and Security (EOTSS) to establish an IT strategy committee that meets regularly to ensure IT governance, determine acceptable risk, align IT resources, and create strategies to mitigate risk to an acceptable level in line with business needs.
Finding 2 **Page 7**	DOR did not have documented and tested incident response procedures.
Recommendations **Page 8**	1. DOR should develop and document security incident response procedures to facilitate the implementation of its "Security Incident Response Policy" and associated incident response controls. 2. Once security incident response procedures are documented, DOR should test them regularly.
Finding 3 **Page 9**	DOR did not assess and document third-party vendor risks.
Recommendations **Page 10**	1. DOR should update its "Third Party Security Policy" to include procedures necessary to assess and document third-party risks. 2. DOR should assess and document third-party risks.
Finding 4 **Page 10**	DOR and EOTSS did not have an interdepartmental service agreement (ISA) that defined and documented updated roles and responsibilities.
Recommendation **Page 11**	DOR should work with EOTSS to negotiate an updated ISA that spells out roles and responsibilities related to information security and IT governance at DOR.

OVERVIEW OF AUDITED ENTITY

The Department of Revenue (DOR), an agency within the Executive Office for Administration and Finance (EOAF), was established by Section 1 of Chapter 14 of the Massachusetts General Laws. According to its website,

> *The DOR's mission is to gain full compliance with the tax, child support, and municipal finance laws of the Commonwealth. DOR is committed to enforcing these laws in a fair-minded and respectful manner.*

DOR has four main divisions: Tax Administration, Child Support Enforcement, the Division of Local Services (DLS), and the Underground Storage Tank (UST) Program. The focus of DOR's tax administration function is to manage the Commonwealth's tax collection, and the focus of DOR's child support function is to establish paternity and administer child support orders. Additionally, DOR helps cities and towns manage their finances through DLS. Finally, the UST Program was established to administer the Massachusetts Underground Storage Tank Petroleum Product Cleanup Fund, created in 1991 under Chapter 21J of the General Laws.

The Executive Office of Technology Services and Security's (EOTSS's) predecessor agency was the Massachusetts Office of Information Technology, which had a supervisory role over information technology (IT) at executive branch agencies within the Commonwealth. On August 1, 2017, EOTSS was formed by the Governor with the goal of consolidating more IT functions in executive branch agencies into a central agency. This was called the One Network initiative.

EOTSS and EOAF manage DOR's IT services. Although EOTSS has had an increasing role in DOR's IT Department, DOR is still responsible for establishing controls to ensure the proper safeguarding of the information it collects and retains in its systems.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of certain activities of the Department of Revenue (DOR) for the period July 1, 2016 through December 31, 2018. For our review of DOR's training programs, we used attendance records from April 19, 2018 through June 4, 2019.

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. Does DOR have a governing committee tasked with identifying, classifying, and mitigating information security risks?	**No; see Finding 1**
2. Has DOR designed and implemented user training programs and acknowledgement forms to protect personally identifiable information (PII)?	**Yes**
3. Have policies supporting PII protection been defined and documented?	**Yes**
4. Does DOR have documented and tested procedures to handle information security incidents?	**No; see Finding 2**
5. Does DOR manage risks with third-party vendors to meet Executive Office of Technology Services and Security (EOTSS) standards and National Institute of Standards and Technology (NIST) standard 800-53r4 related to the protection of PII?	**No; see Findings 3 and 4**

We conducted this performance audit by using criteria from policies, procedures, and standards issued by DOR, as well as policies and standards issued by the Massachusetts Office of Information Technology (MassIT) before October 15, 2018. MassIT is the predecessor agency to EOTSS. In addition, we referred to enterprise security policies and standards issued by EOTSS, which had an effective date of October 15, 2018.

We also referred to NIST's Special Publication 800-53, Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations*, and Special Publication 800-122, titled *Guide to Protecting the Confidentiality of Personally Identifiable Information,* as well as the Information Systems Audit and Control Association's (ISACA's) *Control Objectives for Information and Related Technology 4.1*. Although DOR is not required to follow these industry standards, OSA believes they represent best practices for information security.

We gained an understanding of the internal controls we deemed significant to our audit objectives through interviews and observations. To achieve our audit objectives, we conducted the following activities.

- To assess whether DOR had a governing committee tasked with identifying, classifying, and mitigating information security risks, we performed the following procedures:
    - We interviewed employees to determine whether an information technology (IT) strategy committee was in place and active at DOR.
    - We reviewed both sets of meeting minutes by DOR's security review board from the audit period to determine the content of the meetings and whether they constituted an IT strategy committee.
- To assess the design and implementation of DOR's user training programs and acknowledgement forms aimed at protecting PII, we performed the following procedures:
    - We reviewed both DOR's and the Executive Office for Administration and Finance's confidentiality policies to determine whether they complied with ISACA best practices.
    - We reviewed DOR's "Safeguarding DOR's Critical Assets: Information and Public Trust" training program to determine whether it addressed the 2019 "Confidentiality Policy" and "Acceptable Use Policy."
    - We obtained DOR's training attendance records from its Learning Management System (LMS) between April 19, 2018 and June 4, 2019 and reviewed records for all 1,950 users assigned to the 2018 "Safeguarding DOR's Critical Assets: Information and Public Trust" program, and all 1,939 users required to sign the 2019 "Confidentiality Policy," to determine whether the users completed them.
- To assess DOR's IT security policies and determine whether DOR had policies and procedures to cover all 16 of EOTSS's information security policies and standards, we cross-referenced DOR's policies and procedures with EOTSS's.
- To assess DOR's security incident response procedures and determine whether they constituted a security incident response plan, we obtained and reviewed DOR's "Security Incident Response Policy."

- To assess DOR's risk management with its third-party contractors, we performed the following procedures:
    - We reviewed a judgmental sample of 17 out of 22 DOR contracts with vendors identified by DOR officials as having received or accessed PII during our audit period to determine whether the contracts contained applicable information security and confidentiality provisions.
    - We asked whether DOR had documented risk assessments for its third-party vendors.
    - We reviewed DOR's interdepartmental service agreement with EOTSS to determine whether it clearly spelled out each entity's roles and responsibilities.

To assess the completeness and accuracy of training records from LMS, we interviewed the system administrator at DOR. In addition, we observed an LMS administrator obtaining the training records from LMS. We performed electronic tests to check for duplicate records and other abnormalities and assessed the query that was used to extract the data to determine its sufficiency for our testing purposes. To assess the accuracy of DOR's list of vendors that received PII, we vouched[1] vendors from this list to vendors in the Commonwealth Information Warehouse. However, because there was no other way for us to determine which vendors had access to PII, we relied on the list provided by DOR. Based on the results of these data reliability assessment procedures, we determined that the information obtained for our audit was sufficiently reliable for the purpose of our audit.

[1] Vouching is the act of comparing auditee-provided documentation to source documentation to determine the accuracy of data.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Department of Revenue did not establish an information technology strategy committee.

The Department of Revenue (DOR) did not have an information technology (IT) strategy committee whose role would include ensuring IT governance, determining acceptable risk, aligning IT resources, and creating strategies to mitigate risk to an acceptable level in line with business needs. DOR previously had a security review board, but the board has not been active since early 2017. In addition, it did not have governance over the allocation of IT resources or the determination of acceptable risks. Without a committee or board charged with governing DOR's IT environment, responsibility for IT governance and risk is not clear. This can result in information security risks and investments not being aligned with business needs.

Authoritative Guidance

The Information Systems Audit and Control Association's *Control Objectives for Information and Related Technology 4.1* establishes the following best practices for IT governance.

> ***PO4 Define the IT Processes, Organization and Relationships . . .***
>
> *A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritization of IT resources in line with business needs. . . .*
>
> ***PO4.2 IT Strategy Committee***
>
> *Establish an IT strategy committee at the board level. This committee should ensure that IT governance, as part of enterprise governance, is adequately addressed; advise on strategic direction; and review major investments on behalf of the full board. . . .*
>
> ***PO4.8 Responsibility for Risk, Security and Compliance***
>
> *Embed ownership and responsibility for IT-related risks within the business at an appropriate senior level. Define and assign roles critical for managing IT risks, including the specific responsibility for information security, physical security and compliance. Establish risk and security management responsibility at the enterprise level to deal with organization-wide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Obtain direction from senior management on the appetite for IT risk and approval of any residual IT risks.*

Reasons for Noncompliance

As part of the One Network initiative, the Executive Office of Technology Services and Security (EOTSS) is responsible for IT governance throughout the Commonwealth. However, EOTSS and DOR have not yet defined roles and responsibilities related to governance at DOR.

Recommendation

DOR should work with EOTSS to establish an IT strategy committee that meets regularly to ensure IT governance, determine acceptable risk, align IT resources, and create strategies to mitigate risk to an acceptable level in line with business needs.

Auditee's Response

> *DOR will work with EOTSS to establish a Governance, Risk, and Compliance (GRC) committee comprised of the following and/or their designees:*
>
> - *Commissioner*
> - *Chief Financial Officer*
> - *General Counsel*
> - *Chief Risk Officer*
> - *Chief Information Officer.*
>
> *GRC will meet at least annually or as needed to determine whether governance, risk management efforts, and resources (IT and non-IT) support the Agency's ability to achieve its mission.*

Auditor's Reply

Based on its response, DOR is taking measures to address this issue.

2. DOR did not have documented and tested incident response procedures.

Although DOR had a "Security Incident Response Policy," which included a policy outline and high-level responsibilities, it had not developed the "Security Incident Response Procedure" document that DOR management officials told us they planned to develop. This document would have outlined what DOR would do to implement its "Security Incident Response Policy" and what controls it would put in place to detect, respond to, and resolve incidents affecting the security of the personally identifiable information (PII) that DOR maintains. In addition, DOR could not provide evidence of an incident response test.

Without documented and tested incident response procedures, there is a higher-than-acceptable risk that DOR may not be able to respond properly to information security incidents, which may result in delayed identification of an incident, additional loss of data, or negative public opinion.

Authoritative Guidance

DOR's "Security Incident Response Policy," dated July 1 2015, states,

> *The DOR Security Incident Response Procedure should be consulted for more detailed process information.*

In addition, the "Incident Response" section of the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, Revision 4, establishes the following best practices:

> ***IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES***
>
> *Control: The organization:*
>
> *a. Develops, documents, and disseminates . . .*
>
> *1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and*
>
> *2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls. . . .*
>
> ***IR-3 INCIDENT RESPONSE TESTING***
>
> *Control: The organization tests the incident response capability for the information system . . . to determine the incident response effectiveness and documents the results.*

Reasons for Issue

DOR management officials stated that because of the vast number of scenarios that this incident response plan would have to cover, they are still in the process of developing it. They could not tell us when it would be developed.

Recommendations

1. DOR should develop and document security incident response procedures to facilitate the implementation of its "Security Incident Response Policy" and associated incident response controls.
2. Once security incident response procedures are documented, DOR should test them regularly.

Auditee's Response

> *The Incident Response Policy and Incident Response Plan (Plan) have been under revision. The Plan includes roles, responsibilities, and communication strategies for notifying and informing the appropriate individuals and groups. DOR will collaborate with [Executive Office for Administration and Finance] IT to develop and execute annual tests of the Plan, which may include (but not be limited to) tabletop exercises and drills.*

Auditor's Reply

Based on its response, DOR is taking measures to address this issue.

3. DOR did not assess and document third-party vendor risks.

During our audit period, DOR did not assess and document third-party risks for any of the vendors that received, or had access to, PII from DOR. To do this, DOR would need to assess both its use of vendors and the control risks at third-party vendors. A lack of assessment of third-party risks increases the chance that information security risks with such vendors will not be identified and mitigated promptly or at all, which results in a higher-than-acceptable risk of sensitive data being inappropriately accessed.

Authoritative Guidance

Section 6.2 of EOTSS standard IS.015, "Third-Party Information Security," effective October 15, 2018, requires the following of all executive state agencies:

> *All contracts by which a **third party** provides services to the Commonwealth or allows a **third party** to access, store, process, analyze, or transmit Commonwealth **confidential information** shall be assessed, prior to entering into an agreement, to determine the **third party's** capability to maintain the confidentiality, integrity and availability of Commonwealth **information assets.***

Previously, the "Enterprise Information Security Organization Policy" issued by EOTSS's predecessor agency, the Massachusetts Office of Information Technology, was effective from March 6, 2014 through October 14, 2018. Section 2 of the policy required all executive agencies to do the following for external parties, which include third-party vendors.

> ***[Document] the specific responsibilities of External Parties:*** *The documentation should include the identification of third party risks to the agency's information from business processes involving external parties with appropriate controls implemented prior to granting access, by:*
>
> *2.1 Performing a risk assessment of the identified security risks associated with conducting business with the third party prior to granting access and determine whether:*

> *2.1.1 The security risks can be remediated either by third parties or agency action.*
>
> *2.1.2 Compensating controls may be applied to satisfactorily diminish the security risks.*
>
> *2.1.3 The security risks can be effectively managed without undue risk to the agency.*

Reasons for Issue

DOR's "Third Party Security Policy" does not specify the steps DOR should take to assess and document third-party risks.

Recommendations

1. DOR should update its "Third Party Security Policy" to include procedures necessary to assess and document third-party risks.
2. DOR should assess and document third-party risks.

Auditee's Response

> *DOR will convene a working group to research and develop criteria and tools for evaluating and monitoring third party vendor risks.*

Auditor's Reply

Based on its response, DOR is taking measures to address this issue. We urge the agency and its working group to update DOR policies to include the criteria and tools developed and the monitoring process for third-party vendor risks.

4. DOR and EOTSS did not have an interdepartmental service agreement that defined and documented updated roles and responsibilities.

During our audit period, DOR migrated important IT functions, such as network security and user account management, to EOTSS. However, DOR did not have an interdepartmental service agreement (ISA) with EOTSS detailing each agency's roles and responsibilities related to information security in these areas. Unclear roles and responsibilities may result in activities related to IT security not being effectively managed.

Authoritative Guidance

Section SA-9 of NIST's Special Publication 800-53, Revision 4, establishes the following best practice:

> *[An] organization . . . defines and documents government oversight and user roles and responsibilities with regard to external information system services.*

Because EOTSS is an external agency to DOR, DOR should follow this best practice.

Reasons for Noncompliance

DOR management officials told us that they had been trying for three years to negotiate an ISA with EOTSS. They mentioned organizational and managerial changes at EOTSS as a cause of the delay.

Recommendation

DOR should work with EOTSS to negotiate an updated ISA that spells out roles and responsibilities related to information security and IT governance at DOR.

Auditee's Response

> *An ISA between DOR and EOTSS is currently being updated. The ISA will include roles and responsibilities of both parties.*

Auditor's Reply

Based on its response, DOR is taking measures to address this issue. We urge the agency to prioritize the development of an ISA to ensure that each agency's roles and responsibilities related to information security are properly defined.