OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued March 20, 2024

Department of Fire Services

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

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

March 20, 2024

Jon Davine, State Fire Marshal
Department of Fire Services
1 State Road, PO Box 1025
Stow, MA 01775

Dear Mr. Davine:

I am pleased to provide to you the results of the enclosed performance audit of the Department of Fire Services. 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 Department of Fire Services. 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

DFS	Department of Fire Services
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 Department of Fire Services (DFS) for the period July 1, 2021 through December 31, 2022. In this performance audit, we determined the following:

- whether DFS'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 DFS 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**	DFS's website is not fully accessible for all Massachusetts residents.
Recommendation **Page 15**	DFS 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 DFS to all Commonwealth residents.**Error! Reference source not found.**
Finding 2 **Page 16**	DFS did not update its business continuity plan.
Recommendation **Page 16**	DFS should update its business continuity plan annually and whenever a major organizational change occurs.
Finding 3 **Page 17**	DFS relies on an information security incident response plan and procedures that do not include all of the required elements.
Recommendation **Page 18**	DFS should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DFS 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.
Finding 4 **Page 19**	DFS did not provide its contractors with cybersecurity awareness training.
Recommendations **Page 19**	1. DFS should ensure that its contractors complete cybersecurity awareness training. 2. DFS should ensure that its contractors have access to its cybersecurity awareness training platform.

OVERVIEW OF AUDITED ENTITY

The Department of Fire Services (DFS) was established under Section 109 of Chapter 151 of the 1996 Massachusetts Acts and Resolves and codified in Section 1 of Chapter 22D of the Massachusetts General Laws. The State Fire Marshal directs DFS and its divisions. The Executive Office of Public Safety and Security develops policies and oversees the budget for DFS.

According to its internal control plan, DFS's mission is as follows:

> *To provide the citizens of Massachusetts with the ability to create safer communities; to assist and support the fire service community in the protection of life and property; to promote and enhance firefighter safety; and to provide a fire service leadership presence in the Executive Office of Public Safety and Security in order to direct policy and legislation on all fire related matters.*

DFS provides training and assistance to fire departments in the Commonwealth through its Massachusetts Firefighting Academy. DFS provides further assistance to communities through its Hazardous Materials Emergency Response Division, Special Operations Team, Fire and Explosion Investigation Unit, and Division of Fire Safety.

DFS's state appropriations for fiscal years 2021, 2022, and 2023 were $31,897,664, $30,092,332, and $32,444,914, 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,[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 established precise technical requirements to which electronic and information technology (IT) products

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.

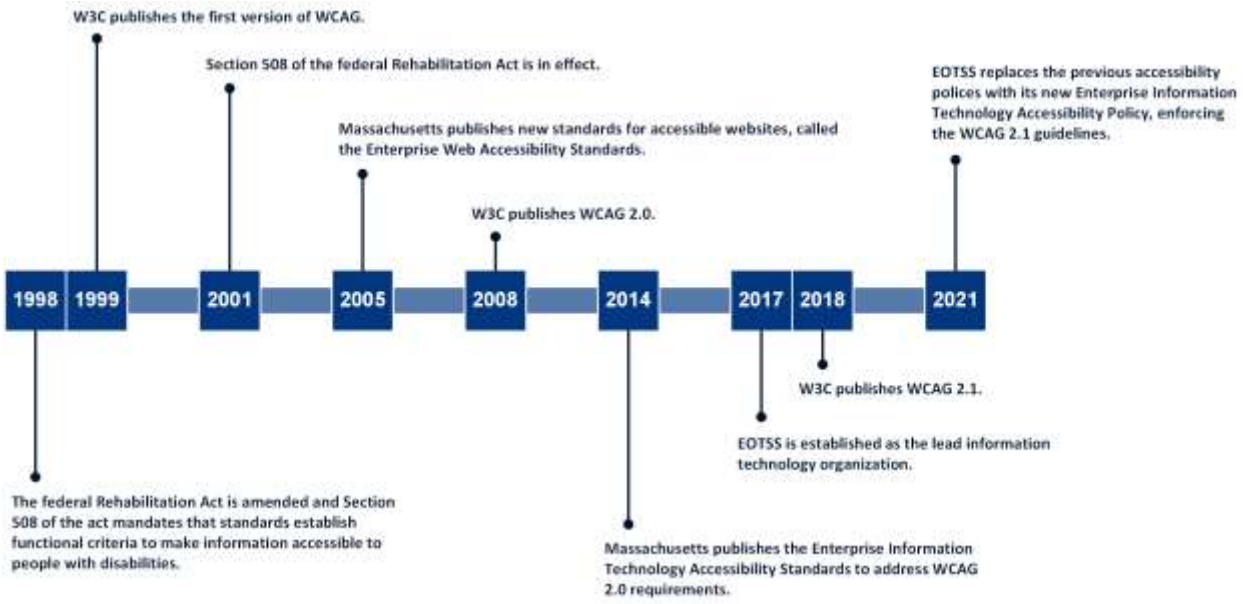
must adhere. This technology includes, but is not limited to, products such as software, websites, multimedia products, and certain physical products, such as standalone terminals.

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.

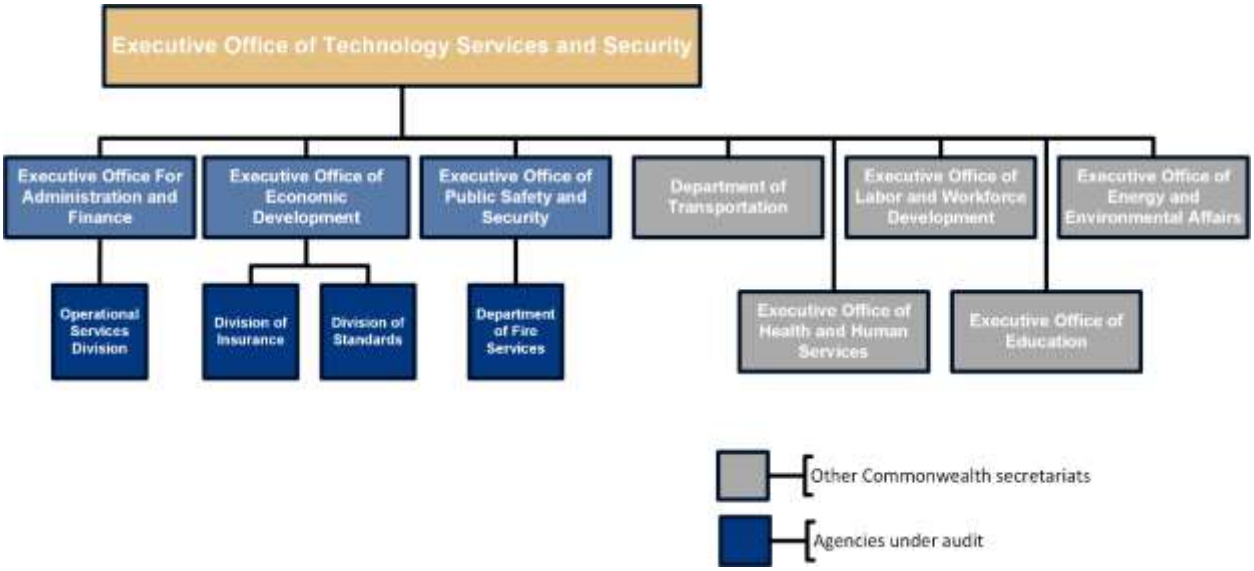
In 2018, W3C published WCAG 2.1, which built on WCAG 2.0 to improve web accessibility on mobile devices and to further improve web accessibility for people with visual impairments and cognitive disabilities. EOTSS published the Enterprise Information Technology Accessibility Policy in 2021 to meet Levels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

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



While EOTSS establishes standards for executive branch agencies, individual agencies, such as DFS, 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]



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, 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.
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

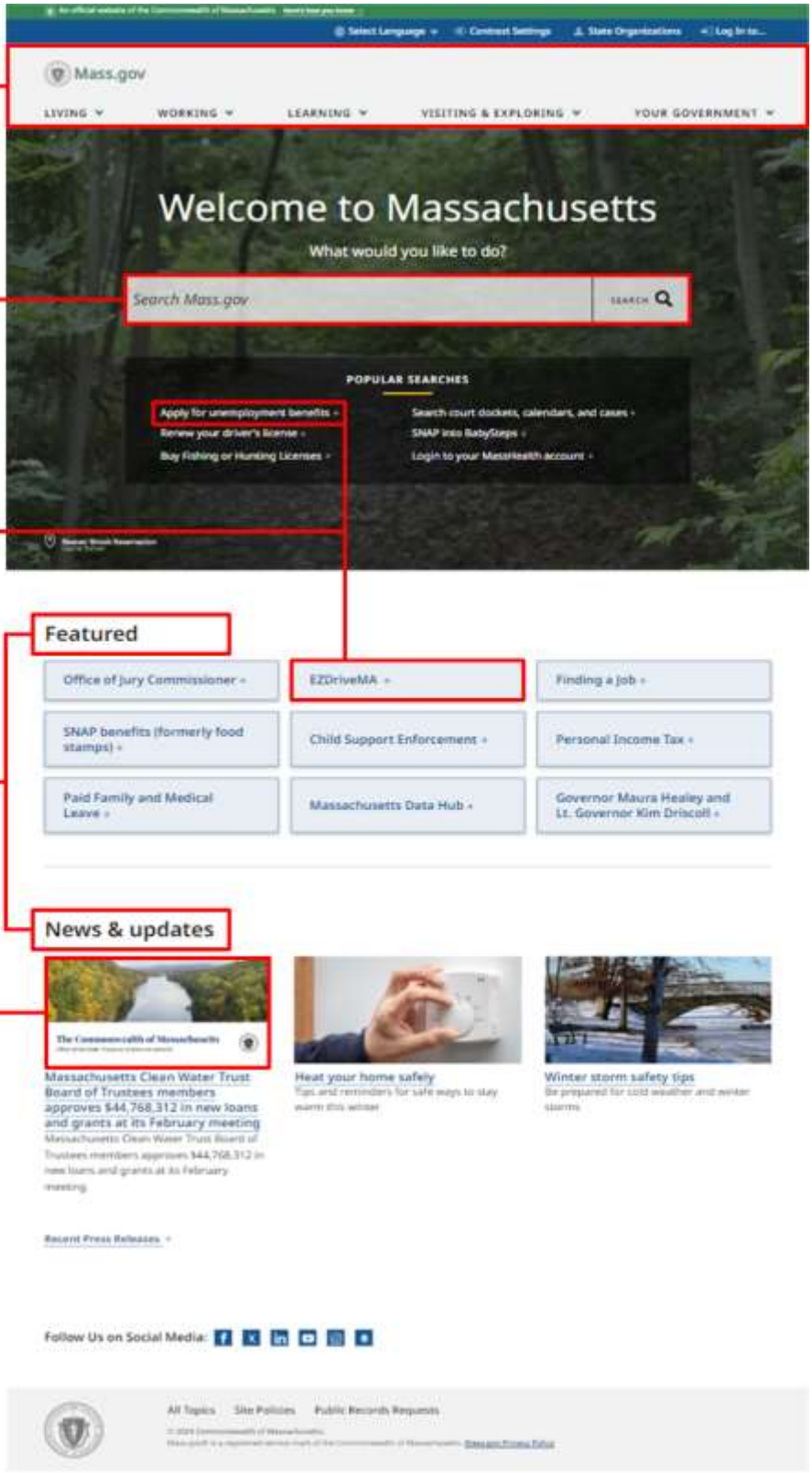
A site's header can appear throughout an entire site and contain links to main content areas.

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 Department of Fire Services (DFS) 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 DFS'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?	**Partially; see Finding 1**
2. Did DFS establish information technology (IT) governance policies and procedures for 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, 3, and 4**

To achieve our audit objectives, we gained an understanding of DFS's internal control environment related to the objectives by reviewing applicable policies and procedures and by interviewing DFS 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 DFS'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 60 out of a total of 972 DFS 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 to help users locate content.
- We determined whether related hyperlinks allowed users to navigate to the intended webpages.

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 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 DFS's website.

IT Governance

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

Business Continuity and Disaster Recovery

To determine whether DFS'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 DFS employees and inspected DFS's business continuity plan to ensure that it addressed the following: critical business processes, DFS'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 DFS'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 DFS employees and inspected DFS'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 employees facility access 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 DFS's business continuity plan.

Information Security Incident Response Plan and Procedures

To determine whether DFS'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 DFS employees and requested DFS's information security incident response plan and procedures. We learned that DFS relied on the Executive Office of Public Safety and Security for an information security incident response plan and procedures, so we inspected the Executive Office of Public Safety and Security's information security incident response plan and procedures to determine whether they met the requirements of the aforementioned EOTSS policy.

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

Cybersecurity Awareness Training

To determine whether DFS'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 5 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 20 out of a population of 93 employees who had been employed by DFS 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.

See Finding 4 for an issue we identified with DFS's cybersecurity awareness training.

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 DFS management, we interviewed knowledgeable DFS employees 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 DFS site map and traced them to the corresponding webpage on DFS's website, checking that each URL and page title matched the information on the DFS website. We also selected a random sample of 20 URLs from DFS'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 DFS 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 20 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 20 employees from CTHRU and traced their names back to the employee list to ensure that we received a complete and accurate employee list from DFS.

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.

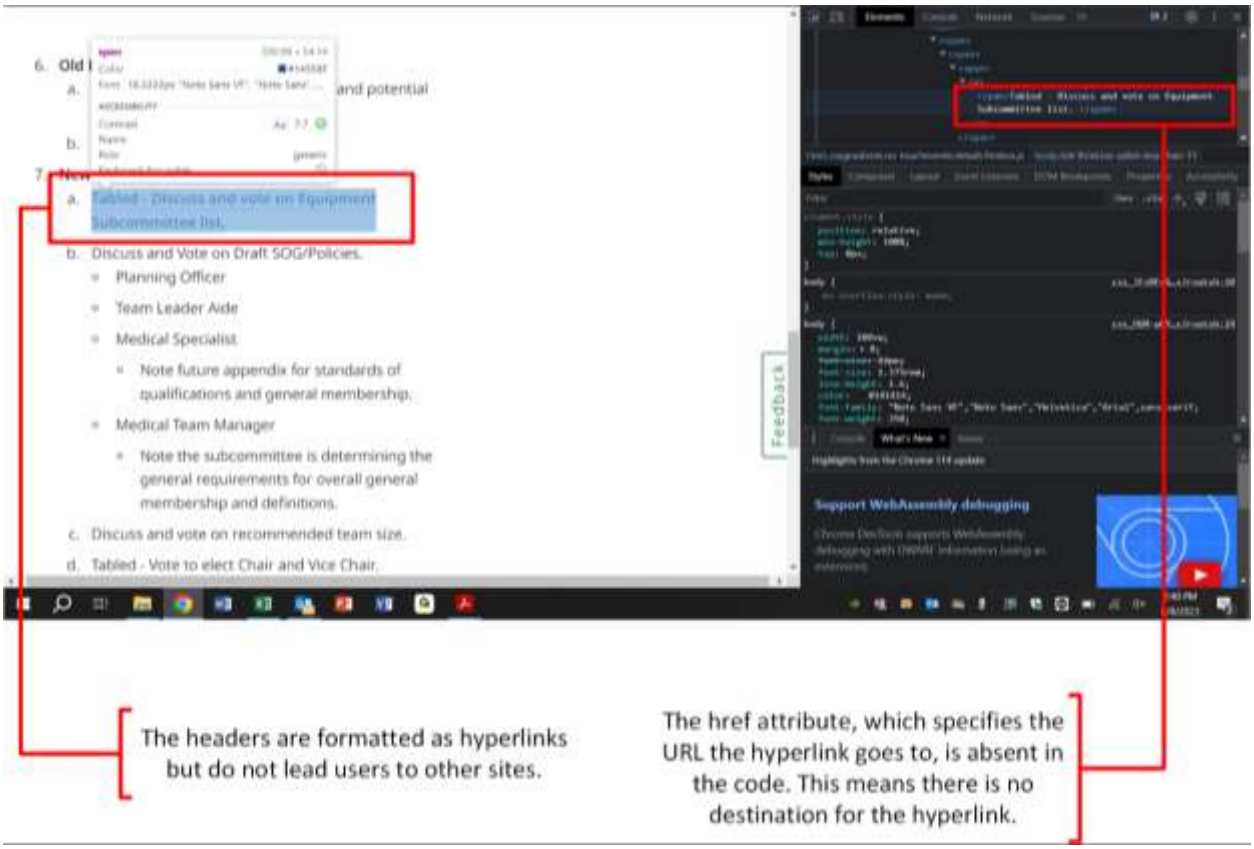
5. A URL uniquely identifies an internet resource, such as a website.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Department of Fire Services' website is not fully accessible for all Massachusetts residents.

Some of the Department of Fire Services' (DFS's) webpages do not comply with state information technology (IT) accessibility standards for navigation accessibility. During our audit, we determined that 1 out of the 60 DFS webpages we tested contained a hyperlink that did not allow users to navigate to the intended page (i.e., a broken or faulty hyperlink).

Broken or faulty hyperlinks negatively impact the user experience and make it difficult to locate additional relevant information. (See the example below.) They can also limit some users from having equitable access to critical information and key online services offered by DFS (e.g., proper fire safety equipment use or how to be prepared for fire emergencies). 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,

> *In order to implement the various requirements of The Rehabilitation Act of 1973, the Americans with Disabilities Act of 1990, the Commonwealth Constitution, [Section 3 of Chapter 7D of the Massachusetts General Laws], Commonwealth of Massachusetts Executive Order 348, and other applicable obligations, EOTSS establishes the following IT Accessibility Standards.*
>
> 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

DFS management stated that the broken hyperlink was the result of a formatting error that occurred when the original content was copied from a word processing document and pasted into a text box on their content management platform.

Recommendation

DFS 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 DFS to all Commonwealth residents.

Auditee's Response

> *The issue in question was not a broken hyperlink and did not prevent any website user from accessing any web page or information. DFS acknowledges that an HTML formatting error caused plain text to appear as a hyperlink. DFS staff corrected this formatting error immediately upon learning of it. In addition to reviewing DFS webpages for broken links, which is done on a regular basis, staff are now reviewing new content for formatting errors such as the one identified here.*

Auditor's Reply

Based on its response, DFS has taken measures to address our concerns on this matter.

2. The Department of Fire Services did not update its business continuity plan.

DFS did not update its business continuity plan in 2021.

Without an updated business continuity plan, DFS cannot ensure that it has procedures for protecting information assets or a plan to recover critical operations when an interruption or disaster occurs. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect DFS's ability to accomplish its mission. Additionally, an updated business continuity plan would help DFS respond adequately to unplanned business disruptions like the COVID-19 pandemic.

Authoritative Guidance

Section 6.1.1.4.3 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005 states that business continuity plans "shall be updated whenever a major organizational change occurs or at least annually, whichever comes first."

Reasons for Issue

DFS management stated that it did not update its business continuity plan in 2021 because of disruptions from the COVID-19 pandemic.

Recommendation

DFS should update its business continuity plan annually and whenever a major organizational change occurs.

Auditee's Response

> *The DFS Continuity of Operations Plan (COOP) was implemented and successfully utilized throughout the COVID-19 pandemic. DFS is in the process of updating the COOP plan and will ensure that it is updated annually and whenever a major organizational change occurs.*

Auditor's Reply

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

3. The Department of Fire Services 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 DFS relies on do not include guidance for implementing corrective actions or post-incident analysis, criteria for business recovery, data backup processes, or an analysis of legal requirements for reporting IT system compromises.

Without an adequate information security incident response plan and procedures, DFS 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

DFS management stated that the Executive Office of Public Safety and Security and EOTSS handle DFS's information security incident response management functions.

Recommendation

DFS should rely on an information security incident response plan and procedures that include all required elements. Alternatively, DFS 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

The Department of Fire Services currently follows the Executive Office of Public Safety & Security (EOPSS) established process for reporting incidents through the [Secretariat Chief Information Officer], [Chief Information Security Officer] and to the EOTSS Security Operations Center. DFS will continue to collaborate with EOPSS and develop a DFS supplemental plan which will complement the secretariat-wide standards, and which will identify Information Security Response actions and procedures specific to DFS.

Auditor's Reply

While we acknowledge that EOTSS (as the oversight agency) plays a role in ensuring that DFS has a sufficient information security incident response plan, DFS 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 DFS, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DFS is taking measures to address our concerns on this matter.

4. The Department of Fire Services did not provide its contractors with cybersecurity awareness training.

DFS did not provide its contractors with cybersecurity awareness training for the 2021–2022 training cycle.

Contractors make up approximately 87% of the DFS workforce. A lack of cybersecurity awareness training for these contractors may lead to user error or compromise the integrity and security of protected information in DFS's IT systems.

Authoritative Guidance

EOTSS's Information Security Risk Management Standard IS.010 states,

> *6.2 Information Security Training and Awareness*
>
> *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.*
>
> *6.2.1 Implement an enterprise-wide information security awareness and training program.*
>
> *6.2.1.1 Develop appropriate training materials in collaboration with Human Resources and Legal.*
>
> *6.2.1.2 Conduct periodic refresher training for* ***personnel*** *and, where relevant, contractors and temporary staff.*

Reasons for Issue

DFS management stated that contractors were not given access to the training platform it uses, Mass Achieves, during the 2021–2022 mandatory training session. They stated that Mass Achieves did not have access solutions for contractors to complete this training.

Recommendations

1. DFS should ensure that its contractors complete cybersecurity awareness training.
2. DFS should ensure that its contractors have access to its cybersecurity awareness training platform.

Auditee's Response

DFS has always required contract employees to participate in Cyber Security Awareness Training, which has historically been delivered through a 3rd party on-line platform launched and managed by the Executive Office of Technology Services and Security. In [fiscal year (FY)] 2022, the on-line training was launched by the Human Resources Division (HRD) via a new statewide employee training platform called Mass Achieve. In FY 2022, HRD was not able to provide Mass Achieve access for contract employees statewide, not limited to just DFS, and therefore contract employees were not required to take the training. In FY 2023, HRD was able to provide all statewide contract employees with access to Mass Achieve and the DFS contract employees completed all mandatory training. DFS continues to ensure that all contract employees attain access to the training platform and complete mandatory training within 30 days of hire, and annually thereafter.

Auditor's Reply

While we acknowledge that EOTSS (as the oversight agency) plays a role in ensuring that DFS provides cybersecurity awareness training to its contractors, DFS must train contractors in compliance with EOTSS's Information Security Risk Management Standard IS.010. This is pursuant to Section 2 of Chapter 7D of the General Laws, which requires all state executive branch agencies, including DFS, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." Based on its response, DFS has taken measures to address our concerns on this matter.