OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued April 25, 2024

Operational Services Division

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

April 25, 2024

Gary Lambert, Assistant Secretary for Operational Services
Operational Services Division
1 Ashburton Place, Room 1608
Boston, MA 02108

Dear Mr. Lambert:

I am pleased to provide to you the results of the enclosed performance audit of the Operational Services Division. 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 Operational Services Division. 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

CUG	contract user guide
EOTSS	Executive Office of Technology Services and Security
IT	information technology
MBPO	master blanket purchase order
OSD	Operational Services Division
PO	purchase order
SWC	Statewide Contract
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 Operational Services Division (OSD) for the period July 1, 2021 through December 31, 2022. In this performance audit, we determined the following:

- whether OSD's Mass.gov website met the accessibility standards established by the Executive Office of Technology Services and Security (EOTSS) and the Web Content Accessibility Guidelines (WCAG) 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility;
- whether OSD ensured that all contracts posted to its COMMBUYS website complied with EOTSS's Enterprise Information Technology Accessibility Policy and WCAG 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility; and
- whether OSD established information technology 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 22**	OSD's Mass.gov website is not fully accessible for all Massachusetts residents.
Recommendations **Page 25**	1. OSD should review its Mass.gov webpages to ensure that all hyperlinks lead to related information to provide equitable access to critical information and services offered online by OSD for all Massachusetts residents and state agencies. 2. OSD should ensure that content on its Mass.gov webpages displays clearly, even when zoomed up to 400%, resulting in a user experience that is inclusive of all Massachusetts residents and state agencies.
Finding 2 **Page 26**	OSD did not ensure that all of its hyperlinks within contract user guides (CUGs) led to related information.
Recommendation **Page 27**	OSD should regularly review its posted CUGs and ensure that hyperlinks within them are up-to-date and functional.
Finding 3 **Page 27**	OSD did not ensure that all contracts posted to COMMBUYS had a language tag.
Recommendations **Page 28**	1. OSD should ensure that all attached contract forms have a language tag. 2. OSD should establish criteria and user guides that include accessibility requirements for attached contract forms.

Finding 4 **Page 29**	OSD did not ensure that its COMMBUYS website provided correction suggestions.
Recommendations **Page 30**	1. OSD should ensure that all fields on its webpages properly identify errors when a user inputs an incorrect data type into an entry field. 2. OSD should ensure that it provides correction suggestions when a user inputs an incorrect data type into an entry field.
Finding 5 **Page 30**	OSD relies on an information security incident response plan and procedures that do not include all required elements.
Recommendation **Page 32**	OSD should establish information security incident response procedures for implementing corrective action or post-incident analysis, criteria for business recovery, data backup processes, and an analysis of legal requirements for reporting information technology system compromises.
Finding 6 **Page 32**	OSD does not have a business continuity plan or a disaster recovery plan.
Recommendations **Page 33**	1. OSD should develop, document, and test a business continuity plan. 2. OSD should develop, document, and test a disaster recovery plan for both onsite and offsite recovery locations.

OVERVIEW OF AUDITED ENTITY

In 1996, the former Department of Procurement and General Services was restructured and renamed the Operational Services Division (OSD). Section 4A of Chapter 7 of the Massachusetts General Laws created OSD and placed it within the Executive Office for Administration and Finance. The secretary of the Executive Office for Administration and Finance appoints a state purchasing agent, who serves as the administrative head of OSD.

Section 4A of Chapter 7 of the General Laws establishes the following as the basic functions of OSD:

- to manage and assist in the acquisition of goods, equipment, and services for executive branch agencies;
- to administer a collective purchasing program from third-party vendors for the Commonwealth and its political subdivisions (e.g., counties and municipalities);
- to offer copying and printing services for state and municipal governments and agencies and other eligible entities (e.g., qualified nonprofit organizations);
- to manage the use and maintenance of vehicles owned by executive branch agencies;
- to administer state and federal surplus property programs in which OSD sells unneeded government equipment and supplies to the public;
- to administer the Supplier Diversity Office, established under OSD by Chapter 56 of the Acts of 2010, to help businesses owned by people of color, women, and veterans obtain contracts, subcontracts, and financing to sell goods and services to the Commonwealth and its political subdivisions; and
- to establish the Bureau of Purchased Services, according to Section 22N of Chapter 7 of the General Laws, which reviews independent audit reports regarding financial statements and compliance supplements submitted by human service providers (e.g., special education, mental health, and elder services program providers) and the providers' public accountants.

Additionally, OSD uses COMMBUYS as a web-based procurement platform for Commonwealth agencies and political subdivisions. COMMBUYS allows public buyers[1] to post bid solicitations,[2] enter into contracts with vendors for goods and services, and make purchases on new and existing contracts. COMMBUYS also

[1] Public buyers include state executive branch agencies, Massachusetts cities and towns, public school districts, housing authorities, and public higher education groups.

[2] A bid solicitation (which is also known as a request for responses or a bid) is an invitation for vendors to offer prices on fulfilling contracts. For existing contracts, this is known as a request for a quote. COMMBUYS uses these terms interchangeably.

allows vendors to post quotes in response to bid solicitations. OSD maintains the platform's website, qualifies vendors, negotiates prices, and provides training and support to vendors and other users.

OSD is located at 1 Ashburton Place in Boston and had 110 full-time employees as of December 31, 2022. OSD's main sources of revenue are fees imposed on contractors and fees for services that OSD provides to different state agencies. In fiscal year 2022, OSD had a budget of $11,555,197 and generated $27,120,000 in revenue. OSD received state appropriations, which totaled $8,463,465 in fiscal year 2022, for capital improvements—such as purchasing and repairing state vehicles and improving its computer systems—and other purposes.

COMMBUYS Procurement Process

Public buyers can procure goods and services on COMMBUYS through either a Statewide Contract (SWC) or a limited-use contract, if no applicable SWC exists.

SWCs

In certain instances, OSD enters into contracts with multiple vendors to provide a specific good or service that can be used by multiple executive branch agencies or other public buyers. OSD established the Strategic Sourcing Services Unit to manage and oversee the procurements for these contracts. These contracts are called SWCs and provide access to a variety of goods or services— such as fuel, medical supplies, actuarial services, and office supplies—to meet the needs of public buyers.

If an executive branch agency requires a good or service provided by an SWC, the agency must use the SWC for procurement. All other Commonwealth agencies, including constitutional offices, public authorities, commissions, and cities and towns, may also use SWCs to procure goods and services, but they are not required to do so.

After OSD awards a contract to a vendor, OSD's Strategic Sourcing Services Unit creates a master blanket purchase order (MBPO), which is a type of purchase order (PO) that acts as a contract under which public buyers can make multiple purchases over the life of the contract. Following this, the Strategic Sourcing Services Unit creates a contract user guide (CUG), which details the types of goods or services on the contract, provides instructions for making purchases, and includes information about the contracted vendor. The Strategic Sourcing Services Unit posts the MBPO and CUG on COMMBUYS and Mass.gov.

If COMMBUYS users wish to procure goods or services from an SWC, they must first consult the associated CUG because different contracts will have different terms. For example, some SWCs require buyers to request quotes (which are offers to provide the goods or services outlined in the bid solicitation at a certain price) from vendors listed on the CUG, some allow buyers to directly issue requisitions to the vendor, and some require buyers to request quotes only if the engagement exceeds a certain dollar threshold.

Public buyers make SWC purchases under an MBPO and document the purchase in COMMBUYS with a requisition number and a release PO, which are unique to each purchase.

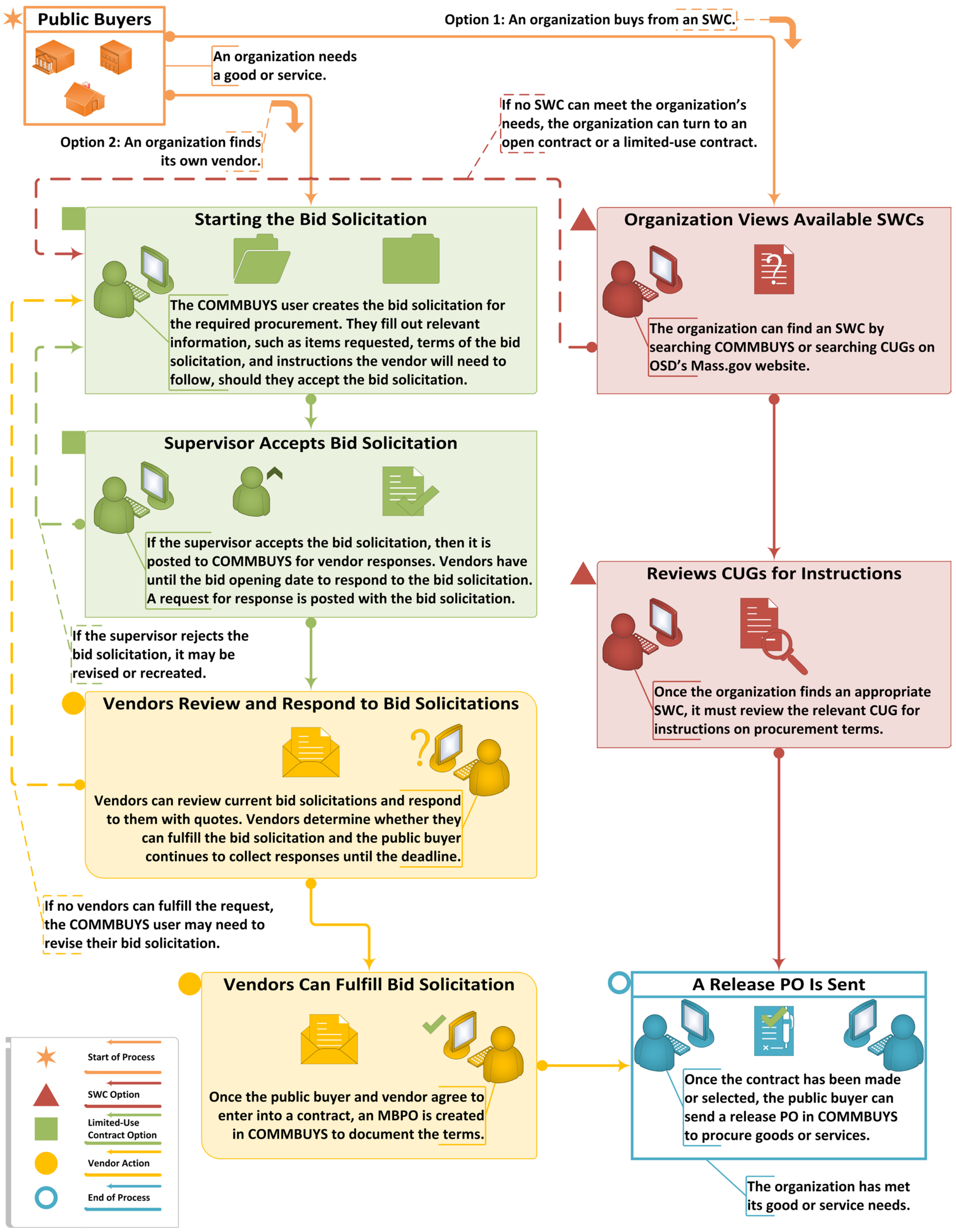
Limited-Use Contracts

If a public buyer’s need cannot be fulfilled by an SWC, they can also use COMMBUYS to create a limited-use contract. The public buyer uses COMMBUYS to create a bid solicitation. Public buyers create bid solicitations in COMMBUYS by entering data into predetermined fields and attaching any necessary documentation to the posting.

Once a public buyer posts a bid solicitation in COMMBUYS, vendors can respond to it and create quotes directly in COMMBUYS by entering data into predetermined fields.

Public buyers use COMMBUYS to create requisitions for limited-use contracts similarly to how public buyers use the platform for SWCs. Goods or services procured under a limited-use contract are documented in COMMBUYS with an MBPO. The public buyer often attaches to the MBPO standard contract forms (which are PDF templates provided by the Office of the Comptroller of the Commonwealth) to document additional contract terms.

COMMBUYS Procurement Process



Public Buyers

An organization needs a good or service.

Option 1: An organization buys from an SWC.

Option 2: An organization finds its own vendor.

If no SWC can meet the organization's needs, the organization can turn to an open contract or a limited-use contract.

Starting the Bid Solicitation

The COMMBUYS user creates the bid solicitation for the required procurement. They fill out relevant information, such as items requested, terms of the bid solicitation, and instructions the vendor will need to follow, should they accept the bid solicitation.

Organization Views Available SWCs

The organization can find an SWC by searching COMMBUYS or searching CUGs on OSD's Mass.gov website.

Supervisor Accepts Bid Solicitation

If the supervisor accepts the bid solicitation, then it is posted to COMMBUYS for vendor responses. Vendors have until the bid opening date to respond to the bid solicitation. A request for response is posted with the bid solicitation.

If the supervisor rejects the bid solicitation, it may be revised or recreated.

Reviews CUGs for Instructions

Once the organization finds an appropriate SWC, it must review the relevant CUG for instructions on procurement terms.

Vendors Review and Respond to Bid Solicitations

Vendors can review current bid solicitations and respond to them with quotes. Vendors determine whether they can fulfill the bid solicitation and the public buyer continues to collect responses until the deadline.

If no vendors can fulfill the request, the COMMBUYS user may need to revise their bid solicitation.

Vendors Can Fulfill Bid Solicitation

Once the public buyer and vendor agree to enter into a contract, an MBPO is created in COMMBUYS to document the terms.

A Release PO Is Sent

Once the contract has been made or selected, the public buyer can send a release PO in COMMBUYS to procure goods or services.

The organization has met its good or service needs.

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 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 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.

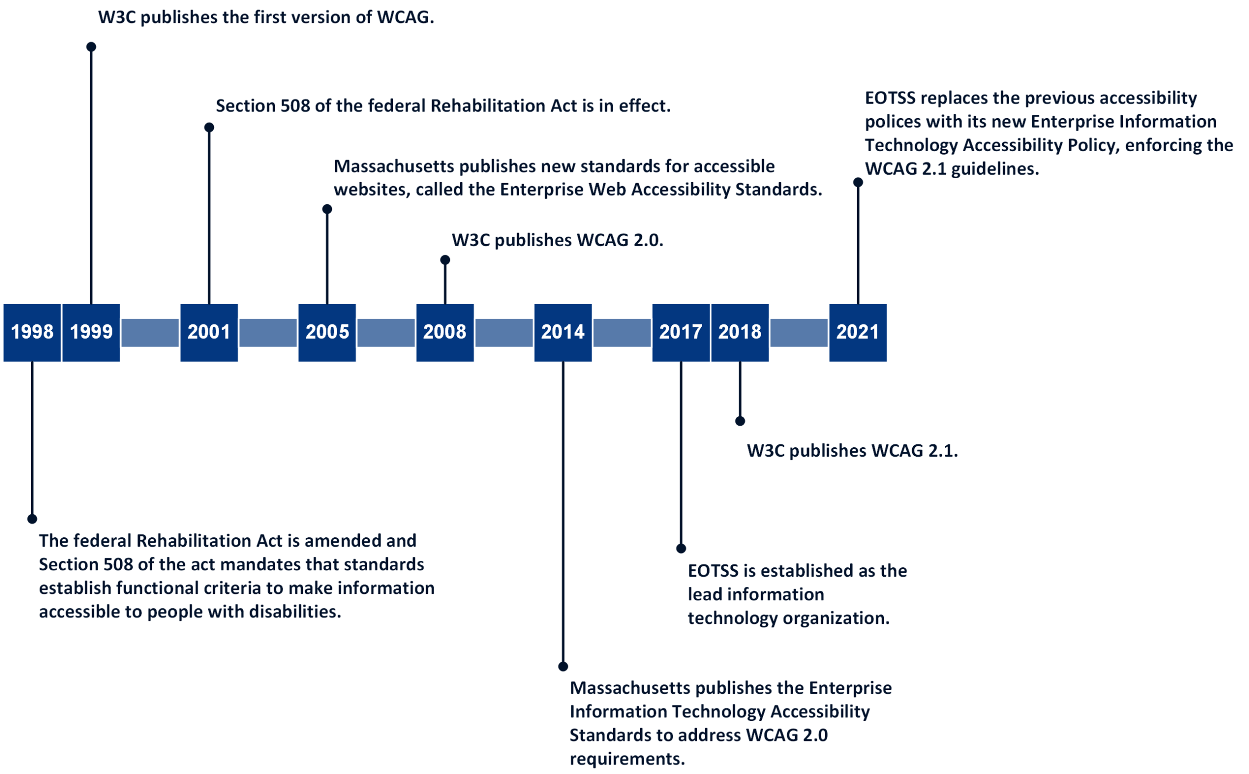
In 2008, W3C published WCAG 2.0. In 2014, the Massachusetts Office of Information Technology added a reference to WCAG 2.0 in its Enterprise Information Technology Accessibility Standards.

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 branch 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.

[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.

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.

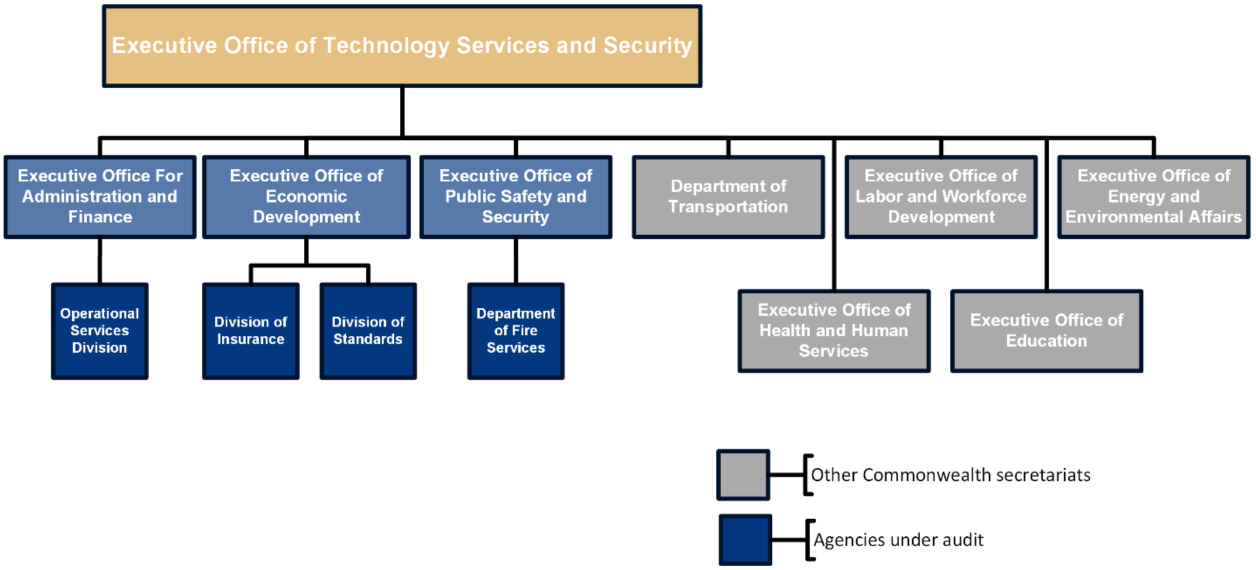
2017: EOTSS is established as the lead information technology organization.

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 OSD, 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]


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[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 Internet

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 Office of the State Auditor also audited the Division of Insurance, Department of Fire Services, and Division of Standards. These audits are separate and the reports can be found on the Office of the State Auditor's website.

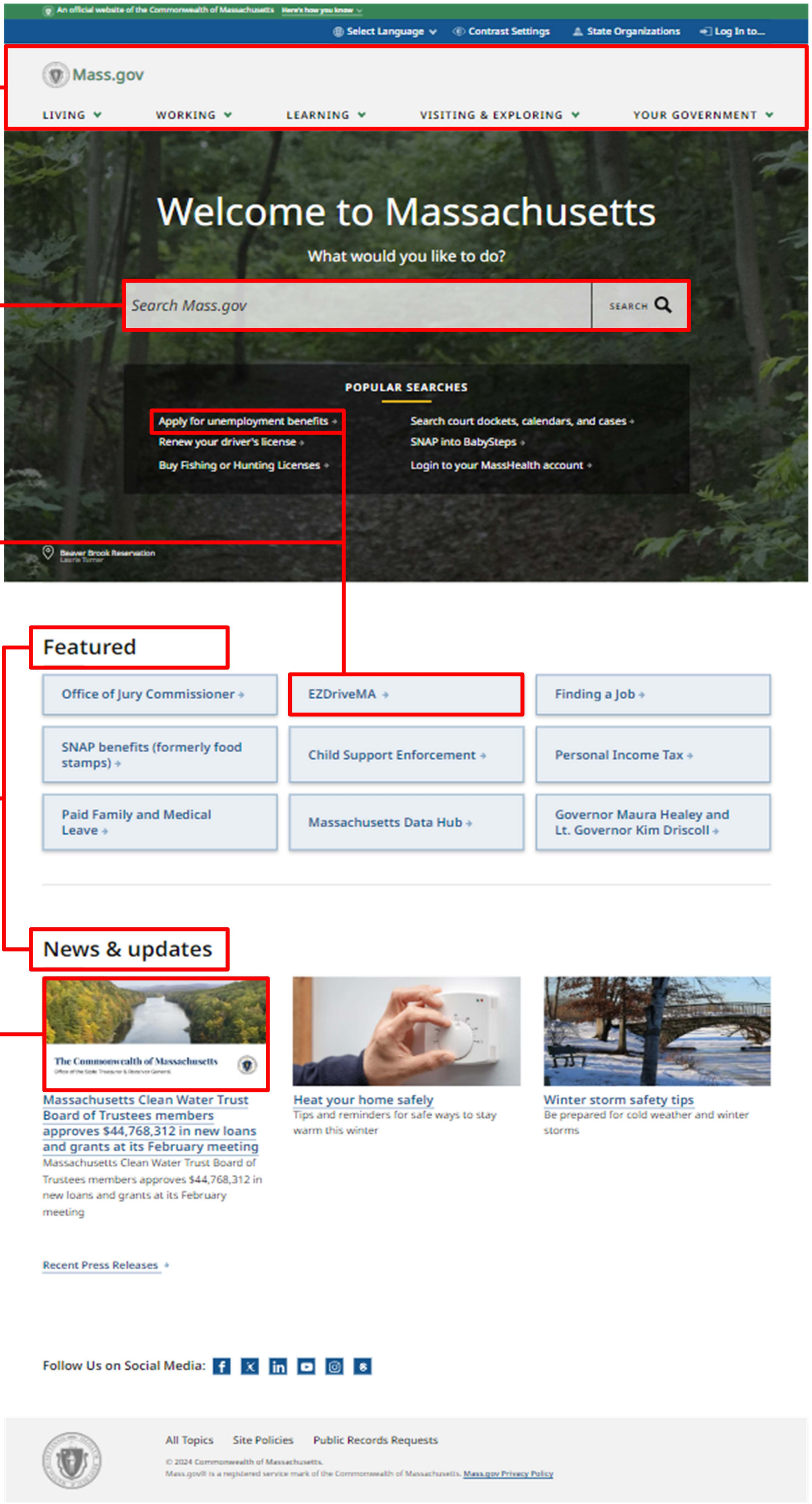
[5] Deloitte is an international company that provides tax, accounting, and audit services to businesses and government agencies.

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 that people with disabilities employ to enhance their web interaction.[6] These strategies might involve increasing text size, adjusting mouse speed, or enabling captions.

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

[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



An official website of the Commonwealth of Massachusetts Here's how you know

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

Beaver Brook Reservation
Laurie Turner

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

The Commonwealth of Massachusetts

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

Recent Press Releases

Follow Us on Social Media:

All Topics Site Policies Public Records Requests

© 2024 Commonwealth of Massachusetts.
Mass.gov® is a registered service mark of the Commonwealth of Massachusetts. Mass.gov Privacy Policy

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 branch agencies adopt 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 course every year. All newly hired employees must complete an initial security awareness training course 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 Operational Services Division (OSD) 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 OSD's Mass.gov website comply with 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 OSD ensure that all contracts posted to its COMMBUYS website complied with EOTSS's Enterprise Information Technology Accessibility Policy and WCAG 2.1 for user accessibility, keyboard accessibility, navigation accessibility, language, error identification, and color accessibility?	**No; see Findings 2, 3, and 4**
3. Did OSD 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 5 and 6**

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

To obtain sufficient, appropriate evidence to address our audit objectives, we performed the following procedures.

Web Accessibility

To determine whether OSD's Mass.gov website met 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 35 out of a total of 189 OSD Mass.gov webpages in the audit population. We performed the following procedures on the sampled webpages.

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[7] 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.

[7] An element is a part of a webpage that contains data, text, or an image.

Language

- We determined whether words that appeared on the webpage matched the language tag[8] to which the webpage was set by examining its properties.

- 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 regarding hyperlinks on OSD's Mass.gov website.

Contract Accessibility

To determine whether contracts posted to OSD's COMMBUYS website met 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 inspected a random, nonstatistical sample of 40 unique purchase orders (POs) out of a population of 364.[9]

We also inspected statistical samples of 60 bid solicitations out of a population of 13,897 and 60 master blanket purchase orders (MBPOs) out of a population of 3,413, using a 95% confidence level, a 0% expected error rate, and a 5% tolerable error rate.

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

[9] We arrived at this population by examining unique PO numbers to avoid testing a sample that included duplicate PO numbers (i.e., that included a PO with multiple requisitions). This resulted in a smaller, more diverse population of contracts that did not skew toward contracts that appeared multiple times.

- The 60 MBPOs in our sample contained references to 25 CUGs. Of these 25 CUGs, 10 were no longer in use at the time of our audit and 4 appeared twice. This gave us a total population of 11 unique CUGs that we tested for accessibility, as described below.

- Of the 60 MBPOs in our sample, 40 MBPOs contained attached contract forms. Of these 40 MBPOs, 24 contained one attached contract form and 16 contained multiple contract forms. This gave us a total of 71 unique attached contract forms that we tested for accessibility, as described below.

Additionally, to determine whether the processes for bid solicitation creation, quote creation, and PO creation related to Statewide Contracts (SWCs) met 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 inspected all 30 webpages available on COMMBUYS (12 related to the bid solicitation creation process, 8 related to the quotes creation process, and 10 related to creating POs from SWCs). We performed the following procedures on the preceding samples.

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 or PDF matched the language tag to which the webpage or PDF was set by examining its properties.

- 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.

See Findings 2, 3, and 4 for issues we identified regarding CUGs, attached contract forms, and the COMMBUYS bid solicitation and purchase creation processes.

IT Governance

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

Information Security Incident Response Plan and Procedures

To determine whether OSD'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 OSD staff members and requested OSD's information security incident response plan and procedures. We learned that OSD relies on its secretariat agency, the Executive Office for Administration and Finance, for an information security incident response plan and procedures, so we inspected the Executive Office for Administration and Finance's information security incident response plan and procedures to determine whether they complied with the aforementioned EOTSS policy.

See Finding 5 for an issue we identified regarding OSD's information security incident response plan and procedures.

Business Continuity and Disaster Recovery

To determine whether OSD'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 OSD staff members and inspected OSD's business continuity plan to ensure that it addressed the following: critical business processes, manual and automated processes used by the agency, 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 OSD's disaster recovery plan complied with Section 6.2.1 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, we interviewed knowledgeable OSD staff members and inspected OSD'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 6 for an issue we identified regarding OSD's business continuity plan.

Cybersecurity Awareness Training

To determine whether OSD'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 a random sample of 15 out of a total population of 48 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 20 out of a total population of 60 employees to determine whether they completed the annual refresher cybersecurity awareness training.

We noted no exceptions in our testing; therefore, we conclude that, during the audit period, OSD 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 a combination of statistical and nonstatistical sampling methods for testing and 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 we received from OSD management, we interviewed knowledgeable OSD staff members 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)[10] that could be accessed independently from the OSD site map and traced them to the corresponding webpage, checking that each URL and page title matched the information on OSD's Mass.gov website. We also selected a random sample of 20 URLs from OSD's Mass.gov 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.

COMMBUYS Data

To assess the reliability of the COMMBUYS lists of MBPOs, POs, and bid solicitations that we received from OSD, 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 hidden rows or columns, and that all MBPOs, POs, and bid solicitations in the data set were active during the audit period. We then selected random samples of 20 each of MBPOs, POs, and bid solicitations from the appropriate lists and traced them to the COMMBUYS website. Additionally, we selected random

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

samples of 20 each of MBPOs, POs, and bid solicitations from COMMBUYS and traced them to our lists of MBPOs, POs, and bid solicitations.

IT Governance Testing

To determine the reliability of the employee list we received from OSD 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 OSD 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, the COMMBUYS data lists, and the employee list were sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

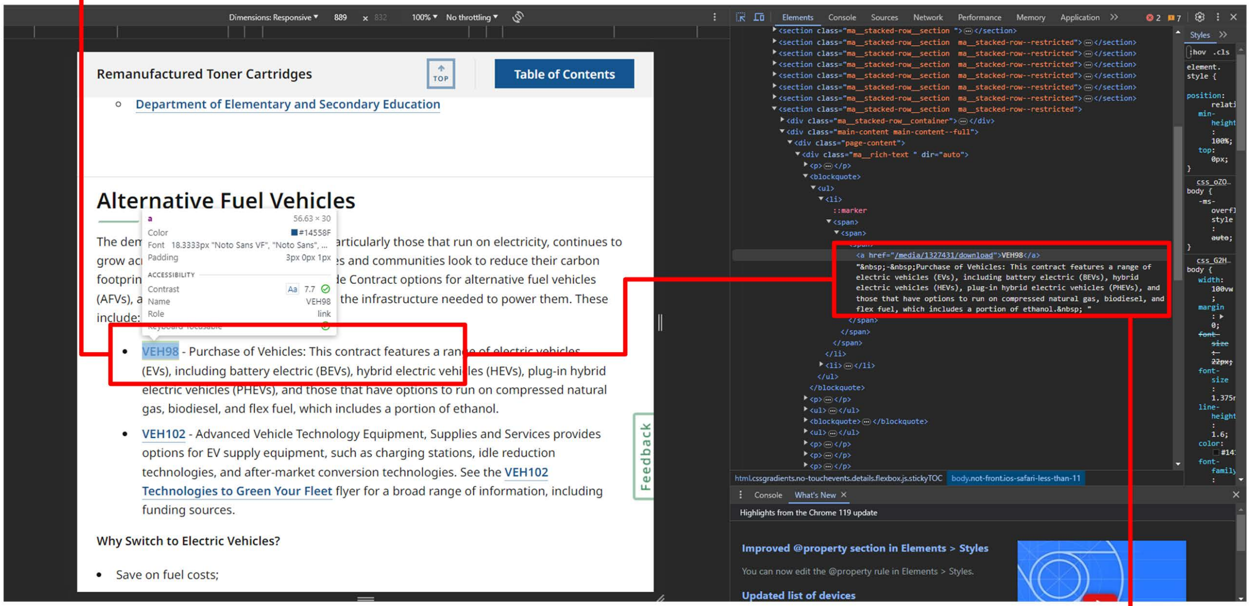
1. The Operational Services Division's Mass.gov website is not fully accessible for all Massachusetts residents.

Some of the Operational Services Division's (OSD's) Mass.gov webpages do not comply with state information technology (IT) accessibility standards for navigation accessibility and content display. We determined that 11 out of the 35 OSD mass.gov webpages tested contained hyperlinks that did not allow users to navigate to related pages (i.e., broken and faulty hyperlinks). For display testing, we determined that 1 out of the 35 OSD Mass.gov webpages we tested did not display content correctly when zoomed to 400%.

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 OSD. Specifically, these hyperlinks could increase the likelihood that residents will access outdated or incorrect information or will be directed to webpages that no longer exist.

The hyperlink is supposed to redirect the user to a file download.



Remanufactured Toner Cartridges

- Department of Elementary and Secondary Education

Alternative Fuel Vehicles

The dem… articularly those that run on electricity, continues to grow ac… es and communities look to reduce their carbon footprin… de Contract options for alternative fuel vehicles (AFVs), a… the infrastructure needed to power them. These include:

a	56.63 × 30
Color	#14558F
Font	18.3333px "Noto Sans VF", "Noto Sans", ...
Padding	3px 0px 1px
ACCESSIBILITY	
Contrast	Aa 7.7 ✓
Name	VEH98
Role	link
Keyboard-focusable	✓

- VEH98 - Purchase of Vehicles: This contract features a range of electric vehicles (EVs), including battery electric (BEVs), hybrid electric vehicles (HEVs), plug-in hybrid electric vehicles (PHEVs), and those that have options to run on compressed natural gas, biodiesel, and flex fuel, which includes a portion of ethanol.
- VEH102 - Advanced Vehicle Technology Equipment, Supplies and Services provides options for EV supply equipment, such as charging stations, idle reduction technologies, and after-market conversion technologies. See the VEH102 Technologies to Green Your Fleet flyer for a broad range of information, including funding sources.

Why Switch to Electric Vehicles?

- Save on fuel costs;

```
<section class="ma__stacked-row__section ">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">…</section>
<section class="ma__stacked-row__section  ma__stacked-row--restricted">
  <div class="ma__stacked-row__container">…</div>
  <div class="main-content main-content--full">
    <div class="page-content">
      <div class="ma__rich-text " dir="auto">
        <p>…</p>
        <blockquote>
          <ul>
            <li>
              ::marker
              <span>
                <span>
                  <span>
                    <a href="/media/1327431/download">VEH98</a>
                    "&nbsp;-&nbsp;Purchase of Vehicles: This contract features a range of
                    electric vehicles (EVs), including battery electric (BEVs), hybrid
                    electric vehicles (HEVs), plug-in hybrid electric vehicles (PHEVs), and
                    those that have options to run on compressed natural gas, biodiesel, and
                    flex fuel, which includes a portion of ethanol.&nbsp; "
                  </span>
                </span>
              </span>
            </li>
            <li>…</li>
          </ul>
        </blockquote>
        <p>…</p>
        <ul>…</ul>
        <blockquote>…</blockquote>
        <ul>…</ul>
        <p>…</p>
        <p>…</p>
        <p>…</p>
```

```
element.style {
  position: relati
  min-height: 100%;
  top: 0px;
}
css_oZO…
body {
  -ms-overflow-style: auto;
}
css_G2H…
body {
  width: 100vw;
  margin: ▶ 0;
  ~~font-size: 22px;~~
  font-size: 1.375r
  line-height: 1.6;
  color: #14
  font-family:
```

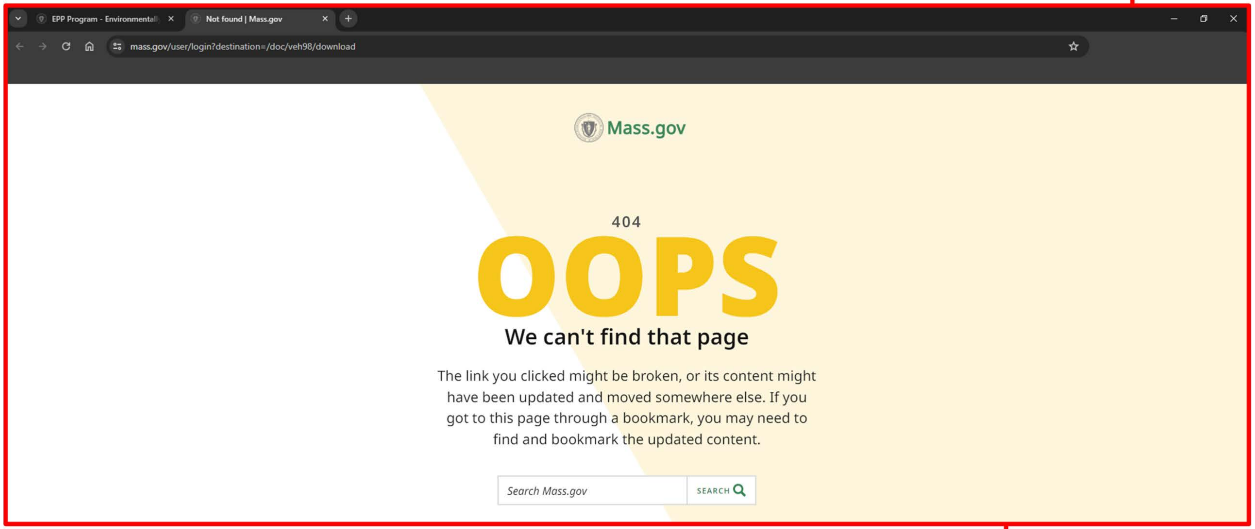
html.cssgradients.no-touchevents.details.flexbox.js.stickyTOC body.not-front.ios-safari-less-than-11

Highlights from the Chrome 119 update

Improved @property section in Elements > Styles

You can now edit the @property rule in Elements > Styles.

Updated list of devices



mass.gov/user/login?destination=/doc/veh98/download

404

OOPS

We can't find that page

The link you clicked might be broken, or its content might have been updated and moved somewhere else. If you got to this page through a bookmark, you may need to find and bookmark the updated content.

Search Mass.gov

However, the redirect link brings the user to a 404 error page, which indicates that the content cannot be found.

Navigation Accessibility: Content Display

If content does not display correctly (e.g., in a single column) when a user zooms or enlarges the content on a webpage, users may not be able to read the content without additional assistive technology that they may not typically need.

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 (WCAG) 2.1 states,

> *Success Criterion 1.4.10 Reflow*
>
> *(Level AA)*
>
> *Content can be presented without loss of information or functionality, and without requiring scrolling in two dimensions [i.e., in more than one column] for:*
>
> - *Vertical scrolling content at a width equivalent to 320 [cascading style sheet (CSS)] pixels;*
> - *Horizontal scrolling content at a height equivalent to 256 CSS pixels.*
>
> *Except for parts of the content which require two-dimensional layout for usage or meaning. . . .*
>
> *Note: 320 CSS pixels is equivalent to a starting viewport width of 1280 CSS pixels wide at 400% zoom. For web content which is designed to scroll horizontally (e.g. with vertical text), the 256 CSS pixels is equivalent to a starting viewport height of 1024 [pixels] at 400% zoom. . . .*
>
> *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

OSD told us that the hyperlinks were broken or faulty because certain webpages became defunct and others changed domains. The content display issue occurred because OSD chose a webpage template that did not display enlarged text in one column.

Recommendations

1. OSD should review its Mass.gov webpages to ensure that all hyperlinks lead to related information to provide equitable access to critical information and services offered online by OSD for all Massachusetts residents and state agencies.
2. OSD should ensure that content on its Mass.gov webpages displays clearly, even when zoomed up to 400%, resulting in a user experience that is inclusive of all Massachusetts residents and state agencies.

Auditee's Response

> *OSD maintains 473 pages on the mass.gov website. Those pages include numerous hyperlinks. OSD's web team monitors the broken links report regularly and fixes identified links immediately. As part of a recent redesign of OSD's mass.gov webpages, OSD recently conducted a comprehensive review of all OSD pages and fixed the broken links identified in that review. . . .*
>
> *EOTSS controls the appearance of webpages on Mass.gov. Individual agencies are provided with limited options for customization of their pages. It would be helpful if [the Office of the State Auditor] would identify the particular page so this issue should be brought to the attention of EOTSS so that EOTSS may review their templates and identify and correct any issues. Since the audit team identified only one page that failed the content display testing, OSD is hopeful that this issue is limited to a small number of available templates and can be easily corrected by EOTSS.*

Auditor's Reply

Section 2 of Chapter 7D of the Massachusetts General Laws requires all executive branch agencies, including OSD, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security." We acknowledge that EOTSS (as the oversight agency) plays a role in ensuring the accessibility of web content for executive branch agencies; however, the responsibility rests with OSD to ensure that IT solutions and web content are in compliance with EOTSS's Enterprise Information Technology Accessibility Policy. We provided the information on the testing exceptions we identified to OSD (specifically, the Environmentally Preferable Products Index webpage). Although EOTSS provides templates to agencies, it is OSD's responsibility to ensure that the content it displays using these templates is accessible.

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

2. The Operational Services Division did not ensure that all of its hyperlinks within contract user guides led to related information.

OSD did not ensure that all the hyperlinks within contract user guides (CUGs) for Statewide Contracts (SWCs) led to related information. Specifically, 3 of the 11 unique CUGs that we tested contained broken hyperlinks that did not lead to related information.

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 OSD as they relate to SWCs. Specifically, these hyperlinks could increase the likelihood that users will access outdated or incorrect information or will be directed to webpages that no longer exist.

Authoritative Guidance

The IT Accessibility Standards section of 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 WCAG 2.1 states,

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

Reasons for Issues

OSD told us that the hyperlinks were broken or faulty because certain webpages became defunct and others changed domains. Additionally, one of the hyperlinks was incorrectly linked to an OSD internal storage drive, meaning that the hyperlink destination was inaccessible to the public.

Recommendation

OSD should regularly review its posted CUGs and ensure that hyperlinks within them are up-to-date and functional.

Auditee's Response

> *OSD acknowledges this issue and will take steps to implement regular reviews of the contract user guides to identify and fix broken links. OSD is currently in the process of redesigning the contract user guides and will consider what can be incorporated in a new design to lessen issues with broken links.*

Auditor's Reply

Based on its response, OSD will take measures to address our concerns on this matter.

3. The Operational Services Division did not ensure that all contracts posted to COMMBUYS had a language tag.

OSD did not ensure that all contracts that public buyers posted to COMMBUYS had a language tag. Specifically, we determined that 57 of the 71 attached contract forms that we tested did not have language tags.

Readers who are visually impaired may be unable to use screen readers or other accessibility tools to read these documents if the documents do not have a language tag. In addition, without a language tag, a webpage translator cannot always identify the language in which the content is written, which could prevent it from accurately translating content into another language.

Authoritative Guidance

The IT Accessibility Standards section of 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 WCAG 2.1 state,

> *Success Criterion 3.1.1 Language of Page*
>
> *(Level A)*
>
> *The default human language of each Web page can be programmatically determined.*
>
> *Success Criterion 3.1.2 Language of Parts*
>
> *(Level AA)*
>
> *The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language, and words or phrases that have become part of the vernacular of the immediately surrounding text.*

Reasons for Issues

OSD has not established criteria and user guides that include accessibility requirements for attached contract forms.

Recommendations

1. OSD should ensure that all attached contract forms have a language tag.
2. OSD should establish criteria and user guides that include accessibility requirements for attached contract forms.

Auditee's Response

> *As the draft report notes, COMMBUYS is used by numerous state and local entities to post procurement bids and contract documents. Documents posted by other entities are records of those entities and OSD is not responsible for monitoring those records for compliance with accessibility standards. OSD respectfully asks [the Office of the State Auditor] to identify any non-compliant documents it identified that were posted by OSD so that OSD may correct those issues. OSD will incorporate into its training materials notices to COMMBUYS users that they should review their documents for compliance with applicable accessibility standards including use of language tags.*

Auditor's Reply

As part of our testing, we examined 71 standard contract forms, 9 of which were posted by OSD; 7 of those 9 did not have language tags. We provided the information related to these 7 forms to OSD (specifically, the signed forms for Eastern Communications, Haywood Associates, Infrastructure Ltd., Joe Warren and Sons Co. Inc., Royal Steam Heater Company, and Webb, as well as the interim form for Webb).

We agree that updated training material notices for COMMBUYS users will increase compliance with applicable accessibility standards. In addition to updating training materials, OSD should implement controls to ensure that materials posted by both OSD and COMMBUYS users comply with EOTSS accessibility standards. We further recommend that OSD periodically review these materials to ensure that they meet OSD's standards and applicable legal requirements.

4. The Operational Services Division did not ensure that its COMMBUYS website provided correction suggestions.

OSD did not ensure that all fields on its COMMBUYS website did the following two actions when a user input an incorrect data type into an entry field: properly identified errors and provided correction suggestions. Specifically, we found that on OSD's bid solicitation and purchase order (PO) creation webpage, the "accounting" section would fail to load (i.e., the screen went blank) when a user input text in fields that were meant for numbers.

Public buyers would not be able to properly enter information into the "accounting" section or know how to correct incorrect entries without correction suggestions. This means that users may not be able to complete the posting process and the Commonwealth may not have complete responses to bid solicitations from vendors.

Authoritative Guidance

The IT Accessibility Standards section of 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 WCAG 2.1 state,

> *Success Criterion: 3.3.3 Error Suggestion*
>
> *(Level AA)*
>
> *If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.*

Reasons for Issues

OSD told us that it was unaware of the error because public buyers infrequently use the "accounting" section of the COMMBUYS bid solicitation and PO creation webpages.

Recommendations

1. OSD should ensure that all fields on its webpages properly identify errors when a user inputs an incorrect data type into an entry field.

2. OSD should ensure that it provides correction suggestions when a user inputs an incorrect data type into an entry field.

Auditee's Response

> *As stated earlier in this response, OSD does not directly maintain the COMMBUYS webpage or application software. OSD acknowledges this issue and has taken steps to notify the vendor that maintains the site and system software. OSD has requested that the vendor analyze the issue and advise whether a fix can be provided.*

Auditor's Reply

While we acknowledge that OSD has taken steps to work with its vendor to remediate the issue, OSD is responsible for the applications that its vendors provide to the Commonwealth and, as such, is responsible for ensuring that those web-based applications, including COMMBUYS, comply with EOTSS's Enterprise Information Technology Accessibility Policy.

Based on its response, OSD will take measures to address our concerns on this matter.

5. The Operational Services Division 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 on which OSD relies 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, OSD cannot ensure that it takes sufficient containment measures when it identifies a security event and completes proper documentation, investigation, risk analysis, and 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

OSD management stated that its information security incident response management functions are handled by the Executive Office for Administration and Finance and EOTSS.

Recommendation

OSD should establish information security incident response procedures 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

> *As discussed with the audit staff, information security for OSD internal systems and applications is managed by [the Executive Office for Administration and Finance] staff embedded within OSD and information security for Commonwealth enterprise applications utilized by OSD staff is managed by EOTSS. However, OSD acknowledges that it does not have a written plan that is fully compliant with EOTSS's Information Security Incident Management Standard IS.009 and will develop a compliant written information security incident response plan.*

Auditor's Reply

We acknowledge that EOTSS and the Executive Office for Administration and Finance (as the oversight agency and secretariat agency, respectively) play a role in ensuring that OSD has a sufficient information security incident response plan and procedures. Nonetheless, OSD is required to develop an information security incident response plan that complies 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 executive branch agencies, including OSD, to "adhere to the policies, procedures, and objectives established by the executive office of technology services and security."

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

6. The Operational Services Division does not have a business continuity plan or a disaster recovery plan.

OSD does not have a business continuity plan or a disaster recovery plan to ensure the continuity of operations in the case of an interruption or disaster.

Without a business continuity plan or disaster recovery plan, OSD cannot ensure that it has established procedures for the continuation of critical business processes in the event of any organizational or information technology infrastructure failure. An interruption or disaster may result in lost or incorrectly processed data, creating financial losses, expensive recovery effects, and inaccurate or incomplete data. Additionally, if OSD is inoperable, statewide procurement may cease.

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] and risk assessment processes. . . .*
>
> *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

OSD management was unaware that they should develop and maintain business continuity and disaster recovery plans separate from the Executive Office for Administration and Finance's plan and EOTSS policies, procedures, and standards.

Recommendations

1. OSD should develop, document, and test a business continuity plan.
2. OSD should develop, document, and test a disaster recovery plan for both onsite and offsite recovery locations.

Auditee's Response

> *OSD acknowledges that it did not have a written plan that was fully compliant with EOTSS's Business Continuity and Disaster Recovery Standard IS.005. OSD did have an obsolete plan that has been reviewed and updated to comply with the EOTSS standards since the audit took place. OSD will make a copy available to the audit team upon request.*
>
> *OSD would like to note that it has always had procedures and systems in place to ensure that its operations continue in the case of infrastructure failures or disaster. OSD has demonstrated the ability to maintain operations during challenging circumstances. For example, OSD core functions continued with little to no disruption during the transition to remote work during the COVID-19 emergency. OSD also monitors the COMMBUYS website/application and is in constant communication with the vendor that maintains that system to ensure that it remains functioning and accessible to the user community.*

Auditor's Reply

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