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

Official Audit Report – Issued January 6, 2020

Department of Transitional Assistance—Information Security

For the period July 1, 2018 through June 30, 2019

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

January 6, 2020

Ms. Melissa Pullin, Acting Commissioner
Department of Transitional Assistance
600 Washington Street
Boston, MA 02111

Dear Ms. Pullin:

I am pleased to provide this performance audit of the Department of Transitional Assistance. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2018 through June 30, 2019. 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 Transitional Assistance for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Marylou Sudders, Secretary, Executive Office of Health and Human Services
Curt Wood, Secretary, Executive Office of Technology Services and Security

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

BEACON	Benefit Eligibility and Control Online Network
DTA	Department of Transitional Assistance
EAEDC	Emergency Aid to the Elderly, Disabled and Children
EOHHS	Executive Office of Health and Human Services
EOTSS	Executive Office of Technology Services and Security
HR/CMS	Human Resource Compensation Management System
ISACA	Information Systems Audit and Control Association
IT	information technology
MassIT	Massachusetts Office of Information Technology
NIST	National Institute of Standards and Technology
OSA	Office of the State Auditor
PII	personally identifiable information
SNAP	Supplemental Nutrition Assistance Program
SOC	System and Organization Control
SSI	Supplemental Security Income
TAFDC	Transitional Aid to Families with Dependent Children

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted an audit of the Department of Transitional Assistance (DTA) covering the period July 1, 2018 through June 30, 2019. The purpose of this audit was to assess DTA's training programs, information technology policies, password parameters, process for terminating user accounts, incident response procedures, and management of third-party risks.

Our audit of DTA identified an issue that has been omitted from this report in accordance with Exemption (n) of the Commonwealth's public-records law (Section 7[26] of Chapter 4 of the General Laws), which requires the withholding of certain records, including security measures or any other records related to cybersecurity or other infrastructure, if their disclosure is likely to jeopardize public safety or cybersecurity.

In accordance with Sections 7.39–7.41 of the Government Accountability Office's *Government Auditing Standards*, as well as OSA policies, for reporting confidential and sensitive information, we have given a separate, full report to DTA, which will be responsible for acting on our recommendations.

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

OVERVIEW OF AUDITED ENTITY

The Department of Transitional Assistance (DTA) was established by Sections 1 through 39 of Chapter 18 of the Massachusetts General Laws, as amended, and is under the purview of the Executive Office of Health and Human Services (EOHHS). DTA's information technology (IT) is administered by EOHHS. According to its website, DTA "assists and empowers low-income individuals and families to meet their basic needs, improve their quality of life, and achieve long term economic self-sufficiency."

DTA is organized into five regional areas and 22 transitional assistance offices, located throughout the Commonwealth, that are responsible for providing direct services to those seeking assistance. DTA had approximately 1,630 employees during fiscal year 2019. According to its annual organizational report for fiscal year 2019, DTA administered "four primary programs that receive both state and federal funding": the Supplemental Nutrition Assistance Program (SNAP); Transitional Aid to Families with Dependent Children (TAFDC); Emergency Aid to the Elderly, Disabled and Children (EAEDC); and Supplemental Security Income (SSI). The annual report states,

> *SNAP benefits help families supplement their food budgets to afford nutritious food. . . .*
>
> *TAFDC . . . provides financial assistance to families with children, and pregnant women, with little or no assets or income. . . .*
>
> *EAEDC is a state funded program, which provides financial assistance to certain adults who are elderly or disabled . . . as well as children. . . .*
>
> *The SSI program is a federal program that provides cash assistance to the elderly, disabled, and blind.*

The predecessor agency of the Executive Office of Technology Services and Security (EOTSS) was the Massachusetts Office of Information Technology, which had a supervisory role over IT at executive branch agencies within the Commonwealth, including DTA. 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. EOTSS oversees all IT in the Commonwealth. State agencies such as DTA are required to establish policies and procedures to ensure compliance with EOTSS requirements.

DTA's primary information system to administer benefits for SNAP, TAFDC, EAEDC, and SSI is the Benefit Eligibility and Control Online Network (BEACON) system. DTA workers enter information about each client into BEACON, which is programmed to determine each client's eligibility and benefit amounts,

keep track of when clients have to meet with caseworkers, and create notices to send to clients concerning their benefits. A secondary system, Caseview, is also used at three transitional assistance offices to track cases assigned to the offices.

Additionally, DTA uses the Human Resource Compensation Management System (HR/CMS), a Commonwealth application used to administer payroll and other human resource functions. HR/CMS is managed by the Commonwealth's Human Resource Division.

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 Department of Transitional Assistance (DTA) for the period July 1, 2018 through June 30, 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 DTA have user training programs and acknowledgment forms that meet the standards of the National Institute of Standards and Technology (NIST) related to the protection of personally identifiable information (PII)?	**Yes**
2. Has DTA designed and implemented password parameters and a process for terminating user accounts to protect the security of its information?	**Partially; see Finding 1**
3. Does DTA have documented and tested procedures to handle information security incidents?	**Partially; see Finding 2**
4. Does DTA manage risks with third-party vendors to meet Executive Office of Technology Services and Security (EOTSS) standards and NIST standard 800-53r4 related to the protection of PII?	**No; see Finding 3**

We conducted this performance audit using policies, procedures, and standards issued by DTA; enterprise security policies and standards issued by EOTSS; and Chapter 93H of the General Laws as criteria. A preliminary version of the EOTSS enterprise security policies was available to agencies in October 2017, and agencies were required to comply with a finalized version on October 15, 2018. Although compliance with these policies was not required for the whole audit period, they were available for agencies to view on EOTSS's website and represented best practices that should have been

followed by state agencies such as DTA. We also referred to standards issued by the Massachusetts Office of Information Technology (MassIT) before 2017. MassIT is EOTSS's predecessor agency.

We also used NIST Special Publication 800-53, Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST's *Framework for Improving Critical Infrastructure Cybersecurity*; the American Institute of Certified Public Accountants' *Trust Services Criteria*; and the Information Systems Audit and Control Association's (ISACA's) *Control Objectives for Information and Related Technology 4.1*. Although DTA is not required to follow these industry standards, they represent best practices for information security.

By conducting interviews and performing observations, we were able to gain an understanding of the internal controls that we deemed significant to our audit objectives. To achieve our audit objectives, we conducted the following procedures:

- To assess the design of DTA's user training programs and acknowledgement forms aimed at protecting PII, we performed the following procedures.
    - We conducted interviews of staff members charged with administering DTA's training programs to gain an understanding of DTA's training processes.
    - We evaluated the adequacy of the Executive Office of Health and Human Services' 2018 "Acceptable Use Policy," which DTA had adopted, by comparing it with ISACA best practices to determine its adherence to those practices.
    - We reviewed DTA's annual security awareness training materials from 2018 to determine whether they addressed the "Acceptable Use Policy" and complied with NIST best practices.
- To assess DTA's access controls over terminations and password parameters, we performed the following procedures.
    - We obtained a list of employees terminated between July 1, 2018 and June 30, 2019 from the Human Resource Compensation Management System (HR/CMS) to determine the dates employees were terminated from HR/CMS.
    - We took a nonstatistical sample of 25 terminated employees out of a population of 155 to determine whether these employees' access to DTA systems was terminated in a timely manner.
    - We reviewed DTA's password parameters to determine whether they complied with EOTSS standards.

- To assess DTA's security incident response procedures, we performed the following procedures.
    - We reviewed DTA's incident response plan to determine whether it addressed what EOTSS requires from agencies.
    - We asked about incident response tests during our audit period to determine whether DTA regularly performed such tests.
- To assess DTA's risk management with its third-party vendors, we performed the following procedures:
    - We asked whether DTA had documented risk assessments for its third-party vendors.
    - We reviewed DTA's interdepartmental service agreement with EOTSS to determine whether it clearly spelled out each party's roles and responsibilities.
    - We reviewed all four DTA contracts with vendors identified by DTA officials as having received or accessed PII during our audit period to determine whether the contracts contained applicable information security and confidentiality provisions.

To assess the completeness and accuracy of the list of terminated employees from HR/CMS, we interviewed the application security and operations manager, as well as human resource data analysts, at DTA. We also tested for missing data, duplicate data, and data outside the audit period. To assess the accuracy of DTA's list of vendors that received PII, we vouched vendors from this list to vendors in the Commonwealth's Information Warehouse. Because there was no other way for us to determine which vendors had access to PII, we relied on the list provided by the agency. 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 the audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Department of Transitional Assistance (DTA) did not revoke terminated employees' access to one of its systems in a timely manner.

Four out of 25 employees in our nonstatistical sample of employees who were terminated by the Department of Transitional Assistance (DTA) between July 1, 2018 and June 30, 2019 did not have their access to DTA's Benefit Eligibility and Control Online Network (BEACON) system revoked within 24 business hours (three business days) after their termination date. These employees had active accounts in BEACON for 6 to 23 days after their termination dates. This increases the risk that terminated employees could extract personally identifiable information (PII) from the system.

Authoritative Guidance

The American Institute of Certified Public Accountants' document *Trust Services Criteria* establishes the following best practice: "User system credentials are removed when user access is no longer authorized."

Section 6.1.6.2.1 of Executive Office of Technology Services and Security (EOTSS) information security standard IS.003, "Access Management," effective October 15, 2018, states that upon termination, users' access to information systems must be "removed within 24 business hours." Therefore, we used an allowable error of 24 business hours (three business days) in our test.

Reasons for Noncompliance

DTA relies on managers to manually notify DTA's information technology (IT) security team of employee terminations, and this was not always done in a timely manner. DTA uses the Commonwealth's Human Resource Compensation Management System, which does not have automated controls to notify BEACON or the security team when an employee is terminated.

Recommendations

1. DTA should implement additional controls to ensure that access is terminated in a timely manner after an employee is terminated.
2. DTA should consider controls to automatically notify the security team when employees are terminated.

Auditee's Response

The Executive Office of Health and Human Services (EOHHS) provided the following response on DTA's behalf.

> *To meet the needs of the FY2018 Single State Audit remediation plan, the following additional measures were undertaken:*
>
> - *DTA's Human Resource Department notify the DTA Security Team of terminations or lack thereof, on a weekly basis.*
> - *A quarterly review of terminations is conducted by DTA Application Security Management.*
> - *A further review on any user terminations that were not completed within the agreed upon time frame is conducted to ensure that the user did not access the system after their termination date.*
> - *DTA's Security Officer and Internal Controls Officer meet to review the results of the quarterly termination review and any terminations that were not completed within the agreed upon time frame are reported to DTA's Commissioner, Chief Operating Officer, Assistant Chief Information Officer and the EOHHS Chief Security Officer.*
>
> *Because of these additional controls, in the most recent Quarterly Termination Review, DTA was in full compliance with Section 6.1.6.2.1 of the EOTSS information security standard IS.003 "Access Management." DTA had no users who were not inactivated within 3 business days (24 working hours).*
>
> *DTA and EOHHS IT agree with your recommendation that automatic notification to the security team should occur when employees are terminated and believes that DTA would benefit greatly if the State's Human Resource Division updated the HRCMS System to provide this additional functionality.*

Auditor's Reply

Based on its response, DTA has taken measures to address our concerns in this area. The Office of the State Auditor (OSA) has not examined the results of the most recent quarterly review and therefore cannot conclude on the sufficiency of controls implemented after our audit.

2. DTA did not have a tested incident response plan.

During our audit period, DTA did not test an incident response plan. DTA provided us with a copy of an incident response plan, but stated that it was still in draft form and had not been tested at DTA. Without a tested incident response plan, there is a higher-than-acceptable risk that DTA cannot effectively identify and respond to information security incidents.

Authoritative Guidance

Section 6.5.2 of EOTSS information security standard IS.009, "Information Security Incident Management," effective October 15, 2018, requires the following:

> *Commonwealth Offices and Agencies shall establish a process to modify and evolve the **incident** response plan and procedures according to lessons learned. The **incident** response plan and procedures shall be tested at least annually.*

Section IR-8 of the National Institute of Standards and Technology Special Publication 800-53, Revision 4, establishes the following best practices:

> *The organization:*
>
> *a. Develops an incident response plan that:*
>
> *1. Provides the organization with a roadmap for implementing its incident response capability;*
>
> *2. Describes the structure and organization of the incident response capability.*

Reasons for Noncompliance

DTA personnel stated that they had previously conducted incident response tests with the Massachusetts Office of Information Technology (MassIT) before the audit period; however, this was not continued with EOTSS.

Recommendation

DTA should conduct incident response tests annually and modify its plan according to lessons learned.

Auditee's Response

EOHHS provided the following response on DTA's behalf.

> *As acknowledged in the audit report, while EOTSS previously engaged in incident management activities with DTA, those activities have not been conducted for some time. As a result, EOHHS operationalized an incident management program to assist with incident management at DTA and other EOHHS Agencies. EOHHS has developed an enterprise-wide incident response plan in its enterprise standards—which are the agency implementation standards of the EOTSS security policies—and will be meeting with DTA in January to begin operationalization of that plan at DTA. EOTSS has also stated that they will be primarily responsible for incident management at the Commonwealth. EOHHS is awaiting further definition of that role before proceeding too far with its incident response plan, as EOHHS is required to align its plan with EOTSS per the requirements of IS.009.*

Auditor's Reply

Based on its response, EOHHS and DTA are taking measures to address our concerns in this area. DTA, EOHHS, and EOTSS should continue to work together to define their roles in the development and implementation of the incident response plan and ensure that the plan is tested annually.

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

During our audit period, DTA did not assess and document third-party risks for any of the vendors that received, or had access to, PII from DTA. A lack of assessment of third-party risks increases the chance that information security risks with third-party 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, Section 2 of MassIT's "Enterprise Information Security Organization Policy," effective from March 6, 2014 through October 14, 2018, required all executive agencies to do the following:

> ***Documenting 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 Noncompliance

DTA did not develop a third-party security policy that specified the steps it should take to assess and document third-party risks. DTA managers were able to provide us with System and Organization Control (SOC) reports for some vendors,[1] which they believed to be sufficient. However, although SOC reports provide insight from external auditors on the design and effectiveness of vendors' IT controls, they do not assess the risks of DTA's use of vendors.

Recommendations

1. DTA should establish a third-party security policy that includes procedures necessary to assess and document third-party risks.
2. DTA should assess and document third-party risks.

Auditee's Response

EOHHS provided the following response on DTA's behalf.

> *DTA has not operationalized a third-party security policy because EOTSS and EOHHS are both working towards implementation of a third-party security policy. EOHHS has implemented a third-party security management standard in its enterprise standards. . . . EOHHS is working with agencies to operationalize such standards. However, EOTSS has indicated that it will implement contractual standards for managing third parties. Those provisions are still pending.*

Auditor's Reply

OSA acknowledges that EOHHS and EOTSS establish policies that DTA must follow. We encourage DTA to incorporate EOHHS's third-party security management standard as soon as possible in order to sufficiently assess and document third-party risks. We also encourage EOTSS to establish the contractual standards for managing third parties as soon as possible so that all Commonwealth agencies may update their own policies.

1. These reports are generated by external auditors using standards from the American Institute of Certified Public Accountants and provide assurance regarding system and organizational controls.