OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued March 19, 2024

Division of Insurance

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

March 19, 2024

Gary Anderson, Commissioner of Insurance
Division of Insurance
1000 Washington Street, Suite 810
Boston, MA 02118

Dear Mr. Anderson:

I am pleased to provide to you the results of the enclosed performance audit of the Division of Insurance. 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 Insurance. 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
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DOI	Division of Insurance
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 Insurance (DOI) for the period July 1, 2021 through December 31, 2022. In this performance audit, we determined the following:

- whether DOI'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, error identification, and color accessibility and
- whether DOI 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 15**	DOI's website is not fully accessible for all Massachusetts residents.
Recommendations **Page 18**	1. DOI 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 DOI to all Commonwealth residents. 2. DOI should review web content that appears in other languages to ensure that the pages have accurate language attributes to facilitate effective translation and provide a user experience that is inclusive to all Commonwealth residents.
Finding 2 **Page 19**	DOI did not update its business continuity plan or have a disaster recovery plan.
Recommendations **Page 20**	1. DOI should update its business continuity plan annually and whenever a major organizational change occurs. 2. DOI should develop and implement a disaster recovery plan.
Finding 3 **Page 21**	DOI relies on an information security incident response plan and procedures that do not include all required elements.
Recommendation **Page 22**	DOI should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DOI 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, an analysis of legal requirements for reporting IT system compromises, and incident response procedures from required external parties.

OVERVIEW OF AUDITED ENTITY

The Division of Insurance (DOI), located at 1000 Washington Street in Boston, was established in accordance with Chapter 26 of the Massachusetts General Laws and is one of five agencies overseen by the Office of Consumer Affairs and Business Regulation. DOI operates under the direction of the commissioner of insurance, who is appointed by the Governor.

DOI's mission is to regulate the Commonwealth's insurance industry, including but not limited to its domestic[1] and foreign[2] insurers, business entities, health maintenance organizations, insurance producers, and brokers. Additionally, DOI intervenes on behalf of Massachusetts residents who believe they have been victimized by unfair business practices. As of April 2019, there were approximately 1,800 insurers conducting business in the Commonwealth.

According to DOI's website,

> *The DOI monitors financial solvency, licenses insurance companies and producers, reviews and approves rates and forms, and coordinates the takeover and liquidation of insolvent insurance companies and the rehabilitation of financially troubled companies. We also investigate and enforce state laws and regulations pertaining to insurance and respond to consumer inquiries and complaints.*

DOI employed 116 full-time employees as of December 31, 2022. This included attorneys, actuaries, accountants, insurance examiners, and support employees. DOI's state appropriations for fiscal years 2021, 2022, and 2023 were $15.6 million, $15.6 million, and $16.3 million, respectively.

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,[3] with the participation of state government webpage developers, including developers with disabilities, created the Enterprise Web Accessibility

1. An insurer incorporated or formed in the Commonwealth of Massachusetts.
2. An insurer formed by authority of any state or government other than the Commonwealth of Massachusetts.
3. 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.

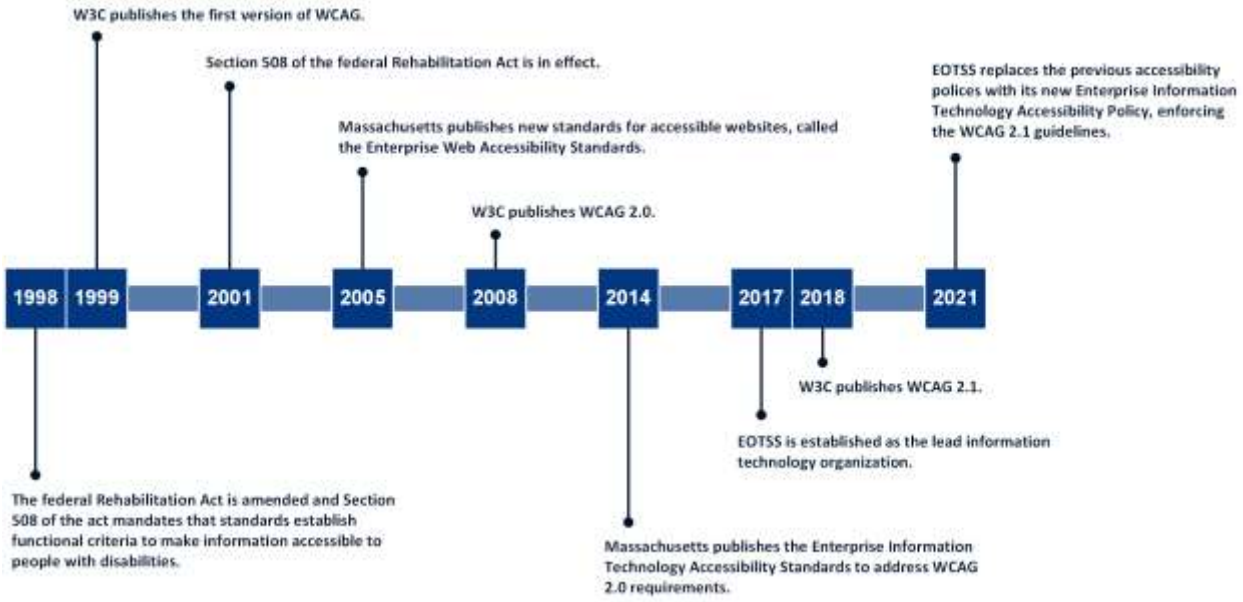
Standards. These standards required all executive branch agencies to follow the guidelines in Section 508 of the Rehabilitation Act amendments of 1998. These amendments went into effect in 2001 and established precise technical requirements to which electronic and information technology (IT) products must adhere. This technology includes, but is not limited to, products such as software, websites, telecommunications, 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.

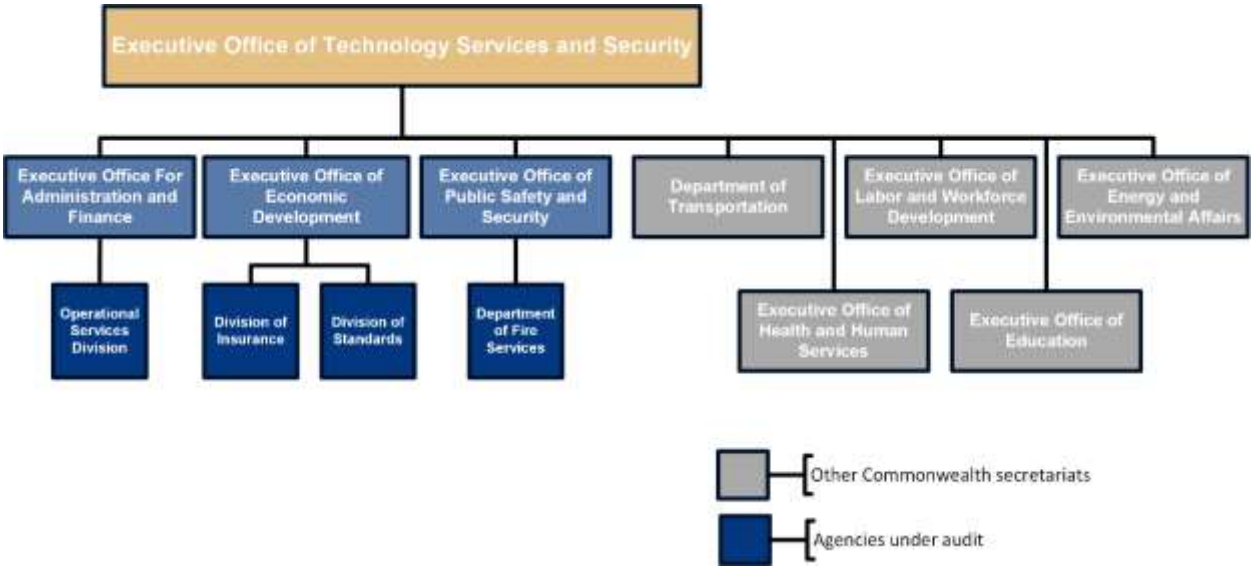
In 2018, W3C published WCAG 2.1, which built on WCAG 2.0 to improve web accessibility on mobile devices and to further improve web accessibility for people with visual impairments and cognitive disabilities. EOTSS published the Enterprise Information Technology Accessibility Policy in 2021 to meet Levels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

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



While EOTSS establishes standards for executive branch agencies, individual agencies, such as DOI, 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[4]



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. According to the analytics dashboard for Mass.gov, 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 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

4. Please note that the Department of Fire Services, Division of Standards, and Operational Services Division audits are separate from this report and can be found on the Office of the State Auditor's website.
5. Deloitte is an international company that provides tax, accounting, and audit services to businesses and government agencies.

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 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.

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.

Common Accessibility Features of a Website

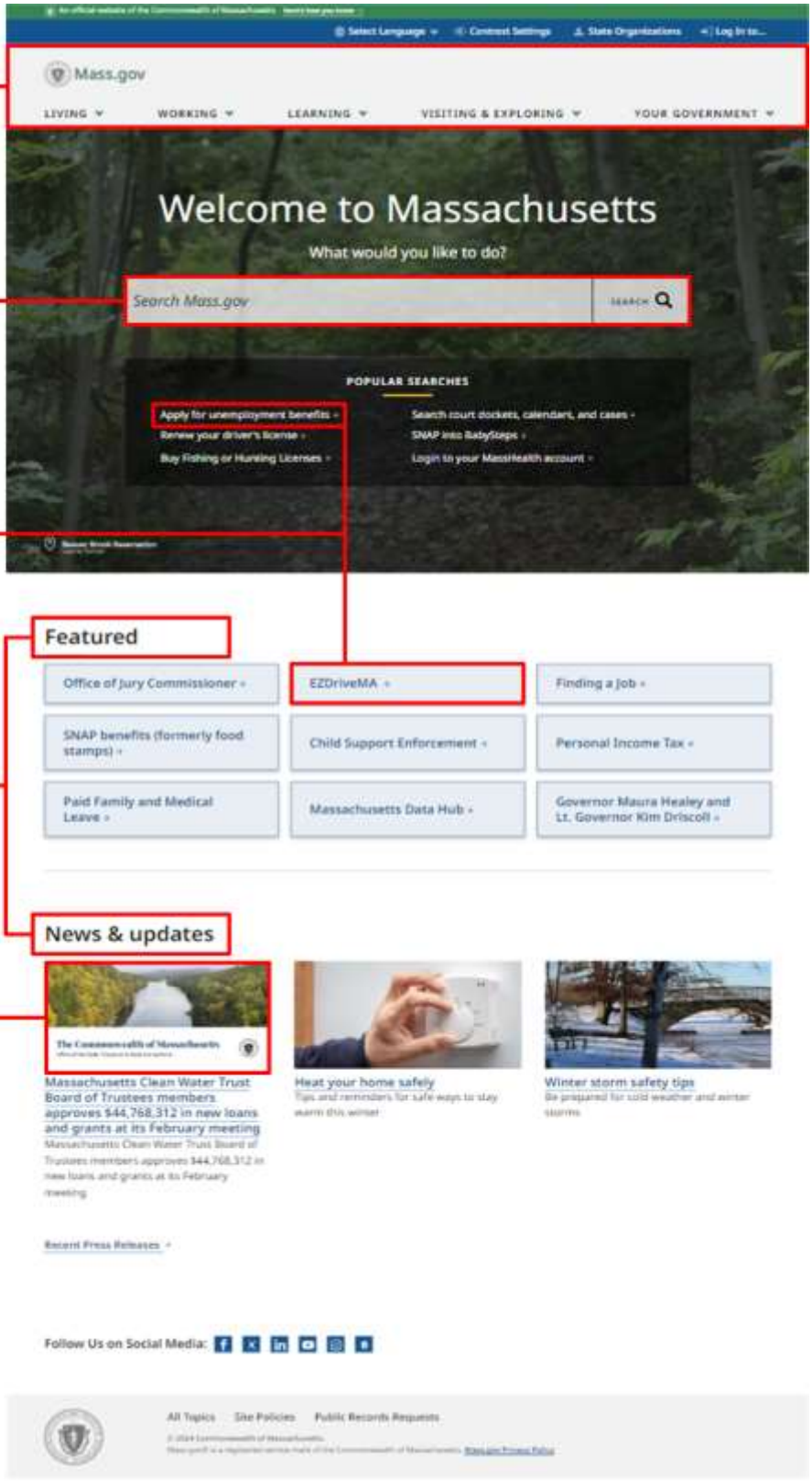
A site's header can appear throughout an entire site and contain links to main content areas.

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 Insurance (DOI) 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 DOI'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, error identification, and color accessibility?	**No, see Finding 1**
2. Did DOI 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 DOI's internal control environment related to the objectives by reviewing applicable policies and procedures and by interviewing DOI 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 DOI's website meets WCAG 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility, we tested a random, nonstatistical sample of 60 out of a total of 930 DOI 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

- 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.
- 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 issues we identified with hyperlinks and language attributes on DOI's website.

IT Governance

To determine whether DOI established effective IT governance policies and procedures, we performed the following procedures.

Business Continuity and Disaster Recovery

To determine whether DOI's business continuity plan complied with Section 6.1.1.4 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, we interviewed knowledgeable DOI employees and inspected DOI's business continuity plan to ensure that it addressed the following: critical business processes, DOI'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 DOI's disaster recovery plan complied with Section 6.2.1 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, we interviewed knowledgeable DOI employees and inspected DOI'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 to support the restoration of 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 regarding DOI's business continuity plan.

Information Security Incident Response Plan and Procedures

To determine whether DOI's information security incident response plan and procedures complied with Sections 6.5.1 and 6.5.2 of EOTSS's Information Security Incident Management Standard IS.009, we interviewed knowledgeable DOI employees and requested DOI's information security incident response plans and procedures. We learned that DOI relies on the Executive Office of Economic Development (formerly the Executive Office of Housing and 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 complied with the aforementioned EOTSS policy.

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

Cybersecurity Awareness Training

To determine whether DOI'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 inspected the cybersecurity awareness training certificates of completion for all six newly hired employees to determine whether they completed the new hire cybersecurity awareness training within 30 days of orientation.
- We inspected the cybersecurity awareness training certificates of completion for a random sample of 35 out of a total population of 116 employees to determine whether they completed the annual refresher cybersecurity awareness training.

We noted no exceptions in our testing; therefore, we conclude that DOI'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 DOI management, we interviewed knowledgeable DOI employees and checked that variable formats (e.g., dates, unique identifiers, and 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, and incomplete records), and no duplicate records and that all values in the data set corresponded with expected values.

We selected a random sample of 20 uniform resource locators (URLs)[7] that could be accessed independently from the DOI site map and traced them to the corresponding webpage, checking that each URL and page title matched the information on the DOI website. We also selected a random sample of 20 URLs from DOI's website and traced each 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 from DOI management, we checked that variable formats (e.g., dates, unique identifiers, and 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, and incomplete records), and no duplicate records and 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 provided by DOI 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.

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

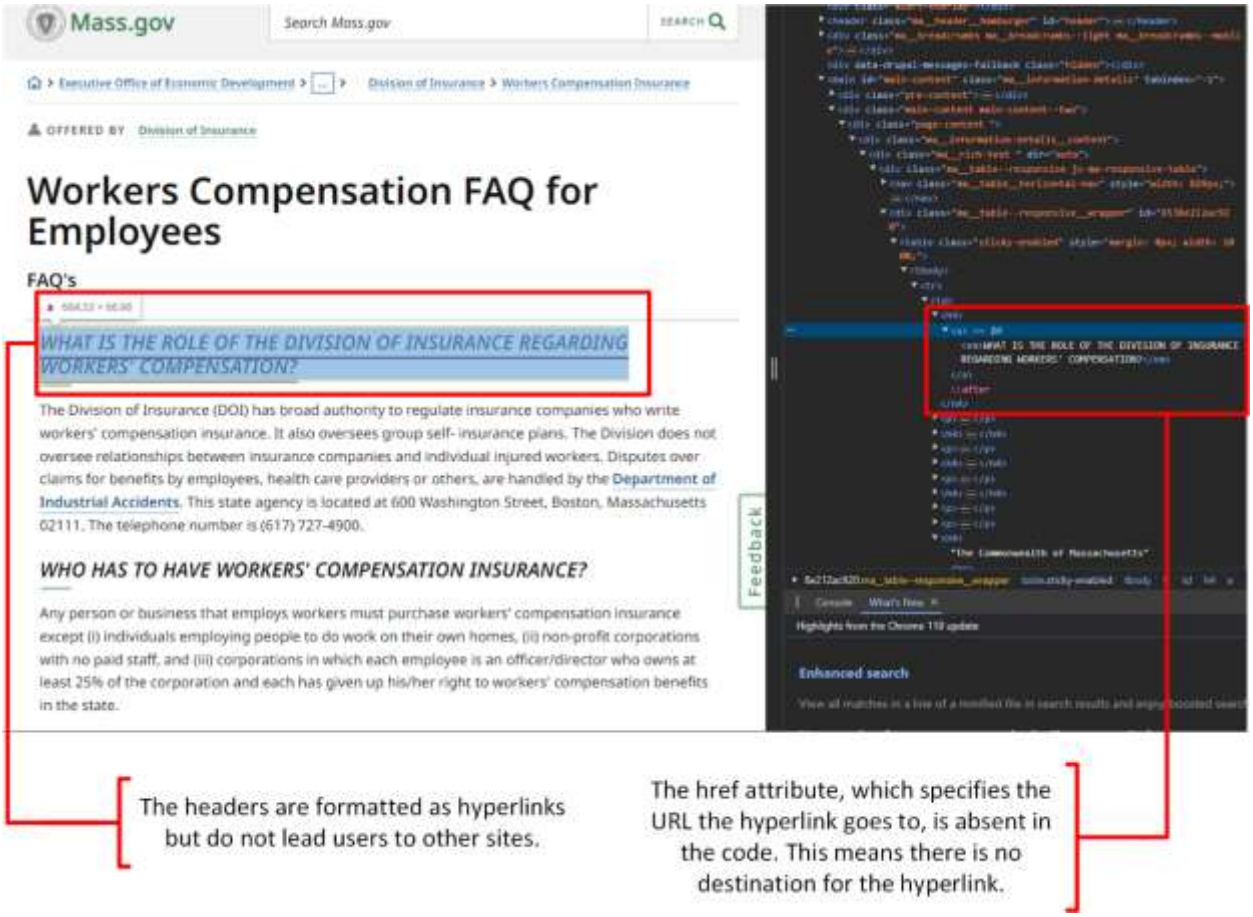
DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

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

Some Division of Insurance (DOI) webpages do not comply with state information technology (IT) accessibility standards for navigation accessibility and language attributes. During our audit, we determined that 3 out of the 60 DOI webpages tested contained hyperlinks that did not allow users to navigate to related pages (i.e., broken and faulty hyperlinks). For language testing, we determined that 1 out of the 60 DOI webpages contained an inaccurate language attribute, which means that words on the webpage did not match the language to which the webpage was set.

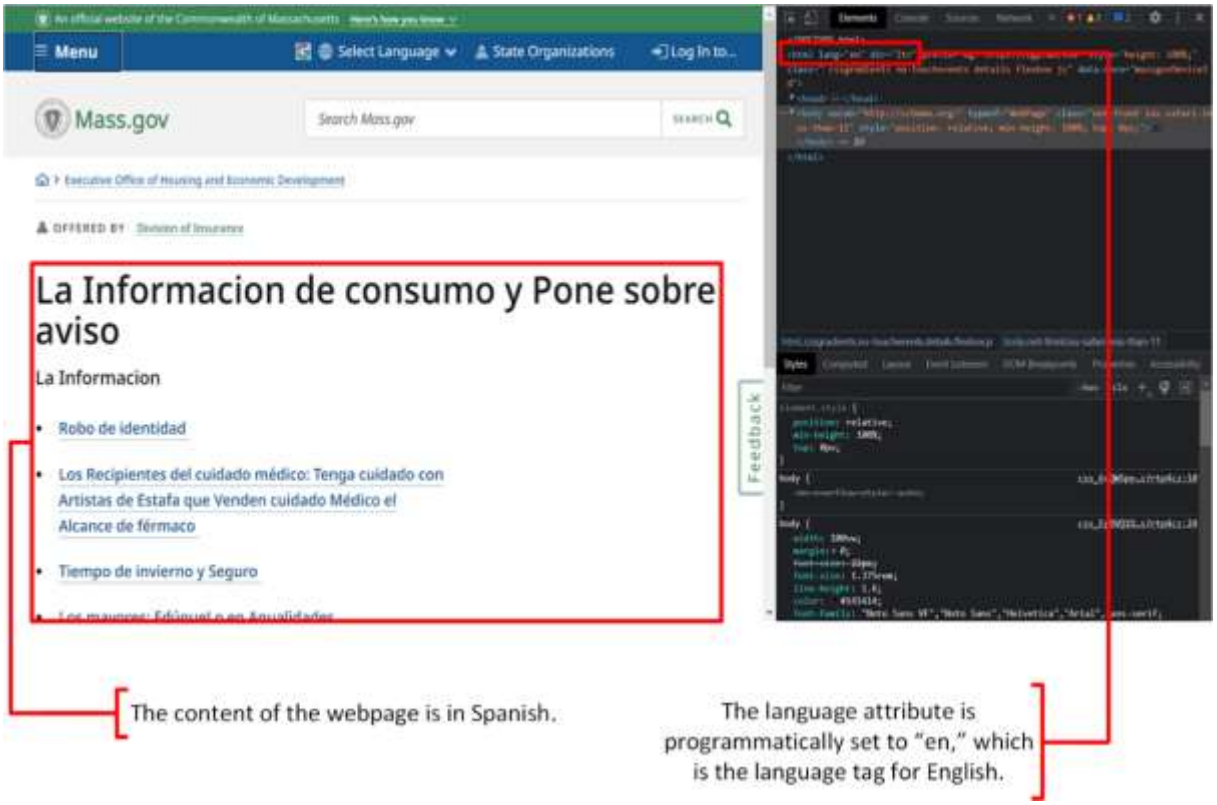
Navigation Accessibility: Broken Hyperlinks

Broken or faulty hyperlinks negatively impact the user experience and make it difficult to locate additional relevant information. (See example below.) They can also limit some users from having equitable access to critical information and key online services offered by DOI (e.g., insurance-related complaint submission). Also, broken or faulty hyperlinks could increase the likelihood that users access outdated or incorrect information or are directed to webpages that no longer exist.



Language: Inaccurate Language Attributes

A language attribute specifies the language of a webpage or an element of a webpage. (See example below.) Inaccurate language attributes can pose a number of challenges for accessibility. Specifically, if DOI does not correctly identify language attributes, people using translation software or a screen reader could lose the ability to interact with or understand critical content on DOI's website. For example, language attributes allow screen readers that support multiple languages to adapt to the specific pronunciation of the language on the page. This allows a screen reader to speak the text in the appropriate accent with proper pronunciation.



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. . . .*
>
> *Success Criterion 3.1.1 Language of Page (Level A)*
>
> *The default human language of each Web page can be programmatically determined.*

Reasons for Issue

DOI management stated that the broken hyperlinks were caused by changes to its website architecture,[8] webpage updates that replaced content, and copy and paste errors that allowed for improper formatting of text. DOI management believes the language attribute was caused by a system error.

Recommendations

1. DOI 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 DOI to all Commonwealth residents.

2. DOI should review web content that appears in other languages to ensure that the pages have accurate language attributes to facilitate effective translation and provide a user experience that is inclusive 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 the DOI this meant sending web content requests to staff in the Information Technology ("IT") group for the Executive Office of Housing & Economic Development.

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. The DOI agrees that continuous review of our website is important. DOI personnel attend [operating system] user group meetings, and work regularly with EOTSS staff and others who view the DOI's website, to address identified issues including broken links. As noted during the audit, DOI believes the website accessibility findings identified by the Auditors were caused by factors not directly in DOI'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 DOI's website to ensure its accuracy and accessibility for all consumers.

The DOI is working to develop a language access plan that will apply across all operational areas, in accordance with the Governor's related Executive Order #615 to improve language access across state government. This will facilitate accurate and effective language translation and provide an inclusive user experience to all who need our services. This effort will include issuing [a request for responses (RFR)] to solicit vendors who can provide immediate translation services when the need for them arises. The DOI also surveyed staff to identify those with fluency in multiple languages,

8. A website's architecture is the structure of a website's webpages (e.g., which pages are linked within other pages).

who could assist as needed until we secure a vendor with broader language capabilities through an RFR process.

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, DOI 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 DOI, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOI has taken measures to address our concerns on this matter.

2. The Division of Insurance did not update its business continuity plan or have a disaster recovery plan.

DOI did not update its business continuity plan and did not have a disaster recovery plan during the audit period.

Without an updated business continuity plan or a disaster recovery plan, DOI cannot ensure that it has procedures for protecting information assets or a plan to recover critical operations when an interruption or disaster occurs. Additionally, a business continuity plan would ensure that DOI has an adequate response 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. . . .

6.1.1.4.3 BCPs shall be updated whenever a major organizational change occurs or at least annually, whichever comes first. . . .

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.

Reasons for Issue

DOI management stated that process changes brought on by the COVID-19 pandemic were the primary cause for not updating the agency's business continuity plan. DOI management added that updates to the 2020 business continuity plan, which will take into account agency-wide process changes, are currently in progress and should be released by the end of calendar year 2023.

DOI management stated that elements of a disaster recovery plan are included in the business continuity plan and internal control plan.

Recommendations

1. DOI should update its business continuity plan annually and whenever a major organization change occurs.
2. DOI should develop and implement a disaster recovery plan.

Auditee's Response

The DOI 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.

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 the DOI to develop independently. The DOI 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 DOI has a sufficient disaster recovery plan, DOI 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 DOI, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOI is taking measures to address our concerns on this matter.

3. The Division of Insurance 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 DOI 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, DOI 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

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

Recommendation

DOI should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DOI 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, an analysis of legal requirements for reporting IT system compromises, and incident response procedures from required external parties.

Auditee's Response

DOI 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 DOI lacks the technical expertise required to independently develop and implement a supplemental incident response plan and procedures as suggested, DOI 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 DOI has a sufficient information security incident response plan, DOI 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 DOI, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DOI is taking measures to address our concerns on this matter.