OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued June 9, 2023

Committee for Public Counsel Services

For the period January 1, 2019 through December 31, 2021

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

June 9, 2023

Anthony Benedetti, Chief Counsel
Committee for Public Counsel Services
75 Federal Street, 6th Floor
Boston, MA 02110

Dear Mr. Benedetti:

I am pleased to provide to you the results of the enclosed performance audit of the Committee for Public Counsel Services. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, January 1, 2019 through December 31, 2021. 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 Committee for Public Counsel 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.

Sincerely,

Diana DiZoglio
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

COVID-19	2019 coronavirus
CPCS	Committee for Public Counsel Services
CTR	Office of the Comptroller of the Commonwealth
EOTSS	Executive Office of Technology Services and Security
ICP	internal control plan
IT	information technology
MMARS	Massachusetts Management Accounting and Reporting System

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 Committee for Public Counsel Services (CPCS) for the period January 1, 2019 through December 31, 2021. The objectives of this audit were to determine the following:

- whether CPCS employees received cybersecurity awareness training and whether employees signed acknowledgment forms regarding computer usage in accordance with Sections 6.2.3, 6.2.4, and 6.2.8 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010, effective October 15, 2018;
- whether CPCS updated its business continuity and disaster recovery plan in accordance with Section 6.1.1.4 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, effective October 15, 2018; and
- whether CPCS updated its internal control plan (ICP), as required by the Office of the Comptroller of the Commonwealth's "[2019 Coronavirus, or COVID-19] Pandemic Response Internal Controls Guidance."

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

Finding 1 **Page 11**	CPCS did not ensure that interns receive cybersecurity awareness training.
Recommendations **Page 11**	1. CPCS should require that interns receive cybersecurity awareness training. 2. CPCS should have a system to document the receipt of emails from interns who watch the cybersecurity awareness training video.
Finding 2 **Page 12**	CPCS did not have a business continuity and disaster recovery plan.
Recommendation **Page 12**	CPCS should develop, document, and test a business continuity and disaster recovery plan to implement.
Finding 3 **Page 14**	CPCS's ICP was not updated with a COVID-19 component.
Recommendation **Page 14**	CPCS should establish policies and procedures to ensure that its ICP is updated annually and when significant changes occur.

OVERVIEW OF AUDITED ENTITY

The Committee for Public Counsel Services (CPCS) was established by Chapter 673 of the Acts of 1983.

According to its website, CPCS is governed by a 15-member committee "appointed by the Governor, the Speaker of the House of Representatives, the President of the Senate, and the Massachusetts Supreme Judicial Court." The committee is responsible for planning, overseeing, and coordinating criminal and non-criminal legal services to people who cannot afford an attorney in the Commonwealth.

CPCS senior staff comprises the chief counsel, the director of administration and operations, the general counsel, the chief financial officer, the chief information officer, the chief human resources officer, the equity and inclusion director, and the communications director. In addition, the chief counsel is assisted by five deputy chief counsels, who oversee the legal divisions listed below.

CPCS is composed of five legal and five operations divisions. The legal divisions are Children and Family Law, Mental Health Litigation, Private Counsel, Public Defender, and Youth Advocacy. The operations divisions are Administration and Finance, General Counsel, Human Resource, Information Technology, and Training.

According to CPCS, in addition to the main office at 75 Federal Street in Boston, there are 20 regional offices in 17 communities[1] in the Commonwealth. During our audit period, CPCS had approximately 868 employees[2] and 16 unpaid interns.

There were 664,761 new cases assigned to CPCS public defenders and private attorneys in calendar years 2019, 2020, and 2021, which encompass four fiscal years.

1. The 17 communities with regional offices are Boston, Brockton, Fall River, Framingham, Holyoke, Hyannis, Lawrence, Lowell, Malden, New Bedford, Northampton, Pittsfield, Quincy, Roxbury, Salem, Springfield, and Worcester. Brockton, Roxbury, and Springfield each have two offices, and the others each have one.
2. This number of employees includes employees who retired or resigned during the audit period.

CPCS Public Defender New Cases

Division	Fiscal Year 2019	Fiscal Year 2020	Fiscal Year 2021	Fiscal Year 2022	Total New Assignments
Children and Family Law	2,269	1,486	1,362	1,610	6,727
Mental Health Litigation	1,063	1,123	947	1,086	4,219
Youth Advocacy	1,756	1,728	1122	1,590	6,196
Public Defender	26,443	20,728	16,399	18,964	82,534
Total New Assignments	31,531	25,065	19,830	23,250	99,676

CPCS Private Attorney New Notices of Assignment of Counsel Issued

Division	Fiscal Year 2019	Fiscal Year 2020	Fiscal Year 2021	Fiscal Year 2022	Total New Notices
Children and Family Law	19,626	16,570	15,486	15,845	67,527
Mental Health Litigation	13,601	12,655	12,340	12,771	51,367
Youth Advocacy	5,403	5,266	4,791	5,452	20,912
Private Counsel	127,755	104,802	92,330	100,392	425,279
Total New Assignments	166,385	139,293	124,947	134,460	565,085

Software

CPCS uses over 15 types of software for public attorney billing, case management, office space reservation, customer service, employee expense management, information technology project management and help desk, data storage, private counsel billing, and court costs.

Cybersecurity Threat

According to CPCS management, on February 27, 2019, CPCS suffered a cyberattack. The agency was able to restore its data in 10 business days. The attack was contained, and the system was cleared of any remaining infected technology. CPCS shut down its intranet and email servers for those 10 business days, but this did not affect court cases.

During these 10 business days, CPCS worked in conjunction with the Office of the Comptroller of the Commonwealth (CTR) and hired a consultant to determine the impact of the attack and provide recommendations. CPCS also hired another consultant to perform a vulnerability assessment.

Based on the consultants' recommendations, CPCS applied new protective measures for patching, detecting breaches of, and monitoring their data centers and network. Information security awareness and training were improved for all employees.

Cybersecurity Awareness Training

According to CPCS's internal control plan (ICP), dated June 30, 2020, regarding cybersecurity awareness, CPCS follows the Enterprise Information Security Policies and Standards established by the Executive Office of Technology Services and Security's (EOTSS's) Enterprise Security Office, which are available and recommended for all Commonwealth agencies to use for guidance.

CPCS requires its employees to sign a Certification of Receipt Personnel Policies Manual form. Section 5.2.2 of CPCS's "Personnel Policies Manual" is its acceptable use policy. An acceptable use policy documents the responsibilities of personnel and that employees must comply with the applicable code of conduct when using Commonwealth-owned IT systems to preserve the confidentiality, integrity, and availability of CPCS's information assets.

CPCS uses KnowBe4 software to administer cybersecurity awareness training and phishing tests.[3] This software retains CPCS employees' test results. Newly hired employees receive cybersecurity awareness training during orientation. However, interns do not attend orientation and, as of May 2021, CPCS started requiring interns to watch a cybersecurity awareness training video and email the Human Resource Department once they have watched the video.

Business Continuity and Disaster Recovery

According to CPCS's ICP, dated June 30, 2020, regarding its business continuity and disaster recovery plan, CPCS follows the Enterprise Information Security Policies and Standards established by EOTSS's Enterprise Security Office, which are available and recommended for all Commonwealth agencies to use for guidance.

EOTSS's Business Continuity and Disaster Recovery Standard IS.005 requires an agency to "establish procedures for the continuation of critical business processes in the event of any organizational or

3. Phishing is when someone sends an email pretending to be a legitimate business or a person the recipient knows to obtain sensitive data, such as the recipient's bank account number. A phishing test lets organizations send a realistic, but fake, phishing email to employees to see how they respond.

information technology (“IT”) infrastructure failure and define the related controls and acceptable practices.”

CTR’s Pandemic Response Guidance

On September 30, 2020, CTR provided guidance for state agencies in response to the 2019 coronavirus (COVID-19) pandemic. The guidance helped state agencies that were experiencing significant changes identify their goals, objectives, and risks associated with the COVID-19 pandemic. Objectives included telework, return-to-work plans, changes to business processes, and safety protocols for staff members and visitors.

American Rescue Plan Act of 2021

The American Rescue Plan Act of 2021, signed on March 11, 2021, was a federal stimulus bill to aid public health and economic recovery from the COVID-19 pandemic. On December 17, 2021, CPCS received a total of $4,500,000 in American Rescue Plan Act of 2021 funds, allocated by Chapter 102 of the Massachusetts Acts and Resolves of 2021.

Chapter 102 stipulates $2,000,000 to address pandemic-related backlogged cases in CPCS’s Public Defender Division; $1,000,000 to temporarily fund staffing levels to address an increased need for legal representation in CPCS’s Children and Family Law Program; and $1,500,000 for the modernization of CPCS’s billing system. As of the conclusion of the audit period (which was December 31, 2021, two weeks after the funds were received), CPCS had not expended any of the $4,500,000.

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 Committee for Public Counsel Services (CPCS) for the period January 1, 2019 through December 31, 2021.

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 where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did CPCS employees receive cybersecurity awareness training and sign acknowledgment forms in accordance with Sections 6.2.3, 6.2.4, and 6.2.8 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010, effective October 15, 2018?	**No; see Finding 1**
2. Did CPCS update its business continuity and disaster recovery plan in accordance with Section 6.1.1.4 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005, effective October 15, 2018?	**No; see Finding 2**
3. Did CPCS update its internal control plan (ICP) as required by the Office of the Comptroller of the Commonwealth's (CTR's) "[2019 Coronavirus, or COVID-19] Pandemic Response Internal Controls Guidance"?	**No; see Finding 3**

To achieve our audit objectives, we gained an understanding of CPCS's internal control environment related to the objectives by reviewing applicable agency policies and procedures, as well as conducting inquiries with CPCS's staff and management. We evaluated the design of controls over cybersecurity awareness training, computer use acknowledgment forms, the business continuity and disaster recovery plan, and the ICP.

Acceptable Use Policy

We obtained a list of all employees during the audit period from CPCS. From this list, we selected a random, nonstatistical sample of 60 CPCS employees from a population of 884. We requested copies of the 60 employees' signed Certification of Receipt Personnel Policies forms (including computer usage) from CPCS's Human Resource Department and verified that there was a signature on each user's form to ensure that all users had signed forms and acknowledged the policies.

Cybersecurity Awareness Training

During our data reliability assessment, we tested all 23 CPCS employees, including 5 hired during the audit period, who had access to the Massachusetts Management Accounting and Reporting System (MMARS) during our audit period to ensure that they had received cybersecurity awareness training.

In addition, to determine whether CPCS newly hired employees without access to MMARS received cybersecurity awareness training within 30 days of new-hire orientation, we selected a nonstatistical, random sample of 35 CPCS newly hired employees from the list of employees without MMARS access from a population of 145. For each newly hired employee in our sample, we requested the orientation date from CPCS's Human Resource Department, and we requested the cybersecurity awareness training materials presented to the newly hired employees from CPCS's Information Technology (IT) Department. Also, we requested the cybersecurity awareness training certificates from CPCS's IT Department to determine whether these newly hired employees received annual cybersecurity awareness training, if applicable.

To determine whether CPCS's existing employees (who were hired before the audit period began) with no MMARS access completed their cybersecurity awareness training, we selected a nonstatistical sample of 50 existing CPCS employees from a population of 716 (which excludes the 18 existing employees with MMARS access). For each existing employee in our sample, we examined their cybersecurity awareness training certificate to determine whether they completed the annual training and the certificate was documented in KnowBe4.

Phishing

We obtained KnowBe4 test results for all employees who received phishing emails as part of the test during the audit period. We examined the test results and determined that 218 CPCS employees failed

the phishing testing during our audit period. In addition, for employees with MMARS access who failed the phishing tests, we determined how many times they each failed. We divided the 218 employees who failed the phishing tests into two strata.

For stratum one, 172 employees failed once, and we targeted the 6 employees with MMARS access and 29 without MMARS access to determine whether these employees took additional cybersecurity awareness training. We reviewed email notifications for additional training dates, interactive PowerPoint presentations used for additional training, and cybersecurity awareness training certificates from KnowBe4. No exceptions were noted with this testing.

For stratum two, there were 46 employees who failed more than once. For this stratum, we selected a random, nonstatistical sample of 10 employees to determine whether they received additional cybersecurity awareness training. We reviewed email notifications for additional training dates, interactive PowerPoint presentations used for additional training, and cybersecurity awareness training certificates from KnowBe4. No exceptions were noted with this testing.

ICP

We requested CPCS's ICPs for fiscal years 2020, 2021, and 2022 to determine whether they were updated with COVID-19 pandemic guidance as required by CTR's "Internal Control Guide," because COVID-19 had caused a significant change to the work environment. We examined a copy of the ICP for fiscal year 2021 to determine whether it contained the components required by CTR's "COVID-19 Pandemic Response Internal Controls Guidance."

Business Continuity and Disaster Recovery Plan

To determine whether CPCS had established a business continuity and disaster recovery plan, we requested the business continuity and disaster recovery plan from CPCS management. CPCS management provided an outline of the business continuity and disaster recovery plan that had not been approved by CPCS management (see Finding 2).

When we used nonstatistical sampling methods for our audit objectives, we did not project the results from the samples to the populations.

Data Reliability Assessment

CPCS Employee List

To determine the completeness and accuracy of the list of all CPCS employees during the audit period generated from MMARS, we compared this list to an employee list provided by CPCS's Human Resource Department and an employee list provided by CPCS's IT Department. In addition, for each of these lists, we tested for duplicate data, missing data, and dates outside the audit period. No exceptions were noted with this testing.

KnowBe4

To assess the reliability of CPCS's phishing test records from KnowBe4, we tested for missing data, duplicate data, and dates outside the audit period. For completeness and accuracy, we compared the names of employees from KnowBe4 to our reconciled employee list.

We assessed the reliability of the cybersecurity awareness training and phishing test records obtained from KnowBe4 using Service Organization Control reports[4] to determine whether there were exceptions in the testing performed for certain general IT controls (security management, access control, configuration management, segregation of duties, and contingency planning). In addition, we reviewed the peer review report of the agency that prepared the Service Organization Control reports.

MMARS

In 2018, the Office of the State Auditor performed a data reliability assessment of MMARS for the period April 1, 2017 through March 31, 2018. The assessment focused on reviewing selected system controls, including access controls, cybersecurity awareness, audit and accountability, configuration management, identification and authentication, and personnel security.

During this audit, we asked CPCS management about the agency's cybersecurity awareness policy and personnel security policy and procedures. We requested cybersecurity awareness training certificates for all 23 employees who had access to MMARS during the audit period.

4. These reports review the effectiveness of internal controls over an organization's information systems and are conducted by independent certified public accountants or accounting firms.

Based on the results of our data reliability assessments, we determined that the information obtained for our audit period was sufficiently reliable for the purpose of our audit objectives.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Committee for Public Counsel Services did not ensure that interns receive cybersecurity awareness training.

The Committee for Public Counsel Services (CPCS) employed 24 interns during the audit period, of whom 20 did not receive cybersecurity awareness training.

CPCS is exposed to a higher risk of cybersecurity attacks and financial and/or reputation losses without educating interns on their responsibility of protecting CPCS's information by requiring training.

Authoritative Guidance

Section 6.2.3 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Management Standard IS.010 states, "All new personnel must complete an Initial Security Awareness Training course. . . . The New Hire Security Awareness course must be completed within 30 days of new hire orientation."

Reasons for Issue

CPCS management stated that interns were not required to attend orientation, which included cybersecurity awareness training. In addition, after implementing the cybersecurity awareness training video requirement for interns in May 2021, CPCS did not have a system in place to document the receipt of emails from interns who watched the video.

Recommendations

1. CPCS should require that interns receive cybersecurity awareness training.
2. CPCS should have a system to document the receipt of emails from interns who watch the cybersecurity awareness training video.

Auditee's Response

CPCS augmented its prior policies and procedures to ensure that all interns receive cybersecurity awareness training, as it does for all agency employees. CPCS completed both development and implementation of a new electronic platform to ensure all interns receive cybersecurity awareness training during onboarding or within 30 days of hire. The electronic platform creates and maintains a record that cybersecurity training was completed by all interns. CPCS management believes that all users of its systems, including all short-term summer interns, must be educated concerning the dangers posed by cybersecurity threats as well as the acceptable use and safeguarding of the agency's electronic resources.

Auditor's Reply

Based on its response, CPCS has taken measures to address our concerns in this area.

2. CPCS did not have a business continuity and disaster recovery plan.

As of the end of our audit period, CPCS had not developed, documented, or tested a business continuity and disaster recovery plan for its business and operational objectives, potential risks and exposures, and the relative importance of the committee's systems and data.

Without a business continuity and disaster recovery plan, employees may not be sufficiently trained in performing recovery efforts, including those related to CPCS's mission-critical applications. In addition, CPCS has not assessed its ability to continue operations in the event of a business interruption, which could lead to reputational loss, financial loss, or breach of data.

Authoritative Guidance

Section 6 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005 states,

> *Commonwealth Executive Offices and Agencies must establish a Business Continuity Program. . . .*
>
> *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.*

Reasons for Issue

CPCS management stated that in fiscal year 2019, the staff member assigned to write the business continuity and disaster recovery plan took a leave of absence, and in fiscal year 2020, CPCS put out a request for proposals for a vendor to prepare a business continuity and disaster recovery plan. In fiscal year 2021, CPCS's chief information officer resigned before CPCS awarded a contract to a vendor, and as of the end of our audit period, CPCS was waiting for a new chief information officer to resume the process.

Recommendation

CPCS should develop, document, and test a business continuity and disaster recovery plan to implement.

Auditee's Response

CPCS has documented a Continuity of Operations Plan ("COOP"). The COOP was developed by CPCS senior management in collaboration with consultants with expertise in creating robust Business Continuity Plans for government agencies. This process was completed last year, and the formal plan has been presented to and reviewed by our governing board.

Further, senior management will be participating in table-top exercises in March 2023 to test and enhance our crisis management skills and the agency's resiliency in the event of a cyber (or other) attack on agency systems which could impact both the provision of legal services to our clients and the regular business operations of CPCS. These exercises will help to hone the skills required to manage the agency during a major crisis or other disruptions with the smallest possible impact on our clients and staff.

Finally, regarding disaster recovery, the [Information Technology, or IT] Department at CPCS oversees several information security products and services to monitor and defend against ongoing cybersecurity risks, including but not limited to:

- *Firewall & Endpoint Protection*
- *Managed Detection and Response*
- *E-Mail & Web Filtering*
- *Multifactor Authentication*
- *Ongoing Cybersecurity Awareness Training and Phishing Testing*
- *Virtual Information Security Officer Strategic Services*

Implementation and ongoing maintenance of these services is sponsored and supported by senior leadership at the agency.

CPCS currently utilizes IT disaster recovery procedures to guide recovery, including but not limited to tightly controlled access to the broader internet as well as a multi-level cloud and on-premises backup strategy.

CPCS' COOP includes an embedded business impact analysis summary to set strategic expectations for recovery objectives. As an additional step, the agency is currently working to further formalize its continuity planning by gathering and integrating business impact analyses from all practice and operational areas into a set of detailed business continuity plans which will inform the IT disaster recovery plan expected to be completed by the end of calendar year 2023.

Auditor's Reply

Based on its response, CPCS is taking measures to address our concerns in this area.

3. CPCS's internal control plan was not updated with a 2019 coronavirus component.

CPCS's internal control plan (ICP) was not updated with a 2019 coronavirus (COVID-19) component as required by the Office of the Comptroller of the Commonwealth's (CTR's) "COVID-19 Pandemic Response Internal Controls Guidance," issued September 30, 2020. CPCS's ICP was last updated in June 2020.

The absence of an up-to-date ICP may hinder CPCS from identifying vulnerabilities that could prevent it from achieving its mission to provide legal assistance to those in need and ensure equal access to legal representation to Massachusetts residents.

Authoritative Guidance

CTR's "COVID-19 Pandemic Response Internal Controls Guidance," dated September 30, 2020, states,

> *Department internal control plans must be based on risk assessments and updated annually, or when significant changes occur. Because the COVID-19 Pandemic has affected all departments, The Comptroller, in consultation with the State Auditor's Office, is providing two options for updating internal controls.*
>
> 1. *If the impact to your department is such that it can be reflected in your Internal Control Plan (ICP), then update the ICP as you would for any other mid-year changes.*
> 2. *Departments experiencing a significant impact, and requiring the accumulation of Substantial documentation (e.g. changes to business processes, requirements of federal and state-specific laws or guidance, new funds or new programs), can draft a separate COVID-19 Pandemic Response Plan Appendix to the ICP as an organized set (hard or soft copies) of emails, documents, risk assessments, policies, and procedures.*

CTR's "Internal Control Guide," revised June 25, 2015, states, "Accordingly, departments are obligated to revise their ICPs whenever significant changes occur in objectives, risks, management structure, program scope, etc. At the very least, the ICP must be reviewed and updated annually."

Reasons for Issue

CPCS did not have policies and procedures to ensure that its ICP is updated annually and when significant changes occurred.

Recommendation

CPCS should establish policies and procedures to ensure that its ICP is updated annually and when significant changes occur.

Auditee's Response

CPCS has updated the agency's Internal Control Plan. Further, CPCS has established systems, policies, and procedures to ensure that the agency's ICP is updated annually and when significant changes occur.

The most recent update to the Internal Control Plan was developed by CPCS management and was completed last year after undertaking a detailed risk assessment. Management believes internal controls are fundamental to achieving the mission, goals, and objectives of the agency and to mitigate potential risks. Further, CPCS management believes internal controls are an integral part of the agency's values and essential to successful program and organizational operations. The latest version of the ICP has been presented to and reviewed by our governing board.

In specific response to the COVID-19 Pandemic Emergency, the Chief Counsel designated the Director of Administration and Operations as the CPCS COVID-19 Response leader in March 2020. The Director oversaw all operational responses to COVID, delivered policy and other guidance via thirty-three (33) emails to staff, held conference calls with agency managers and directors and ensured that staff was regularly updated regarding operational and service changes. The Director also formed a committee of staff from various positions across the Commonwealth to create, review and recommend COVID policies and procedures which maintained the health and safety of staff while serving our clients and fulfilling our agency mission.

For example, CPCS quickly made plans for necessary office coverage at our 20 office locations, adopted systems to ensure that we maintained contact with incarcerated and hospitalized clients by telephone and mail, and instituted virtual conferences. Each office was required to create a reopening plan. All staff were trained on CPCS COVID policies and procedures. When the Governor announced reopening requirements, the agency ensured that COVID Reopening Policies and Procedures complied with the requirements specific to the type of business conducted in each office. As the Governor's reopening requirements were updated, the agency's policies and procedures were likewise updated.

Further, senior staff, including the Chief Counsel, Director of Administration and Operations, General Counsel, Human Resources, IT, and CFO, held virtual town halls with agency managers and staff to address agency policies and procedures during the pandemic to ensure the continued zealous representation of clients as well as staff support.

Throughout the pandemic, CPCS continued to zealously represent clients, supported staff, and met our fiduciary obligations to the Commonwealth as well as our financial obligation to ensure timely payments to private attorneys and vendors.

Auditor's Reply

Based on its response, CPCS has taken measures to address our concerns in this area.