OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued March 19, 2024

Division of Standards

For the period July 1, 2021 through December 31, 2022

OFFICE OF THE STATE AUDITOR
DIANA DIZOGLIO

March 19, 2024

James P. Cassidy, Director
Division of Standards
1000 Washington Street, Suite 510
Boston, MA 02118

Dear Mr. Cassidy:

I am pleased to provide to you the results of the enclosed performance audit of the Division of Standards. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2021 through December 31, 2022. 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 Division of Standards. 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 have any questions.

Best regards,

Diana DiZoglio

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DOS	Division of Standards
EOTSS	Executive Office of Technology Services and Security
IT	information technology
URL	uniform resource locator
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 Division of Standards (DOS) for the period July 1, 2021 through December 31, 2022. In this performance audit, we determined the following:

- whether DOS's website met the accessibility standards established by the Executive Office of Technology Services and Security (EOTSS) and the Web Content Accessibility Guidelines 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language accessibility, error identification, and color accessibility and
- whether DOS established information technology (IT) governance policies and procedures that met the requirements of EOTSS's Enterprise Information Security Policies and Standards for business continuity plans, disaster recovery plans, information security incident response plans and procedures, and cybersecurity awareness training.

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

Finding 1 **Page 14**	DOS's website is not fully accessible for all Massachusetts residents.
Recommendation **Page 15**	DOS should review its webpages to ensure that all hyperlinks lead to related information to provide equitable access to critical information and services offered online by DOS to all Commonwealth residents.
Finding 2 **Page 15**	DOS's business continuity plan does not include all required elements, and it does not have a disaster recovery plan.
Recommendations **Page 17**	1. DOS should update its business continuity plan to include all required elements. It should also update the plan annually and whenever a major organizational change occurs. 2. DOS should develop and implement a disaster recovery plan.
Finding 3 **Page 18**	DOS relies on an information security incident response plan and procedures that do not include all required elements.
Recommendation **Page 19**	DOS should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DOS could establish a supplemental information security incident response plan and procedures that include guidance for implementing corrective action or post-incident analysis, criteria for business recovery, data backup processes, and an analysis of legal requirements for reporting IT system compromises.

OVERVIEW OF AUDITED ENTITY

In 1996, Section 5 of Chapter 24 of the Massachusetts General Laws established the Division of Standards (DOS). DOS is a regulatory agency within the Office of Consumer Affairs and Business Regulation that falls under the Executive Office of Economic Development (formerly the Executive Office of Housing and Economic Development). DOS's main function is to ensure the accuracy of weight and measuring systems in commercial settings (e.g., gasoline pumps). This function dates back to 1637 when colonists would bring weights for their scales to the local constable to be checked for accuracy.

DOS enforces accuracy standards for weighing and measuring devices used in the sale of items such as food and fuel. Additionally, according to its website,

> *DOS regulates the sale of gasoline and sets standards for lubricating oils and antifreeze, including the inspection of all fuel dispensing equipment for required markings pertaining to grade and brand. The Division also tests and approves coin operated devices, licenses auctioneers, [seasonal or temporary vendors], promoters, peddlers, motor fuel and oil retailers and registers auto damage repair shops, and enforces the item pricing law, unit pricing regulations and item pricing waivers to retail food stores.*

To fulfill its responsibilities, DOS has promulgated regulations under Title 202 of the Code of Massachusetts Regulations.

DOS had 21 employees as of December 31, 2022 and is at 1000 Washington Street, Suite 510, in Boston. DOS's state appropriation for fiscal year 2022 was $2,770,900.

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 people with disabilities.

In 2005, the Massachusetts Office of Information Technology,[1] 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 Office of Information Technology became the Executive Office of Technology Services and Security in 2017 following Executive Order 588 from then Governor Charles Baker.

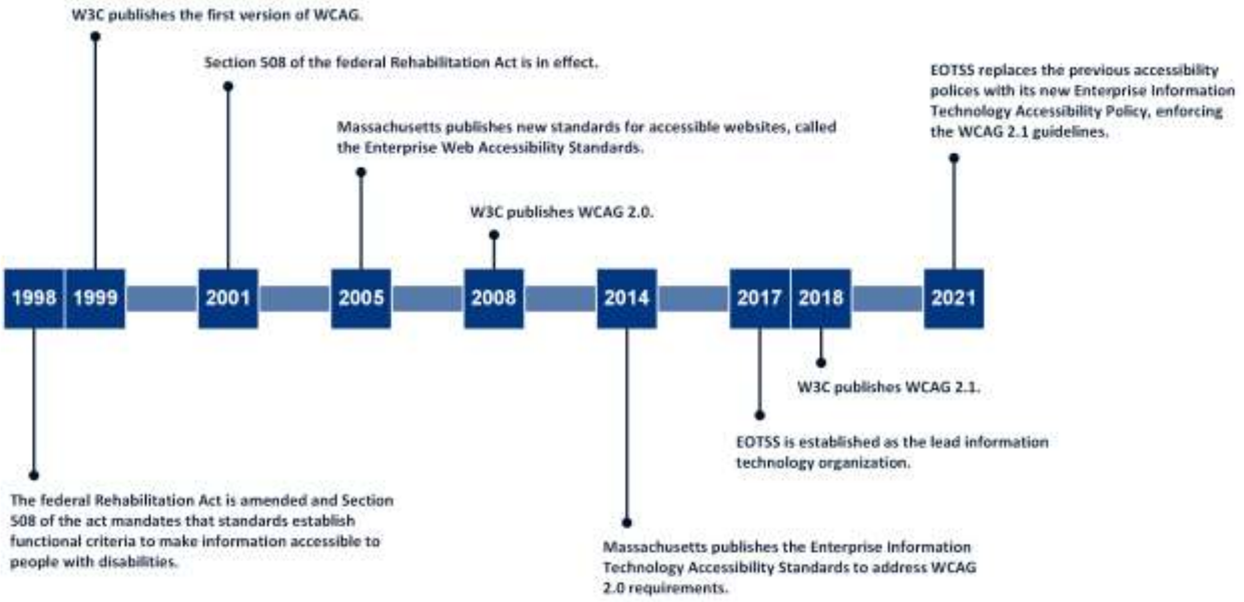
established precise technical requirements to which electronic and information technology (IT) products must adhere. This technology includes, but is not limited to, products such as software, websites, multimedia products, and certain physical products, such as standalone terminals.

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 accessibility requirements.

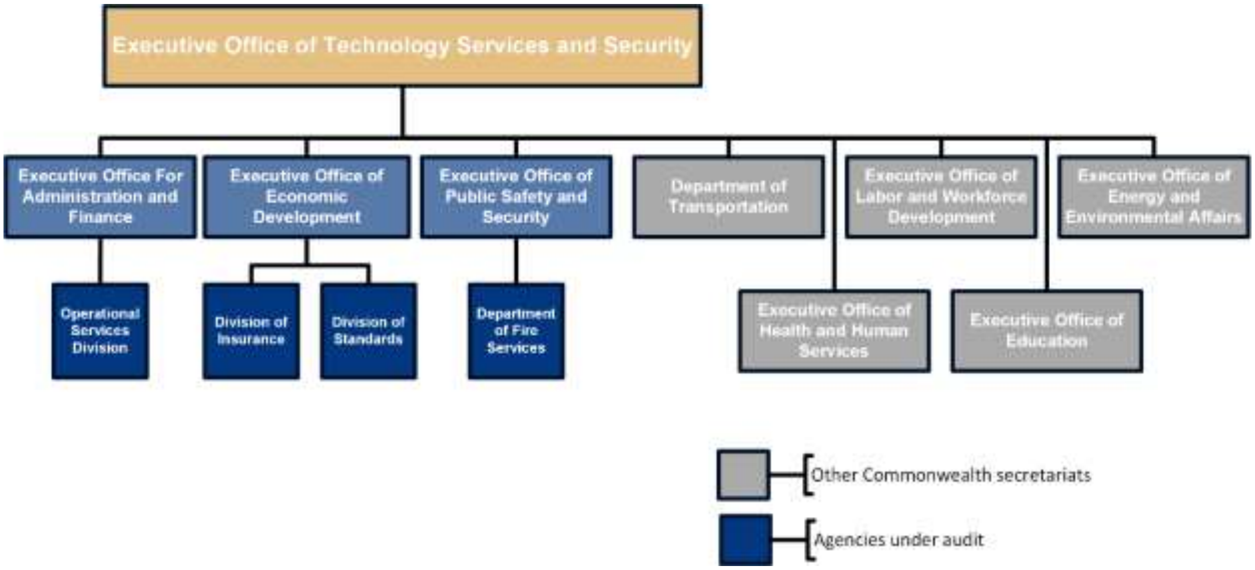
In 2018, W3C published WCAG 2.1, which built on WCAG 2.0 to improve web accessibility on mobile devices and to further improve web accessibility for people with visual impairments and cognitive disabilities. EOTSS published the Enterprise Information Technology Accessibility Policy in 2021 to meet Levels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

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


1998
The federal Rehabilitation Act is amended and Section 508 of the act mandates that standards establish functional criteria to make information accessible to people with disabilities.
1999
W3C publishes the first version of WCAG.
2001
Section 508 of the federal Rehabilitation Act is in effect.
2005
Massachusetts publishes new standards for accessible websites, called the Enterprise Web Accessibility Standards.
2008
W3C publishes WCAG 2.0.
2014
Massachusetts publishes the Enterprise Information Technology Accessibility Standards to address WCAG 2.0 requirements.
2017
EOTSS is established as the lead information technology organization.
2018
W3C publishes WCAG 2.1.
2021
EOTSS replaces the previous accessibility polices with its new Enterprise Information Technology Accessibility Policy, enforcing the WCAG 2.1 guidelines.

While EOTSS establishes standards for executive branch agencies, individual agencies, such as DOS, are responsible for ensuring that their IT solutions and web content fully comply with EOTSS's accessibility standards. The organization chart below shows the structure of EOTSS and other executive branch agencies. 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. This law helps state government agencies evaluate their design and implementation decisions to meet state accessibility requirements.

Organization of Information Security for the Commonwealth[2]


Executive Office of Technology Services and Security
Executive Office For Administration and Finance
Executive Office of Economic Development
Executive Office of Public Safety and Security
Department of Transportation
Executive Office of Labor and Workforce Development
Executive Office of Energy and Environmental Affairs
Operational Services Division
Division of Insurance
Division of Standards
Department of Fire Services
Executive Office of Health and Human Services
Executive Office of Education
Other Commonwealth secretariats
Agencies under audit

Web Accessibility

Government websites are an important way for the general public to access government information and services. Deloitte's[3] 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 had a total of 17,771,709 page views in December 2022 alone.

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 other

[2] Please note that the Division of Insurance, Department of Fire Services, and Operational Services Division audits are separate from this report and can be found on the Office of the State Auditor's website.

[3] Deloitte is an international company that provides tax, accounting, and audit services to businesses and government agencies.

disabilities. 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.

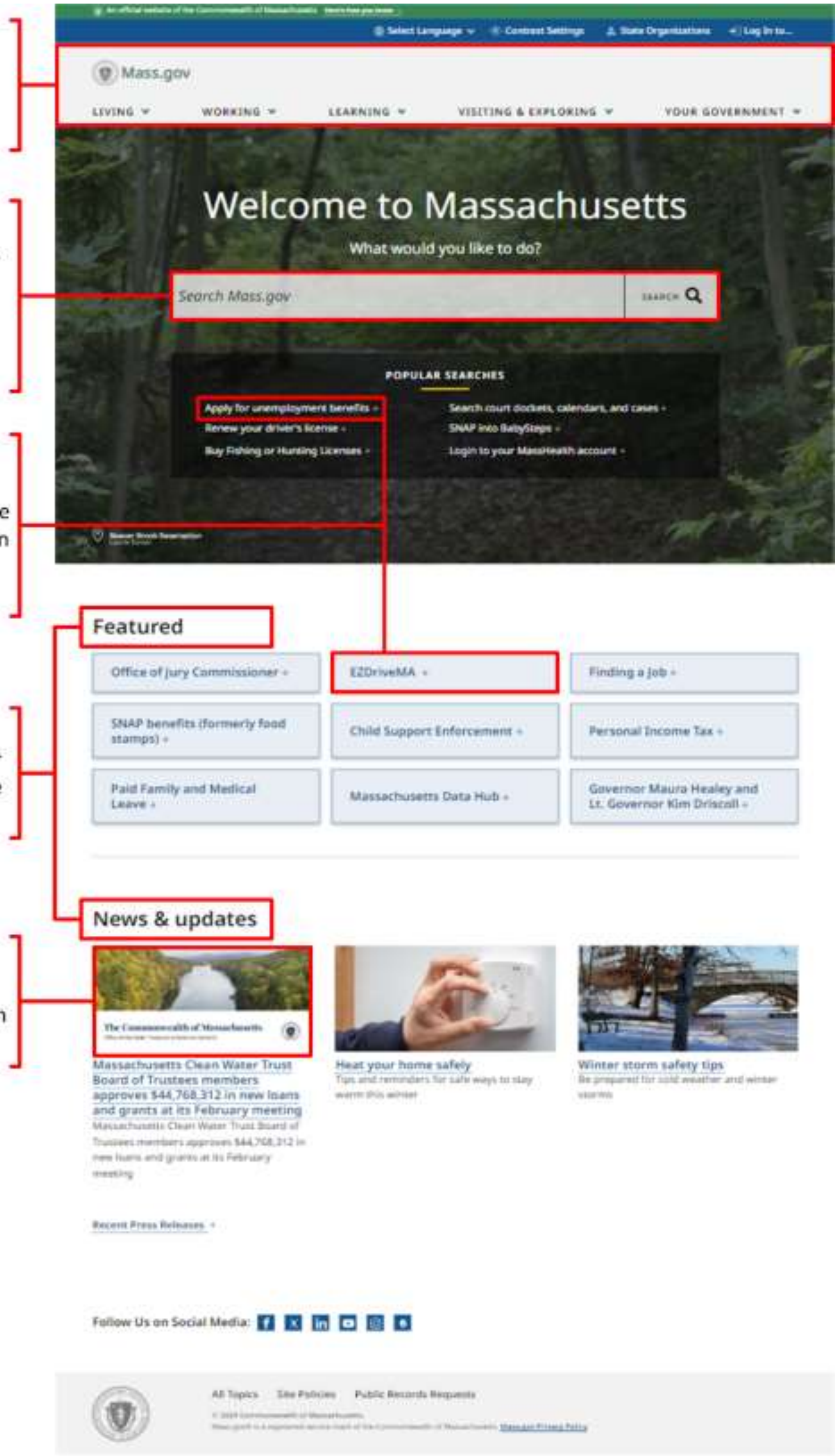
How People with Disabilities Use the Web

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.[4] 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.

[4] 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.

Common Accessibility Features of a Website


Select Language
Contrast Settings
State Organizations
Log In to...
Mass.gov
LIVING
WORKING
LEARNING
VISITING & EXPLORING
YOUR GOVERNMENT
Welcome to Massachusetts
What would you like to do?
Search Mass.gov
SEARCH
POPULAR SEARCHES
Apply for unemployment benefits
Renew your driver's license
Buy Fishing or Hunting Licenses
Search court dockets, calendars, and cases
SNAP into BabySteps
Login to your MassHealth account
Featured
Office of Jury Commissioner
EZDriveMA
Finding a Job
SNAP benefits (formerly food stamps)
Child Support Enforcement
Personal Income Tax
Paid Family and Medical Leave
Massachusetts Data Hub
Governor Maura Healey and Lt. Governor Kim Driscoll
News & updates
Recent Press Releases
Follow Us on Social Media:
All Topics
Site Policies
Public Records Requests

Massachusetts Clean Water Trust Board of Trustees members approves $44,768,312 in new loans and grants at its February meeting

Massachusetts Clean Water Trust Board of Trustees members approves $44,768,312 in new loans and grants at its February meeting

Heat your home safely

Tips and reminders for safe ways to stay warm this winter

Winter storm safety tips

Be prepared for cold weather and winter storms

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

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

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.

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

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

IT Governance

IT governance refers to the processes that state agencies use to manage their IT resources. EOTSS documents these processes in standards that it requires all executive agencies follow and recommends for all other state agencies. 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 business continuity and disaster recovery, information security incident management, and cybersecurity awareness training.

Business Continuity and Disaster Recovery

EOTSS's Business Continuity and Disaster Recovery Standard IS.005 requires each executive branch agency to develop and maintain business continuity and disaster recovery plans. These plans ensure that agencies have procedures to protect their information assets, recover critical operations, and reduce risks from a potential disruption or disaster.

Information Security Incident Management

EOTSS's Information Security Incident Management Standard IS.009 requires executive branch agencies to document procedures and establish a plan for responding to security incidents, like a cyberattack, to limit further damage to the Commonwealth's information assets once a security event is identified.

Cybersecurity Awareness Training

EOTSS has established policies and procedures that apply to all Commonwealth agencies within the executive branch. EOTSS recommends, but does not require, non-executive branch agencies to follow these policies and procedures. Section 6.2 of EOTSS's Information Security Risk Management Standard IS.010 states,

> *The objective of the Commonwealth information security training is to educate users on their responsibility to help protect the confidentiality, availability and integrity of the Commonwealth's* ***information assets****. Commonwealth Offices and Agencies must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity.*

To ensure that employees are clear on their responsibilities, EOTSS's policies require that all employees in state executive branch agencies complete a cybersecurity awareness training every year. All newly hired employees must complete initial security awareness training within 30 days of their orientation.

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 Division of Standards (DOS) for the period July 1, 2021 through December 31, 2022.

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. Did DOS's website meet the Executive Office of Technology Services and Security's (EOTSS's) Enterprise Information Technology Accessibility Policy and the Web Content Accessibility Guidelines (WCAG) 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language accessibility, error identification, and color accessibility?	**No; see Finding 1**
2. Did DOS establish information technology (IT) governance policies and procedures over the following areas: a. business continuity and disaster recovery plans that met the requirements of Sections 6.1.1.4 and 6.2.1 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005; b. information security incident response plan and procedures that met the requirements of Sections 6.5.1 and 6.5.2 of EOTSS's Information Security Incident Management Standard IS.009; and c. cybersecurity awareness training that met the requirements of Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010?	**No; see Findings 2 and 3**

To achieve our audit objectives, we gained an understanding of DOS's internal control environment related to the objectives by reviewing applicable policies and procedures and by interviewing DOS staff members and management.

We performed the following procedures to obtain sufficient, appropriate audit evidence to address the audit objectives.

Web Accessibility

To determine whether DOS's website meets EOTSS's Enterprise Information Technology Accessibility Policy and WCAG 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility, we tested a random, nonstatistical sample of 20 out of a total of 50 DOS webpages in the audit population. We performed the following procedures.

User Accessibility

- We determined whether the webpage could be viewed in both portrait and landscape modes.
- We determined whether, when zoomed in to 200%, content on the webpage was undamaged and remained readable.
- We determined whether, when zoomed in to 400%, content on the webpage was undamaged and in a single column.

Keyboard Accessibility

- We determined whether all elements 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.

Navigation Accessibility

- 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.

Language Accessibility

- We determined whether words that appeared on the webpage matched the language to which the webpage was set.
- We determined whether proper names were identified in PDF files included on the webpage to avoid improper translation or pronunciation errors from screen readers.

Error Identification

- We determined whether there was text explaining why an error occurred when a user input information into an entry field.

- 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.

See Finding 1 for an issue we identified with hyperlinks on DOS's website.

IT Governance

To determine whether DOS established IT governance policies and procedures over the following areas, we performed the following procedures.

Business Continuity and Disaster Recovery

To determine whether DOS's business continuity plan met the requirements of Section 6.1.1.4 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, we interviewed knowledgeable DOS employees and inspected DOS's business continuity plan to ensure that it addressed the following: critical business processes, DOS's manual and automated processes, minimum operating requirements to resume critical functions, the designation of a business continuity lead, clearly defined and communicated roles and responsibilities, assigned points of contact, and annual updates.

To determine whether DOS's disaster recovery plan met the requirements of Section 6.2.1 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, we interviewed knowledgeable DOS staff members and inspected DOS's disaster recovery plan to ensure that it addressed the following:

- developing and maintaining processes for disaster recovery,
- identifying relevant stakeholders,
- conducting damage assessments of impacted IT infrastructure and applications,
- establishing procedures that allow facility access for employees to restore data in an emergency,
- recovering critical agency services,
- implementing interim means for performing critical business processes at or above minimum service levels, and

- restoring service at the original site of impact without interruption.

See Finding 2 for an issue we identified with DOS's business continuity and disaster recovery plans.

Information Security Incident Response Plan and Procedures

To determine whether DOS's information security incident response plan and procedures met the requirements of Sections 6.5.1 and 6.5.2 of EOTSS's Information Security Incident Management Standard IS.009, we interviewed knowledgeable DOS staff members and requested DOS's information security incident response plans and procedures. We learned that DOS relied on the Executive Office of Economic Development for an information security incident response plan and procedures, so we inspected the Executive Office of Economic Development's information security incident response plan and procedures to determine whether they met the requirements of the aforementioned policy.

See Finding 3 for an issue we identified with DOS's information security incident response plan and procedures.

Cybersecurity Awareness Training

To determine whether DOS's cybersecurity awareness training met the requirements of Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010, we performed the following procedures:

- We selected a random sample of 7 from a population of 10 newly hired employees and inspected their cybersecurity awareness training certificates of completion to determine whether they completed the new hire cybersecurity awareness training within 30 days of orientation.
- We selected a random sample of 7 out of a population of 18 DOS employees who had been employed by DOS for more than one year and inspected their cybersecurity awareness training certificates of completion to determine whether they completed the annual refresher cybersecurity awareness training.

We noted no exceptions in our testing; therefore, we conclude that DOS's cybersecurity awareness training met the requirements of Sections 6.2.3 and 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010.

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 Testing

To determine the reliability of the site map spreadsheet that we received from DOS management, we interviewed knowledgeable DOS staff members and checked that variable formats (e.g., dates, unique identifiers, and abbreviations) were accurate. Additionally, we ensured that none of the following issues affected the spreadsheet: abbreviation of data fields, missing data (e.g., hidden rows or columns, blank cells, and absent records), and duplicate records. We also ensured that all values in the data set corresponded with expected values.

We selected a random sample of 20 uniform resource locators (URLs)[5] from the DOS site map and traced them to the corresponding webpage on DOS's website, checking that each URL and page title matched the information on the DOS website. We also selected a random sample of 20 URLs from DOS's website and traced the URL and page title to the site map to ensure that there was a complete and accurate population of URLs on the site map.

IT Governance Testing

To determine the reliability of the employee list we received from DOS management, we checked that variable formats (e.g., dates, unique identifiers, and abbreviations) were accurate. Additionally, we ensured that none of the following issues affected the list: abbreviation of data fields, missing data (e.g., hidden rows or columns, blank cells, and absent records), and duplicate records. We also ensured that all values in the data set corresponded with expected values.

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 we received from DOS 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 employee list were sufficiently reliable for the purposes of our audit.

[5] A URL uniquely identifies an internet resource, such as a website.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Division of Standards' website is not fully accessible for all Massachusetts residents.

Some of the Division of Standards' (DOS's) webpages do not comply with state information technology (IT) accessibility standards for navigation accessibility. During our audit, we determined that 4 out of 20 DOS webpages we tested contained hyperlinks that did not allow users to navigate to the intended webpages (i.e., broken and faulty hyperlinks).

Broken or faulty hyperlinks negatively impact the user experience and make it difficult to locate additional relevant information. They can also limit some users from having equitable access to critical information and key online services offered by DOS (e.g., vendor licenses). Also, broken or faulty hyperlinks could increase the likelihood that users access and rely upon outdated or incorrect information or are directed to webpages that no longer exist.

Authoritative Guidance

The IT Accessibility Standards section of the Executive Office of Technology Services and Security's (EOTSS's) Enterprise Information Technology Accessibility Policy states,

> *1. a. Accessibility of electronic content, applications, or services must be measured with one or more of the applicable following technical standards.*
>
> *i. Web and desktop applications, multimedia content, electronic documents: Web Content Accessibility Guidelines 2.1 (WCAG), level A and AA Guidelines.*

The Web Accessibility Initiative's Web Content Accessibility Guidelines 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

DOS management stated that they do not regularly review website content to ensure that all hyperlinks lead to related information.

Recommendation

DOS should review its webpages to ensure that all hyperlinks lead to related information to provide equitable access to critical information and services offered online by DOS to all Commonwealth residents.

Auditee's Response

> *In 2018, the Commonwealth transitioned to [a new] operating system for agencies to utilize in updating their own content on agency websites. Prior to 2018, information technology staff were responsible for posting new web content and revisions to existing content, and for DOS this meant sending web content requests to staff in the Information Technology group for the Executive Office of Housing & Economic Development (HED-IT).*
>
> *Since 2018, designated staff within each agency, having [operating system] access authority granted by the Executive Office of Technology Services & Security ("EOTSS"), have been responsible for maintaining agency website content. EOTSS staff, however, periodically review web content and inform agencies of any noted issues. DOS agrees that continuous review of our website is important. DOS personnel attend [operating system] user group meetings, and work regularly with EOTSS staff and others who view DOS's website, to address identified issues including broken links. As noted during the audit, DOS believes the website accessibility findings identified by the Auditors were caused by factors not directly in DOS's control but took immediate action to rectify these issues to the Auditors' satisfaction. We will continue to work closely with EOTSS and others who view and analyze DOS's website to ensure its accuracy and accessibility for all consumers.*

Auditor's Reply

While we acknowledge that EOTSS (as the oversight agency) plays a role in ensuring the accessibility of web content for state executive branch agencies, DOS should ensure that IT solutions and content are in compliance with accessibility standards of EOTSS's Enterprise Information Technology Accessibility Policy. This is pursuant to Section 2 of Chapter 7D of the Massachusetts General Laws, which requires all state executive branch agencies, including DOS, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOS has taken measures to address our concerns on this matter.

2. The Division of Standards' business continuity plan does not include all required elements, and it does not have a disaster recovery plan.

DOS's business continuity plan does not include a risk assessment and business impact analysis. Further, DOS's business continuity plan does not identify a business continuity lead, and it was not updated or tested annually during the audit period.

Additionally, DOS does not have a disaster recovery plan.

Without adequate and updated business continuity or disaster recovery plans, DOS cannot ensure that it has procedures for protecting information assets or a plan to recover critical operations when an interruption or disaster occurs. Additionally, DOS could use a business continuity plan to ensure that it responds adequately to unplanned business disruptions like the COVID-19 pandemic.

Authoritative Guidance

EOTSS's Business Continuity and Disaster Recovery Standard IS.005 states,

> *6.1.1.4 Develop business continuity plans (BCP): Each agency shall develop BCPs for critical business processes based on prioritization of likely disruptive events in light of their probability, severity and consequences for information security identified through the [Business Impact Analysis (BIA)] and risk assessment processes. . . .*
>
> *6.1.1.4.2 The primary responsibility for developing, maintaining and testing organizational and functional BCPs shall reside with the Business Continuity Lead. . . .*
>
> *6.1.1.4.2.2 Point(s) of contact should be identified from the customer side for any incident or crisis communication via call, messaging and/or email. The contact details of the point(s) of contact should be validated and updated at least annually. . . .*
>
> *6.2.1 Commonwealth Executive Offices and Agencies must develop and maintain processes for disaster recovery plans at both onsite primary Commonwealth locations and at alternate offsite locations. [Disaster recovery] plans shall include step-by-step emergency procedures, including:*
>
> *6.2.1.1 Identify relevant stakeholders (primary and secondary) and establish a call tree.*
>
> *6.2.1.2 Conduct a damage assessment of the impacted IT infrastructure and applications.*
>
> *6.2.1.3 Establish procedures that allow facility access (e.g., recovery/secondary site) in support of the restoration of lost data in the event of an emergency.*
>
> *6.2.1.4 Recover critical agency services and* ***information assets*** *based on recovery priorities as established during the BIA.*
>
> *6.2.1.5 Provide interim means for performing critical business processes at or above the minimum service level defined in the BCP and within the tolerable length of time.*
>
> *6.2.1.6 Restore service at the original site of impact and migrate from the alternate locations to the original site without unacceptable interruption or degradation in service.*

Reasons for Issue

DOS management was unaware that they should develop and maintain both a business continuity plan and a disaster recovery plan, and that these plans should be separate from the Executive Office of Economic Development's and EOTSS's policies, procedures, and standards.

Recommendations

1. DOS should update its business continuity plan to include all required elements. It should also update the plan annually and whenever a major organizational change occurs.

2. DOS should develop and implement a disaster recovery plan.

Auditee's Response

1. *DOS is working in conjunction with EOTSS to update its current business continuity plan in accordance with all applicable requirements and will issue it as soon as possible. Specifically, DOS is working with EOTSS' Office of Enterprise Risk Management and their vendor . . . to complete this work as soon as possible.*

2. *Two basic requirements of a disaster recovery plan are the identification of a substitute site from which senior management can run agency operations when a disaster occurs, and a back-up IT operation that further enables an agency's network and business functions to continue working at full capacity. These requirements are beyond the scope of DOS to develop independently. DOS is committed to working to ensure that appropriate disaster recovery plans are in place and consistent with the "Business Continuity and Disaster Recovery Standard" established and maintained by the Commonwealth's Chief Information Security Officer.*

Auditor's Reply

While we acknowledge that EOTSS (as the oversight agency) plays a role in ensuring that DOS has a sufficient disaster recovery plan, DOS must develop a disaster recovery plan in compliance with EOTSS's Business Continuity and Disaster Recovery Standard IS.005. This is pursuant to Section 2 of Chapter 7D of the General Laws, which requires all state executive branch agencies, including DOS, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOS is taking measures to address our concerns on this matter.

3. The Division of Standards relies on an information security incident response plan and procedures that do not include all required elements.

The information security incident response plan and procedures that DOS relies on do not include guidance for implementing corrective actions or post-incident analysis, criteria for business recovery, data backup processes, an analysis of legal requirements for reporting IT system compromises, or incident response procedures from required external parties.

Without an adequate information security incident response plan and procedures, DOS cannot ensure that it takes sufficient containment measures when it identifies a security incident and subsequently completes proper documentation, an investigation, a risk analysis, and an impact analysis.

Authoritative Guidance

EOTSS's Information Security Incident Management Standard IS.009 states,

> *6.5.1. **Incident** response procedures*
>
> *Commonwealth offices and agencies must document procedures for responding to security **incidents** to limit further damage to the Commonwealth's **information assets**. Procedures shall include:*
>
> *6.5.1.1. Identification of the cause of the **incident***
>
> *6.5.1.2. Execution of corrective actions*
>
> *6.5.1.3. Post-**incident** analysis*
>
> *6.5.1.4. Communication strategy*
>
> *6.5.2. **Incident** response plan*
>
> *Commonwealth Offices and Agencies shall establish an **incident** response plan. The **incident** response plan shall include, at a minimum:*
>
> *6.5.2.1. Roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of required internal and external parties.*
>
> *6.5.2.2. Specific **incident** response procedures.*
>
> *6.5.2.3. Execution of corrective actions and post-**incident** analysis.*
>
> *6.5.2.4. Establish criteria to activate business recovery and continuity processes. . . .*
>
> *6.5.2.5. Data backup processes. . . .*

6.5.2.6. Analysis of legal requirements for reporting [IT system] compromises.

*6.5.2.7. Reference or inclusion of **incident** response procedures from required external parties.*

Reasons for Issue

DOS management stated that the Executive Office of Economic Development and EOTSS handle DOS's information security incident response management functions.

Recommendation

DOS should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DOS could establish a supplemental information security incident response plan and procedures that include guidance for implementing corrective action or post-incident analysis, criteria for business recovery, data backup processes, and an analysis of legal requirements for reporting IT system compromises.

Auditee's Response

> *DOS relies on and follows the information security incident response plan and procedures adopted by [the Executive Office of Economic Development (EOED)]. As discussed during the Audit, because DOS lacks the technical expertise required to independently develop and implement a supplemental incident response plan and procedures as suggested, DOS will work with EOTSS and EOED IT to ensure that our information security incident response plan and procedures, or any supplements thereto, include all elements required by EOTSS' Information Security Incident Management Standard IS.009.*

Auditor's Reply

While we acknowledge that EOTSS (as the oversight agency) plays a role in ensuring that DOS has a sufficient information security incident response plan, DOS must develop an information security incident response plan in compliance with EOTSS's Information Security Incident Management Standard IS.009. This is pursuant to Section 2 of Chapter 7D of the General Laws, which requires all state executive branch agencies, including DOS, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOS is taking measures to address our concerns on this matter.