OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued May 5, 2025

Office of Consumer Affairs and Business Regulation

For the period July 1, 2022 through June 30, 2023

State House Room 230 ■ Boston, MA 02133 ■ auditor@massauditor.gov ■ www.mass.gov/auditor

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

May 5, 2025

Layla R. D'Emilia, Undersecretary
Office of Consumer Affairs and Business Regulation
1 Federal Street, Suite 0720
Boston, MA 02110

Dear Undersecretary D'Emilia:

I am pleased to provide to you the results of the enclosed performance audit of the Office of Consumer Affairs and Business Regulation. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2022 through June 30, 2023. As you know, my audit team discussed the contents of this report with agency managers. This report reflects those comments.

I appreciate you and all your efforts at the Office of Consumer Affairs and Business Regulation. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team has any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

EOTSS	Executive Office of Technology Services and Security
IT	information technology
OCABR	Office of Consumer Affairs and Business Regulation
PII	personally identifiable information
URL	uniform resource locators
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines

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 Consumer Affairs and Business Regulation (OCABR) for the period July 1, 2022 through June 30, 2023.

The purpose of this performance audit was to determine whether OCBAR's website adhered to the accessibility standards established by the Web Content Accessibility Guidelines (WCAG) 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility. Adherence to WCAG ensures that all users, regardless of ability, can access the content and functions of OCABR's website.

Additionally, we determined whether OCABR had an information classification policy, procedures for disposing of information, and a business impact analysis or risk assessment to classify its information systems. We also evaluated whether access to personally identifiable information (PII) was restricted solely to individuals with a legitimate business need. These information technology (IT) governance practices are critical because they form the foundation of a robust security framework, ensuring compliance with data protection regulations and minimizing the risk of unauthorized access or breaches.

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

Finding 1 **Page 16**	OCABR's website was not fully accessible for all Massachusetts residents and users.
Effect	Broken hyperlinks create barriers for users, particularly people with disabilities who rely on accessible navigation features to engage with online content. When users encounter inaccessible or nonfunctioning links, they may struggle to locate critical consumer protection resources, regulatory information, licensing forms, etc. This lack of accessibility not only impacts user experience but also undermines OCABR's ability to provide equitable access and digital inclusiveness. Additionally, nonfunctional links increase the likelihood that Massachusetts residents will either access outdated or incorrect information or be directed to webpages that no longer exist, potentially leading to confusion, misinformation, or missed opportunities to engage with OCABR services. Ensuring that all website components function properly and meet accessibility standards is essential for providing transparent and inclusive government services to all residents.

Recommendations Page 17	1. OCABR should implement a policy to review its webpages periodically for WCAG 2.1 compliance. 2. OCABR should collaborate with Executive Office of Technology Services and Security (EOTSS) to establish a link validation system using automated tools that regularly scan for broken hyperlinks and incorrect redirects. 3. OCABR should collaborate with EOTSS to develop a web maintenance schedule to review and update outdated or incorrect links on a periodic basis (e.g., quarterly or semiannually). 4. OCABR should assign designated staff members to oversee accessibility compliance and website updates.
Finding 2 Page 17	OCABR did not have an information classification policy and did not classify its data.
Effect	Not classifying information (e.g., PII or regulated information) hinders OCABR's ability to establish effective policies and procedures for information management and data protection. Without effective data policies in place, OCABR's sensitive data may be more vulnerable to unauthorized access, theft, or misuse. The lack of effective information classification can lead to other challenges, such as legal liabilities, regulatory violations, and OCABR reputational damage, particularly if personal information or data protected by privacy regulations is compromised. Improper management of data can not only harm OCABR, but it could also lead to increased risk and security vulnerabilities for Massachusetts residents who have used OCABR's services. Additionally, if the subsets of data contained in information systems are not properly classified, then the risk increases that critical systems are left exposed to threats, such as unauthorized use or theft. This can cause OCABR to face challenges in planning for potential threats such as cybersecurity attacks, natural disasters, or fraud.
Recommendations Page 19	1. OCABR management should develop and implement an information classification policy to comply with EOTSS's Asset Management Standard IS.004 and should assign an information custodian in this policy. 2. OCABR should conduct a data inventory and classification assessment of information based on sensitivity, criticality, and regulatory requirements.
Finding 3 Page 19	OCABR did not have procedures for disposing information.
Effect	OCABR migrated its data to the cloud in 2021 and did not assess whether it is storing unnecessary data. Keeping information for longer than necessary also wastes valuable storage space and leads to additional costs for the agency and the Commonwealth, as large quantities of data can be stored longer than needed in the cloud environment at a financial cost to the agency. Not reviewing information at specified intervals and disposing of it when appropriate forces OCABR to keep information for longer than it should, creating additional security risks such as theft, mismanagement, and unauthorized access of data in its custody. Additionally, any Massachusetts residents who use the services OCABR offers are at greater risk of having their data compromised, as their information is retained, and therefore potentially vulnerable, long after they engaged with OCABR.

Recommendation Page 20	1. OCABR should implement policies and procedures for information disposal to ensure that information is properly disposed of in accordance with Commonwealth retention schedules. 2. OCABR should designate an information custodian responsible for ensuring compliance with data disposal policies. 3. OCABR should implement an internal policy which includes the retention schedules and the procedures necessary to dispose of information, in no event before the expiration of its retention period. 4. OCABR should implement a process in which it justifies the business need for archiving information kept past retention schedules.
Finding 4 Page 21	OCABR did not perform a business impact analysis or risk assessment to classify its information systems.
Effect	Without a business impact analysis or risk assessment to classify information systems, OCABR may not assess the criticality of systems based on the sensitivity of the information stored within them. If vital systems are not classified correctly, then they cannot be protected correctly, whether from cybersecurity threats, natural disasters, or fraud. As a result, OCABR could face challenges in planning for these potential disruptions and may not be able to prioritize IT resources effectively in the event of an emergency.
Recommendations Page 22	1. OCABR management should implement a policy to periodically conduct a business impact analysis or risk assessment in order to classify its information systems. 2. OCABR should review these classifications at least annually or anytime a significant system change occurs.
Finding 5 Page 23	OCABR did not ensure that access to PII was limited to approved personnel members who have business needs to access it.
Effect	Granting personnel members access to PII without requiring formal approval of their business need, as well as appropriate training, exposes OCABR to significant risks, such as data breaches. This can lead to identity theft, damaged reputation, or legal liability for OCABR. Each of these risks would have negative impacts on the people whose information is compromised. The introduction of role-based access controls can be used to ensure that users are being assigned permissions based on their roles and business needs instead of individually assigned permissions on a person-by-person basis. In order to implement role-based access, all information must be classified (see finding 2) to determine what information is confidential, such as PII, and should only be accessed by certain approved individuals in pertinent roles. Limiting access to PII helps protect the privacy of Massachusetts residents and reduces the risk that their information may be accessed by someone who may mismanage or steal it.
Recommendations Page 24	1. OCABR should ensure that every user requiring access to PII has their business need reviewed and approved before access is granted. 2. OCABR should implement role-based access. This new process should align with the principle of least privilege, where users should only be given the minimum level of access necessary to perform their job functions. 3. OCABR should review users' access to determine whether these users have the appropriate approval, and OCABR should perform this review on a periodic basis.

OVERVIEW OF AUDITED ENTITY

The Office of Consumer Affairs and Business Regulation (OCABR) is located at 1 Federal Street in Boston and was established by Chapter 24A of the Massachusetts General Laws. OCABR operates under the direction of its secretariat, the Executive Office of Economic Development, and is headed by a director who is appointed by the Governor.

According to its website, OCABR "protects and empowers consumers through advocacy and education, and ensures a fair playing field for the Massachusetts businesses its agencies regulate." Website accessibility is also important to achieving OCABR's mission.

OCABR oversees five regulatory agencies that license various companies and individuals throughout Massachusetts: the Division of Banks, the Division of Insurance, the Division of Occupational Licensure, the Division of Standards, and the Department of Telecommunications and Cable. OCABR also oversees the state's lemon laws[1] and lemon law arbitration[2], data breach reporting, home improvement contractor programs, and the Commonwealth's Do Not Call registry[3]..

OCABR's state appropriations for fiscal years 2022 and 2023 were $1,804,849 and $2,099,525, respectively. OCABR employed 52 personnel during the audit period.

Massachusetts Requirements for Accessible Websites

In 1999, the World Wide Web Consortium (W3C), an international nongovernmental organization responsible for internet standards, published the Web Content Accessibility Guidelines (WCAG) 1.0 to provide guidance on how to make web content more accessible to those with disabilities.

In 2005, the Massachusetts Office of Information Technology,[4] with the participation of state government webpage developers, including developers with disabilities, created the Enterprise Web Accessibility Standards. These standards required all state executive branch agencies to follow the guidelines in Section 508 of the Rehabilitation Act amendments of 1998. These amendments went into effect in 2001 and

1. The Massachusetts Lemon Law protects consumers who have purchased a used or new car that has defects and is unable to be repaired.
2. If a car fits the criteria of the Lemon Law the car buyer can apply for a state run process in which an impartial arbitrator resolves the dispute between the buyer and the seller over the car defects.
3. Massachusetts residents can add their phone number to the Do Not Call Registry through OCABR to help limit phone calls from telemarketers or other telephone solicitors.
4. The Massachusetts Office of Information Technology became the Executive Office of Technology Services and Security in 2017.

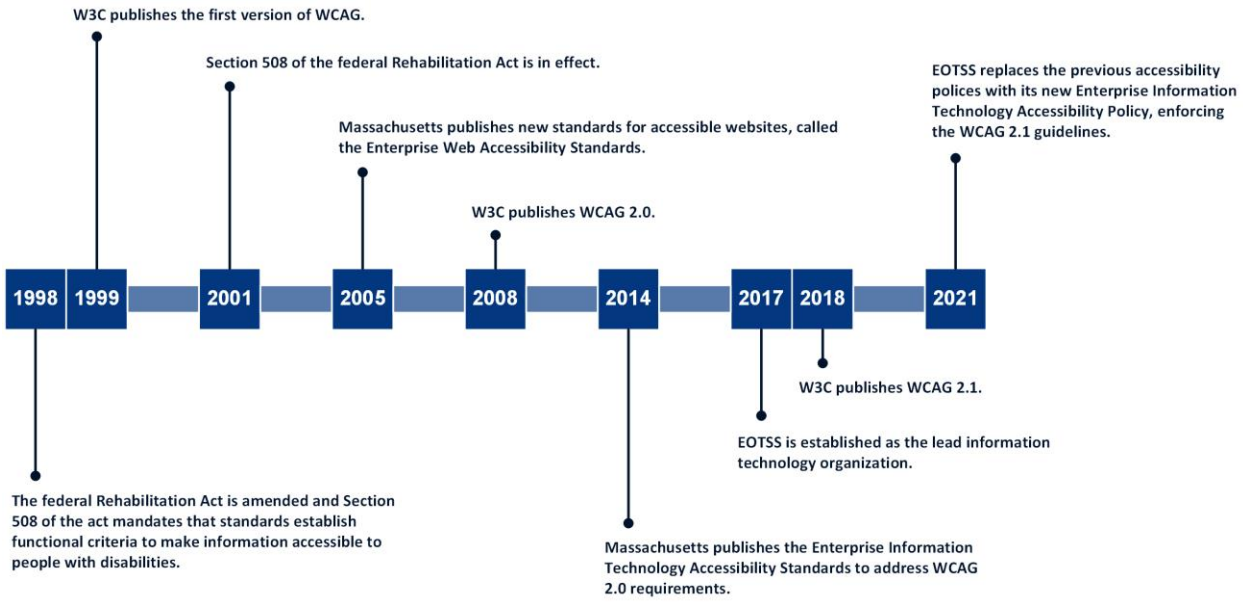
established precise technical requirements to which electronic and information technology (IT) products must adhere. This technology includes, but is not limited to, products such as software, websites, multimedia products, and certain physical products, such as standalone terminals.

In 2008, W3C published WCAG 2.0. In 2014, the Massachusetts Office of Information Technology added a reference to WCAG 2.0 in its Enterprise Information Technology Accessibility Standards.

In 2017, the Executive Office of Technology Services and Security (EOTSS) was designated as the Commonwealth's lead IT organization for the executive branch. EOTSS is responsible for the development and maintenance of the Enterprise Information Technology Accessibility Standards and the implementation of state and federal laws and regulations relating to accessibility. As the principal executive agency responsible for coordinating the Commonwealth's IT accessibility compliance efforts, EOTSS supervises executive branch agencies in their efforts to meet the Commonwealth's technology accessibility requirements.

In 2018, W3C published WCAG 2.1, which built on WCAG 2.0 to improve web accessibility on mobile devices and to further improve web accessibility for people with visual impairments and cognitive disabilities. EOTSS published the Enterprise Information Technology Accessibility Policy in 2021 to meet Levels A and AA of WCAG 2.1.

Timeline of the Adoption of Website Accessibility Standards by the Federal Government and Massachusetts



While EOTSS establishes standards for executive branch agencies, individual agencies, such as OCABR, are responsible for ensuring that their IT solutions and web content fully comply with EOTSS's accessibility standards. When publishing digital content to Mass.gov or other platforms, state agencies must comply with EOTSS's Web Design Guidelines, which were published in 2020 based on the federal 21st Century Integrated Digital Experience Act. EOTSS's Web Design Guidelines help state government agencies evaluate their design and implementation decisions in meeting state accessibility requirements.

Web Accessibility

Government websites are an important way for the general public to access government information and services. Deloitte's[5] 2023 Digital Citizen Survey found that 55% of respondents preferred to interact with their state government services through a website instead of face-to-face interaction or a call center. Commonwealth of Massachusetts websites have millions of webpage views each month.

However, people do not interact with the internet uniformly. The federal government and nongovernmental organizations have established web accessibility standards intended to make websites more accessible to people with disabilities such as visual impairments, hearing impairments, and others. The impact of these standards can be significant, as the federal Centers for Disease Control and Prevention estimates that 1,348,913 adults (23% of the adult population) in Massachusetts have a disability, as of 2021.

How People with Disabilities Use the Web

According to W3C, people with disabilities use assistive technologies and adaptive strategies specific to their needs to navigate web content. Examples of assistive technologies include screen readers, which read webpages aloud for people who cannot read text; screen magnifiers for individuals with low vision; and voice recognition software for people who cannot (or do not) use a keyboard or mouse. Adaptive strategies refer to techniques that people with disabilities employ to enhance their web interaction.[6] These strategies might involve increasing text size, adjusting mouse speed, or enabling captions.

To make web content accessible to people with disabilities, developers must ensure that various components of web development and interaction work together. This includes text, images, and structural code; users' browsers and media players; and various assistive technologies.

5. Deloitte is an international company that provides tax, accounting, and audit services to businesses and government agencies.
6. Web interaction refers to the various actions that users take while navigating and using the internet. It encompasses a wide range of online activities, including, but not limited to, clicking on links, submitting forms, posting comments on webpages, and engaging with web content and services in other forms.

Accessibility Features of a Website

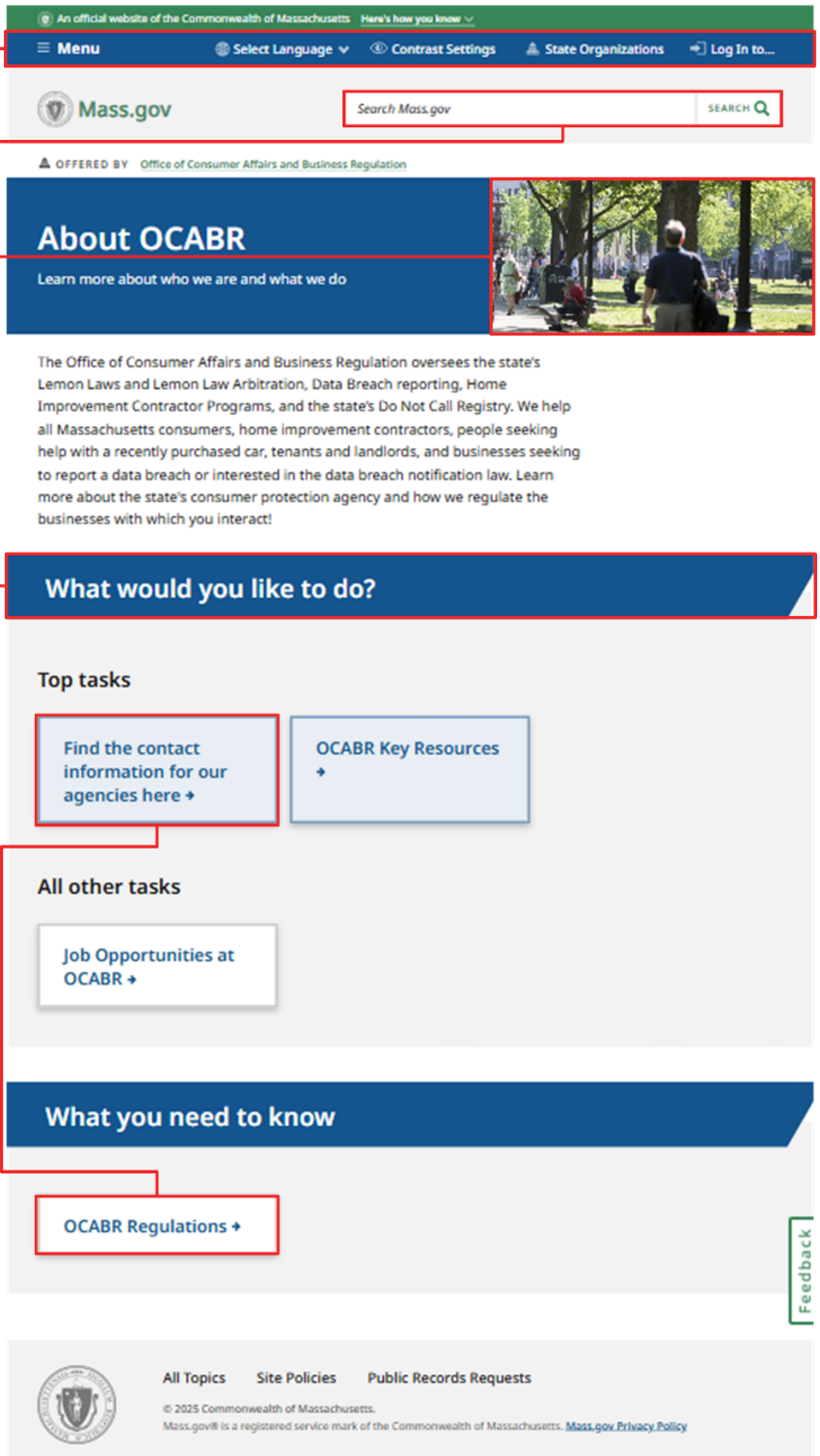
A site's header can appear throughout an entire site and contain links to main content areas

Alternative text should provide a description of an image so screen readers can describe the image

By properly labeling fields where text can be entered, screen readers will read aloud the type of information that a user should enter.

Headings organize web content in a logical manner and allow users to navigate content easily.

Screen reader users and persons with motor disabilities rely in part on the Tab key to navigate between major portions of the website's content.



IT Governance

IT governance refers to the processes that state agencies use to manage their IT resources. EOTSS documents these processes in standards that executive branch state agencies are required to follow. Specifically, Section 2 of Chapter 7D of the General Laws states,

> *Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology.*

IT governance processes include information classification, information disposal, information system classification, and the restriction of information access.

Information Classification Policy

EOTSS Asset Management Standard IS.004[7] requires that state agencies establish classification or sensitivity levels for all of the information in their custody. These classification levels are meant to ensure that information is protected in line with its value. EOTSS's Asset Management Standard IS.004 lists three levels of classification: public, internal use, and confidential.

The public classification involves information that is viewed by the public (e.g., press releases, information on public-facing websites, or advertising for services). The internal use classification involves information that does not reach the level of confidential but should not be viewed by the public (e.g., internal training materials or policies). The confidential classification is the highest level and involves information that should only be accessed by personnel members who need the information to perform their job duties (e.g., personnel performance documentation, personally identifiable information (PII), federal tax information, or passwords). Confidential information is sensitive by nature and could cause damage to the Commonwealth and its residents if it is compromised.

Information Disposal Procedures

EOTSS Asset Management Standard IS.004 requires that all executive branch state agencies establish information disposal procedures for information in their custody. Section 6.4.2.4 of this standard states that each agency must "Identify and securely delete stored information that exceeds defined retention periods on a quarterly basis." Information disposal reduces the risk of data becoming compromised by

7. The title of EOTSS's Asset Management Standard IS.004 was changed in 2025 to Asset Management Standard IS.015.

limiting the amount of data that could potentially be stolen. Additionally, specific types of information (e.g., tax data) are subject to state retention schedules with which agency policymakers must comply.

Information System Classification

EOTSS Asset Management Standard IS.004 requires that all executive branch state agencies perform a business impact analysis[8] or risk assessment[9] in order to classify their information systems. Classifying information systems promotes a consistent approach to risk management and disaster recovery. Information systems classifications are separated into the following four levels:

- low: public information;
- medium: internal use information;
- high: confidential information or business support systems (e.g., email); and
- critical: information with regulatory requirements (e.g., information involving the Health Insurance Portability and Accountability Act or federal taxes).

Information systems contain diverse arrays of data, all of which should be classified in order to better protect the data within. If an information system is not properly classified, the data within can become vulnerable.

Restricting Access to PII

EOTSS Asset Management Standard IS.004 requires that all executive branch state agencies restrict access to confidential information to a narrow subset of personnel members who have a business need to access said information. Specifically, this policy lists PII as confidential information that an agency may have in its custody. Limiting access to PII prevents it from being used in a way that could cause harm to the Commonwealth and its residents, business partners, and customers.

8. In its Glossary of Terms IS.Glossary, EOTSS defines a business impact analysis as "a review that predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies."
9. In its "Special Publication 800-30—Guide for Conducting Risk Assessments," the National Institute of Standards and Technology defines a risk assessment as "the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information 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 Office of Consumer Affairs and Business Regulation (OCABR) for the period July 1, 2022 through June 30, 2023.

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. Was OCABR's website in compliance with the Executive Office of Technology Services and Security's (EOTSS's) Enterprise Information Technology Accessibility Policy and the World Wide Web Consortium's (W3C's) Web Content Accessibility Guidelines (WCAG) 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility?	**No; see Finding 1**
2. Did OCABR do the following to implement certain information technology (IT) governance policies: a. establish classification or sensitivity levels of all information of which it had custody in accordance with Section 6.2. of EOTSS's Asset Management Standard IS.004; b. identify and securely delete stored information that exceeded defined retention periods on a quarterly basis in accordance with Section 6.4.2.4. of EOTSS's Asset Management Standard IS.004; and c. conduct a business impact analysis or risk assessment to determine the classification level of information systems in accordance with Section 6.6.2. of EOTSS's Asset Management Standard IS.004?	**No; see Findings 2, 3, and 4**
3. Did OCABR restrict access to personally identifiable information (PII) to a narrow subset of personnel members who had a business need to access the information in accordance with Section 6.2.1. of EOTSS's Asset Management Standard IS.004?	**No; see Finding 5**

To accomplish our audit objectives, we gained an understanding of the aspects of OCABR's internal control environment relevant to our objectives by reviewing applicable policies and procedures and by

interviewing OCABR staff members and management. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

Website Accessibility Testing

To determine whether OCABR's website was in compliance with EOTSS's Enterprise Information Technology Accessibility Policy and W3C's WCAG 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility, we took the actions described below.

We selected a random, nonstatistical sample of 60 OCABR webpages out of a population of 783 OCABR webpages. We performed the procedures described below on the sampled webpages.

User Accessibility

- We determined whether content on the website was able to be viewed in both portrait and landscape modes.
- We determined whether content on the webpage was undamaged and remained readable when zoomed to 200% and 400%.

Keyboard Accessibility

- We determined whether all elements[10] of the webpage could be navigated using only a keyboard.
- We determined whether any elements on the webpage prevented a user from moving to a different element when using only a keyboard to navigate the webpage.
- We determined whether the first focusable control[11] is a hyperlink that redirects to the main content of the website. The first focusable control is known as either a bypass block or a skip link.

Navigation Accessibility

- We determined whether the website contained a title that was relevant to website content.
- We determined whether there was a search function present to help users locate content.
- We determined whether related hyperlinks allowed navigation to the intended webpage.

10. An element is a part of a webpage that contains data, text, or an image.
11. The first focusable control is the first element a user will be brought to on a webpage when navigating with a keyboard.

- We determined whether headings within websites related to the content of the header's section.

Language

- We determined whether video content found within the website had all important sounds and dialogue captioned.
- We determined whether the language of the webpage was tagged with the correct language attribute.[12]
- We determined whether words that appeared on the webpage matched the language to which the webpage was set.

Error Identification

- We determined whether mandatory form fields alerted users if the field was left blank.
- We determined whether there was a label for elements that required user input.
- We determined whether the label was programmed correctly.
- We determined whether there were examples given to assist the user in correcting mistakes (for example, a warning when entering a letter in a field meant for numbers).

Color Accessibility

- We determined whether there was at least a 3:1 contrast in color and additional visual cues to distinguish hyperlinks, which WCAG recommends for users with colorblindness or other visual impairments.

Out of the 60 webpages we selected in our sample, 18 had been removed from OCABR's website by the time we began our testing. OCABR management informed us these 18 webpages were for events that had already occurred, which is why they removed the webpages.

See Finding 1 regarding hyperlinks on OCABR's website.

IT Governance Testing

We took the following actions to determine whether OCABR established IT governance policies and procedures over the areas listed below.

12. A language tag identifies the native language of the content on the webpage or PDF (e.g., a webpage in English should have an EN language tag). The language tag is listed in the webpage's or PDF's properties. This, among other things, is used to help screen readers use the correct pronunciation for words.

Information Classification Policy

To determine whether OCABR's information classification policy met the requirements of Section 6.2 of EOTSS's Asset Management Standard IS.004, we interviewed knowledgeable OCABR staff members and requested OCABR's information classification policy. We learned that OCABR did not have an information classification policy in place during the audit period.

See Finding 2 regarding OCABR's information classification policy.

Information Disposal Plan and Procedures

To determine whether OCABR's information disposal procedures met the requirements of Section 6.4.2.4 of EOTSS's Asset Management Standard IS.004, we interviewed knowledgeable OCABR staff members and requested OCABR's information disposal plan and procedures. We were informed that OCABR had not established a procedure for disposing of stored information that exceeds defined retention periods during the audit period.

See Finding 3 regarding OCABR's information disposal procedures.

Business Impact Analysis or Risk Assessment to Determine Information System Classification

To determine whether OCABR conducted a business impact analysis or risk assessment in accordance with Section 6.6.2 of EOTSS's Asset Management Standard IS.004, we interviewed knowledgeable OCABR staff members and requested OCABR's business impact analysis or risk assessment used to determine the classification levels of its information systems. We were informed that OCABR did not conduct a business impact analysis or risk assessment to determine the classification levels of its information systems.

See Finding 4 regarding OCABR's business impact analysis and/or risk assessment.

Restricted Access to PII

To determine whether OCABR restricted access to PII to the narrow subset of personnel members who had a business need to access the information in accordance with Section 6.2.1. of EOTSS's Asset Management Standard IS.004, we took the actions described below. We requested that knowledgeable OCABR staff members identify personnel members on the OCABR employee list who had access to PII.

Then, we selected a random, nonstatistical sample of 20 employees out of a population of 52 employees who had access to PII. For each employee in our sample, we then inspected IT tickets and emails to determine whether these personnel members were granted the approvals needed before gaining access to PII.

See Finding 5 regarding OCABR's authorization process for access to PII.

Due to the small testing populations, we used nonstatistical sampling methods for testing and therefore did not project the results of our testing to any population.

Data Reliability Assessment

Web Accessibility

To determine the reliability of the site map spreadsheet we received from OCABR management, we interviewed knowledgeable OCABR staff members and checked that variable formats (e.g., dates, unique identifiers, or abbreviations) were accurate. Additionally, we ensured that there was no abbreviation of data fields, no missing data (e.g., hidden rows or columns, blank cells, or absent records), no duplicate records, and that all values in the dataset corresponded with expected values.

We selected a random sample of 20 uniform resource locators (URLs)[13] that could be accessed independently from the OCABR site map and traced each to the corresponding webpage, checking that each URL and webpage title matched the information on the OCABR website. We also selected a random sample of 20 URLs from OCABR's website and traced each URL and webpage title to the site map to ensure that there was a complete and accurate population of URLs on the site map.

IT Governance

To determine the reliability of the employee list we received from OCABR management, we interviewed OCABR management and knowledgeable OCABR staff members and checked that variable formats (e.g., dates, unique identifiers, or abbreviations) were accurate. Additionally, we ensured that there was no abbreviation of data fields, no missing data (e.g., hidden rows or columns, blank cells, or absent records), no duplicate records, and that all values in the dataset corresponded with expected values.

13. A URL uniquely identifies an internet resource, such as a website.

We selected a random sample of 10 employees from the employee list and traced their names to CTHRU, the Commonwealth's statewide payroll open records system, to verify the list's accuracy. We also selected a random sample of 10 employees from CTHRU and traced their names back to the employee list provided by OCABR to ensure that we received a complete and accurate employee list.

Based on the results of the data reliability assessment procedures described above, we determined that the site map and the employee list we obtained during the course of our audit were sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Office of Consumer Affairs and Business Regulation's website was not fully accessible for all Massachusetts residents and users.

The Office of Consumer Affairs and Business Regulation's (OCABR's) website was not fully accessible. We determined that 15 webpages out of a sample of 60 OCABR webpages were not accessible in accordance with Web Content Accessibility Guidelines (WCAG) 2.1 for navigation accessibility. Of these, we determined that all 15 webpages contained hyperlinks that did not allow the user to navigate to intended webpages.

Broken hyperlinks create barriers for users, particularly people with disabilities who rely on accessible navigation features to engage with online content. When users encounter inaccessible or nonfunctioning links, they may struggle to locate critical consumer protection resources, regulatory information, licensing forms, etc. This lack of accessibility not only impacts user experience but also undermines OCABR's ability to provide equitable access and digital inclusiveness.

Additionally, nonfunctional links increase the likelihood that Massachusetts residents will either access outdated or incorrect information or be directed to webpages that no longer exist, potentially leading to confusion, misinformation, or missed opportunities to engage with OCABR services. Ensuring that all website components function properly and meet accessibility standards is essential for providing transparent and inclusive government services to all residents.

Authoritative Guidance

WCAG 2.1 states,

> *[Success Criterion] 2.4.5: Multiple Ways (Level AA) . . .*
>
> *More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process.*

Reasons for Issue

OCABR management informed us that the broken hyperlinks were the result of (1) the uniform resource locators (URLs) being updated by outside organizations without any redirects and (2) links leading to webpages that had been unpublished due to outdated information.

Recommendations

1. OCABR should implement a policy to review its webpages periodically for WCAG 2.1 compliance.
2. OCABR should collaborate with the Executive Office of Technology Services and Security (EOTSS) to establish a link validation system using automated tools that regularly scan for broken hyperlinks and incorrect redirects.
3. OCABR should collaborate with EOTSS to develop a web maintenance schedule to review and update outdated or incorrect links on a periodic basis (e.g., quarterly or semiannually).
4. OCABR should assign designated staff members to oversee accessibility compliance and website updates.

Auditee's Response

OCABR implemented an Enterprise Information Technology Accessibility Policy after the audit period and effective March 27, 2025, requiring quarterly accessibility reviews.

OCABR communications and [Executive Office of Economic Development (EOED) information technology (IT)] staff have and will continue to coordinate with EOTSS, including using EOTSS' SiteImprove Reports and related dashboard. SiteImprove assists with accessibility monitoring of OCABR pages by identifying broken links and other accessibility and user experience issues. OCABR communications and EOED IT staff review these reports, and address issues accordingly. OCABR has proactively and periodically checked the accessibility ratings directly in the SiteImprove platform to determine where improvements can be made. Site improvements are reflected in a dashboard. For example, OCABR's accessibility score on 11/18/24 was 78.1% and has improved to 90.7% as of 3/27/25, with one broken link flagged in the system and 7 to review.

OCABR is also actively working on improving content for accessibility, including rewriting pages for plain language, adding alt text to images, and implementing accessibility improvements available through EOTSS mass.gov authoring tools. Important content is being rewritten and placed directly on public-facing web pages so that information is more inclusive. OCABR communications director has served in this role since December 2023 and has attended EOTSS accessibility training for web pages, documents, presentations, and other content. Further, EOED IT staff is working in coordination with EOTSS to hire an Accessibility Officer.

Auditor's Reply

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

2. The Office of Consumer Affairs and Business Regulation did not have an information classification policy and did not classify its data.

OCABR revealed to us in interviews that it did not have an information classification policy and did not establish classification levels for its information assets (i.e., public, internal use, and confidential), leaving sensitive data without a clear framework for protection and management.

Not classifying information (e.g., personally identifiable information [PII] or regulated information) hinders OCABR's ability to establish effective policies and procedures for information management and data protection. Without effective data policies in place, OCABR's sensitive data may be more vulnerable to unauthorized access, theft, or misuse.

The lack of effective information classification can lead to other challenges, such as legal liabilities, regulatory violations, and OCABR reputational damage, particularly if personal information or data protected by privacy regulations are compromised. Improper management of data can not only harm OCABR, but it could also lead to increased risk and security vulnerabilities for Massachusetts residents who have used OCABR's services.

Additionally, if the subsets of data contained in information systems are not properly classified, then the risk increases that critical systems are left exposed to threats, such as unauthorized use or theft. This can cause OCABR to face challenges in planning for potential threats such as cybersecurity attacks, natural disasters, or fraud.

Authoritative Guidance

EOTSS's Asset Management Standard IS.004 states,

> *6.2. Information Classification*
>
> *The classification or sensitivity level of all information must be established to ensure that appropriate measures are taken to protect the information commensurate with its value to the organization and the legal restrictions on its dissemination.*

Reasons for Issue

OCABR management informed us that they used an application rating system for the initial inventory of information systems, with the later goal of producing a detailed inventory of data that included information classification and sensitivity levels. This goal was not met because Executive Office of Economic Development information technology (IT) staff members transitioned to EOTSS in 2023. This created a vacuum for resources and many competing priorities.

Recommendations

1. OCABR management should develop and implement an information classification policy to comply with EOTSS's Asset Management Standard IS.004 and should assign an information custodian[14] in this policy.

2. OCABR should conduct a data inventory and classification assessment of information based on sensitivity, criticality, and regulatory requirements.

Auditee's Response

OCABR developed a written Information Asset Policy after the audit period and effective October 2024.

OCABR's written Information Asset Policy identifies the classification levels to be used for stored information (restricted, confidential, internal use, and public), the responsible person for recommending classification levels (the Information Owner who is the business owner for each OCABR unit), and the role of the Information Custodian (the General Counsel) in working with the Information Owners both to set and to update classification levels on a periodic basis. In particular, OCABR only posts information on its website classified as public, and semi-annual reviews are conducted to consider existing classification levels for information.

Auditor's Reply

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

3. The Office of Consumer Affairs and Business Regulation did not have procedures for disposing information.

OCABR management revealed to us in interviews that they did not have procedures for information disposal and that they did not identify and dispose of information that exceeded retention periods on a quarterly basis in accordance with Section 6.4.2.4 of EOTSS's Asset Management Standard IS.004.

OCABR migrated its data to the cloud in 2021 and did not assess whether it is storing unnecessary data. Keeping information for longer than necessary also wastes valuable storage space and leads to additional costs for the agency and the Commonwealth, as large quantities of data can be stored longer than needed in the cloud environment at a financial cost to the agency. Not reviewing information at specified intervals and disposing of it when appropriate forces OCABR to keep information for longer than it should, creating additional security risks such as theft, mismanagement, and unauthorized access of data in its custody. Additionally, any Massachusetts residents who use the services OCABR offers are at greater risk of having

14. Information custodians are responsible for assigning appropriate classification levels to information in their custody.

their data compromised, as their information is retained, and therefore potentially vulnerable, long after they engaged with OCABR.

Authoritative Guidance

EOTSS's Asset Management Standard IS.004 states,

> *6.4.2.4 Identify and securely delete stored information that exceeds defined retention periods on a quarterly basis.*

The *Massachusetts Statewide Records Retention Schedule* states,

> *B06-26: Data Breach Records*
>
> *Retain 6 years.*
>
> *Documents data breach notifications sent to the Attorney General as required by statute. Includes data breach notifications directed to the Attorney General and copies of data breach notifications directed to the Office of Consumer Affairs and Business Regulation, copies or samples of data breach notifications directed to Massachusetts consumers, copies of Written Information Security Programs, implemented pursuant to [Section 17.03 of Title 201 of the Code of Massachusetts Regulations], and related correspondence. Also documents civil and criminal investigations of data breaches pursuant to [Chapter 93H and Chapter 93A of the Massachusetts General Laws], including complaints, investigative notes and reports, civil investigative demands, substantive support materials, and related correspondence.*

Reasons for Issue

OCABR management stated that the absence of procedures was due to a lack of resources caused by the transition of the Executive Office of Economic Development's IT employees to EOTSS over the last two years. This transition left areas like information disposal without dedicated resources or attention. OCABR management stated that their new "Information Asset Policy" will establish new operational procedures to comply with the EOTSS policy. Additionally, the Executive Office of Economic Development's new chief information security officer, who joined the agency in October 2024, has identified the need to focus attention on security areas, including information asset inventory, disposal, and control.

Recommendations

1. OCABR should implement policies and procedures for information disposal to ensure that information is properly disposed of in accordance with Commonwealth retention schedules.

2. OCABR should designate an information custodian responsible for ensuring compliance with data disposal policies.

3. OCABR should implement an internal policy which includes the retention schedules and the procedures necessary to dispose of information, in no event before the expiration of its retention period.

4. OCABR should implement a process in which it justifies the business need for archiving information kept past retention schedules.

Auditee's Response

OCABR developed a written OCABR Record Retention Schedule after the audit period and effective October 2024 and designated its General Counsel as Information Custodian. The policy requires OCABR's Information Custodian/General Counsel to submit requests to the Record Conservation Board ("RCB") for the disposal of hard copy information that is past the designated record retention schedule.

This written policy details that OCABR must log the disposal of restricted and/or confidential information to maintain an audit trail; verify that the information assets containing any restricted and/or confidential information have been removed or securely overwritten prior to disposal or reuse; render media unusable (e.g., degaussing), unreadable or indecipherable prior to disposal; use acceptable industry best practices and standards for information erasure to ensure information is unrecoverable; use a third-party service that specializes in information or media disposal; identify and securely delete stored information that exceeds defined retention periods on a quarterly basis (such information shall be identified by each Information Owner who provides said information to the General Counsel who, in turn, shall send a request to the RCB for destruction permission); ensure that hard copies of information will only be generated when necessary; obtain a disposal certificate or other written attestation from the third-party confirming proper disposal; and, identify any business needs for archiving information kept past retention schedules.

In addition, OCABR works with [Executive Office of Economic Development] IT and partners to delete electronic information on a quarterly basis.

Auditor's Reply

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

4. The Office of Consumer Affairs and Business Regulation did not perform a business impact analysis or risk assessment to classify its information systems.

OCABR management revealed to us in interviews that they did not perform a business impact analysis or risk assessment to classify their information systems. Information systems should be classified as low, medium, high, or critical, depending on the use of the system and the information it contains.

Without a business impact analysis or risk assessment to classify information systems, OCABR may not assess the criticality of systems based on the sensitivity of the information stored within them. If vital systems are not classified correctly, then they cannot be protected correctly, whether from cybersecurity threats, natural disasters, or fraud. As a result, OCABR could face challenges in planning for these potential disruptions and may not be able to prioritize IT resources effectively in the event of an emergency.

Authoritative Guidance

EOTSS's Asset Management Standard IS.004 states,

> *6.6.2 Commonwealth Agencies and Offices must conduct a business impact analysis or a risk assessment to determine information system classifications for their information assets.*

Reasons for Issue

OCABR management stated that during the last two years, they went through a transition period where IT personnel members from the Executive Office of Economic Development transitioned to EOTSS, leaving OCABR without proper IT staffing. During this time, the Executive Office of Economic Development began using a system for an initial inventory and creating macro-level risk classifications for over 90 applications used by the Executive Office of Economic Development, including OCABR's applications. Although the majority of information was deemed accurate by the OCABR team, OCABR has found some inaccuracies which require detailed reviews and updates. OCABR management expects the aforementioned review to be completed by the end of the first quarter of 2025, after which a deeper-level risk assessment and business impact analysis will be conducted.

Recommendations

1. OCABR management should implement a policy to periodically conduct a business impact analysis or risk assessment in order to classify its information systems.
2. OCABR should review these classifications at least annually or anytime a significant system change occurs.

Auditee's Response

> *During and following the audit period, [Executive Office of Economic Development (EOED)] IT implemented an initial macro-level risk classification of over 90 applications using the Application Inventory Rating System (AIRS), including OCABR applications. While this first iteration provided a high-level view of business risk, these metrics represent an overall assessment and do not fully capture the nuanced operational and data sensitivity aspects of each application. A more comprehensive and detailed iteration is currently underway.*

EOED IT recently onboarded a Salesforce developer who is helping to enhance AIRS, including the addition of key fields and refined calculation logic to enable more granular and policy-aligned classification of applications. This effort will better reflect the business impact and data sensitivity of each application, supporting more accurate prioritization and risk mitigation strategies.

OCABR is working to validate and update existing records and expects EOED's enhanced AIRS-based risk classification framework to be in place by the end of [quarter] 3 2025. Following this, formal business impact analyses and deeper-level risk assessments will be conducted on a rolling basis for OCABR applications, in alignment with IS.004 and IS.010 requirements.

A policy for periodic reassessment—at least annually or in response to significant changes—will be formalized to maintain compliance and ensure adaptive risk management.

Auditor's Reply

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

5. The Office of Consumer Affairs and Business Regulation did not ensure that access to personally identifiable information was limited to approved personnel members who have business needs to access it.

OCABR did not ensure that access to PII was limited to personnel members with business needs to access it. Specifically, 11 out of 20 personnel members sampled did not have an approved user access request before being granted access to PII.

Granting personnel members access to PII without requiring formal approval of their business need, as well as appropriate training, exposes OCABR to significant risks, such as data breaches. This can lead to identity theft, damaged reputation, or legal liability for OCABR. Each of these risks would have negative impacts on the people whose information is compromised.

The introduction of role-based access controls can be used to ensure that users are being assigned permissions based on their roles and business needs instead of individually assigned permissions on a person-by-person basis. In order to implement role-based access, all information must be classified (see finding 2) to determine what information is confidential, such as PII, and should only be accessed by certain approved individuals in pertinent roles.

Limiting access to PII helps protect the privacy of Massachusetts residents and reduces the risk that their information may be accessed by someone who may mismanage or steal it.

Authoritative Guidance

EOTSS's Asset Management Standard IS.004 states,

> *6.2.1. Confidential—organization or customer information that if inappropriately accessed or disclosed could cause adverse financial, legal, regulatory, or reputational damage to the Commonwealth, its constituents, customers, and business partners. . . .*
>
> *Except as required by law, confidential information must be access-restricted to a narrow subset of personnel who have a business need to access the information. Examples may include but are not limited to:*
>
> *6.2.1.1. Personally identifiable information (PII).*

Reasons for Issue

OCABR management stated that newly hired personnel members are granted specific role-based access control assignments, which may include authorization for the specific user to access PII if they have a business need to do so. Often this is modeled on existing staff members who, due to their job responsibilities, have access to PII. Currently, these records are documented using the EOTSS-provided IT ticketing system, ServiceNow. Before the implementation of this system, requests could be made and approved via email, in-person conversations, or phone calls.

A list of security groups in Active Directory (a service that IT administrators use to store and manage information on a network about users and devices, such as access permissions) is used to manage systems and data access. Currently, access requests are managed through ServiceNow. Requests for access are routed through the appropriate information technology liaison and designated security officer for review and approval. However, requests before 2023 were not as well documented and some were fulfilled through email requests.

Recommendations

1. OCABR should ensure that every user requiring access to PII has their business need reviewed and approved before access is granted.
2. OCABR should implement role-based access. This new process should align with the principle of least privilege, where users should only be given the minimum level of access necessary to perform their job functions.
3. OCABR should review users' access to determine whether these users have the appropriate approval, and OCABR should perform this review on a periodic basis.

Auditee's Response

Prior to full implementation of the ServiceNow system in 2023, access to PII was provided in several controlled ways that did not consistently document approval, including verbal or e-mail requests from appropriate leadership. Approval and access were controlled in the following ways:

1. *Initial Onboarding: New-hire requests specify Role-Based Access Control (RBAC) Assignments, access authorization for the specific user to access PII as part of their job function. Often this is modeled on existing staff who, due to their job responsibilities, have access to PII. These records are formal using the ServiceNow ticketing system, however, prior to the implementation of this system, much of the requests were made and approved via email or by audio discussion.*

2. *Acceptable Use Policy: New hires are required to acknowledge the Acceptable Use Policy as part of the on-boarding process, and annual security training requirements. This is a key explanation and acceptance of working with PII. These records are retained in our training system (Mass Achieve, Cornerstone) however, these records do not go back further than 2022.*

3. *Security Group Management: This management reflects role-based access. An extensive list of security groups (SG) in Active Directory (MS Azure Entra) is tied to roles and departments and utilized to manage systems and data access. Today, access requests are managed via ServiceNow.*

   Requests for access are routed through the appropriate Information Technology Liaison (ITL) and Designated Security Officer (DSO) for review and approval.

4. *[Executive Office of Economic Development (EOED)] and Sub-division Training: EOED has hired a dedicated [chief information security officer] who started in October 2024. In addition, there is a new on-boarding security training, providing new team members an understanding of desired behaviors and security best practices with PII. This new training will be added to the annual security re-training requirement. Additionally, subdivisions are conducting their own awareness training on the location, and authorized access to PII.*

OCABR and EOED IT incorporate the ServiceNow system to document access requests and are implementing more stringent controls to ensure PII access is properly authorized to minimum levels, monitored, and periodically reviewed.

OCABR is also taking the following actions:

- *Historical Remediation: A retrospective access review of PII-related security groups in Active Directory is underway. Any users without documented business justification will have access reevaluated or revoked where appropriate. We expect to have this completed by end of Q3 2025.*

- *Role-Based Access Controls: EOED is developing role-based access controls (RBAC) for OCABR applications and Active Directory groups. Roles are being defined based on job functions, and access rights will be aligned to these roles under the principle of least privilege. This work is dependent on the application, and those which do not have this capability to use RBAC and/or AD, are being further evaluated for modernization. A*

report on which applications are compliant and which require modernization will be completed by end of Q3 2025.

- *Periodic Reviews: OCABR is implementing a quarterly access review process to ensure all PII access remains appropriate, with reports generated from Active Directory and ServiceNow where possible.*

- *Access Training Requirements: The onboarding process for PII access will now include verification of required privacy and security training, in accordance with Acceptable Use and Security Awareness policies.*

Auditor's Reply

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