OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued June 18, 2025

Massachusetts State College Building Authority

For the period July 1, 2022 through June 30, 2024

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

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

June 18, 2025

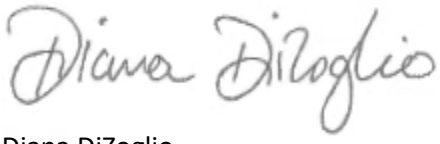
Sean P. Nelson, Executive Director
Massachusetts State College Building Authority
10 High Street, Suite 201
Boston, MA 02110

Dear Mr. Nelson:

I am pleased to provide to you the results of the enclosed performance audit of the Massachusetts State College Building Authority. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2022 through June 30, 2024. 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 Massachusetts State College Building Authority. 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 has any questions.

Best regards,



Diana DiZoglio
Auditor of the Commonwealth

cc: Michael Fallon, Chair of the Massachusetts State College Building Authority Board of Directors

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

BCP	business continuity plan
CMR	Code of Massachusetts Regulations
CTR	Office of the Comptroller of the Commonwealth
EOTSS	Executive Office of Technology Services and Security
ICP	internal control plan
MSCBA	Massachusetts State College Building Authority
OSA	Office of the State Auditor
SDO	Supplier Diversity Office
SDP	Supplier Diversity Program

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of the Massachusetts State College Building Authority (MSCBA) for the period July 1, 2022 through June 30, 2024.

The purpose of our audit was to determine the following:

- whether MSCBA had a process in place to ensure that it met the fiscal years 2023 and 2024 benchmarks set by the Supplier Diversity Office (SDO) for contracting with minority-, women-, and veteran-owned businesses;
- to what extent MSCBA ensured that its residential buildings on university campuses met the minimum public health and safety requirements, in accordance with Section 101.3 of Title 780 of the Code of Massachusetts Regulations and MSCBA's established procedures for monitoring its properties;
- whether MSCBA took corrective actions to address the issue identified in the prior OSA audit (Audit No. 2018-0209-3A) regarding its business continuity plan (BCP); and
- whether MSCBA took corrective actions to address the issue identified in the prior OSA audit (Audit No. 2018-0209-3A) regarding its internal control plan (ICP).

Below is a summary of our findings, the effects of those findings, and our recommendations, with hyperlinks to each page listed.

Finding 1 **Page 14**	MSCBA did not ensure that it met the annual benchmarks for diverse supplier spending set by SDO.
Effect	MSCBA has demonstrated a commitment to promoting diversity in its procurement process by voluntarily participating in the Supplier Diversity Program (SDP). However, because MSCBA did not have an established process for meeting these spending benchmarks, MSCBA limited its ability to evaluate and improve the effectiveness of its efforts to promote diversity in its procurement process.
Recommendations **Pages 15**	1. MSCBA should develop, document, and implement policies and procedures to effectively monitor the extent to which it achieves SDO annual benchmarks for diverse supplier spending. These policies should incorporate the updated requirements of the SDP, which, effective July 1, 2024, include spending benchmarks for businesses owned by LGBTQ individuals and individuals with disabilities. 2. MSCBA should develop strategies aimed at enhancing the participation of diverse businesses in its procurement process. This could include expanding targeted outreach to certified diverse vendors to increase their participation as both prime contractors and subcontractors.
Finding 2 **Page 16**	MSCBA's BCP was missing critical components.

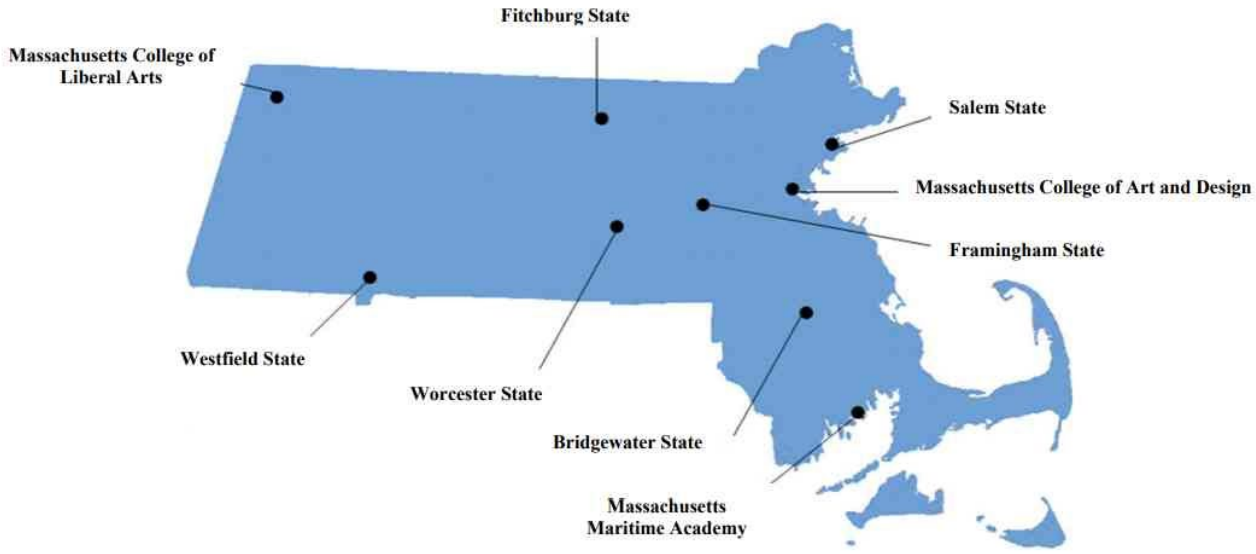
Effect	Without a comprehensive BCP, MSCBA cannot ensure that it has adequate procedures in place to protect critical information assets or to recover essential operations in the event of a disruption or disaster.
Recommendation Page 17	MSCBA should update its BCP to include all critical components outlined by the Executive Office of Technology Services and Security.
Finding 3 Page 18	MSCBA's ICP was not based on an agency-wide risk assessment and was missing key elements of enterprise risk management.
Effect	Without a sufficiently developed ICP based on an agency-wide risk assessment, MSCBA is limited in its ability to identify vulnerabilities, which could prevent it from achieving organizational goals.
Recommendations Page 19	1. MSCBA should develop an ICP based on a current agency-wide risk assessment that includes all aspects of its business activities. MSCBA should ensure that its ICP includes all the critical components of enterprise risk management. 2. After completing its ICP, MSCBA should ensure that the ICP is communicated to all employees, used within its operations, and reviewed and updated at least annually.
Finding 4a Page 20	MSCBA did not adequately manage employee access rights.
Effect	Without management approval, MSCBA does not have sufficient verification that system users were approved to access the system at all or that user accounts were limited to the fewest privileges necessary for the employees' job duties.
Finding 4b Page 21	MSCBA could not provide evidence that its employees completed cybersecurity awareness training.
Effect	If MSCBA does not ensure that its employees complete cybersecurity awareness training, then it is exposed to an increased risk of cyberattacks and financial and/or reputational losses.
Finding 4c Page 22	MSCBA was missing documentation for a completed background check.
Effect	Without proper screening, MSCBA assumes a higher-than-acceptable risk of hiring individuals who may pose security threats to its systems and data.
Finding 4d Page 22	MSCBA did not promptly revoke access rights to its accounting and project management system.
Effect	If MSCBA does not promptly revoke former employees' access rights to its system, then there is an increased risk that former employees could improperly access and/or change information in the system.
Finding 4e Page 23	MSCBA did not have session lock mechanisms in place.
Effect	If MSCBA does not have session lock mechanisms in place, then employees may remain logged on indefinitely, increasing the risk of unauthorized access and reducing the organization's ability to effectively monitor and control system activity.
Finding 4f Page 24	MSCBA did not have a documented configuration management policy.

Effect	Without a configuration management policy, MSCBA makes its accounting and project management system vulnerable to misconfigurations, security threats, and performance issues.
Finding 4g **Page 25**	MSCBA did not have established procedures to review audit logs.
Effect	If MSCBA does not run regular audit logs of its accounting and project management system, then it exposes itself to a higher-than-acceptable risk of unauthorized user activity. It also exposes itself to a higher-than-acceptable risk that security incidents and policy violations go undetected by MSCBA management.
Recommendations **Page 26**	1. MSCBA should ensure that documented records are kept to evidence supervisory approval for system user rights for its accounting and project management system. 2. MSCBA should develop and implement policies and procedures to ensure that all employees receive cybersecurity awareness training within 30 days of orientation and annually thereafter. Also, MSCBA should maintain certificates of completion of these trainings for all of its employees. 3. MSCBA should ensure that all employees with access to confidential information undergo background checks, as required by its policy. MSCBA should maintain documentation of these screenings to ensure accountability and compliance. 4. MSCBA should ensure that system privileges are revoked within 24 business hours of termination. Additionally, MSCBA should consider temporarily suspending employees' privileges when they are on leaves of absence. 5. MSCBA should configure both its network and its accounting and project management system to lock out after a five-minute period of inactivity. 6. MSCBA should establish controls to ensure that configuration management procedures are in place to safeguard its accounting and project management system. 7. MSCBA should ensure that audit logs are run for its accounting and project management system on a regular basis, so that system user activity is tracked.

OVERVIEW OF AUDITED ENTITY

The Massachusetts State College Building Authority (MSCBA) was established under Chapter 703 of the Acts of 1963. MSCBA is authorized to finance and oversee the design and construction of housing, dining, athletic, parking, and other student activity facilities at the 15 community colleges[1] and nine state universities.[2] This financing and oversight authority, which is established by its enabling legislation, is subject to written approval from the Secretary of Administration and Finance and the Commissioner of Higher Education for Massachusetts. MSCBA is also authorized to issue bonds and collect student rents and fees for the operation of student living facilities.

MSCBA oversees residence halls that house approximately 16,500 students across 54 residential complexes. These facilities accommodate about 50% of the total undergraduate student population in Massachusetts state colleges and universities and span approximately 4.5 million square feet across the nine state university campuses (as shown below). There are no residence halls located on community college campuses.



Source: MSCBA's Annual Report Fiscal Year 2023 (https://www.mscba.org/docs/143_2024-01-31MSCBAFY2023AnnualReportwithFinancialStatements.pdf)

1. The community colleges are Berkshire, Bristol, Bunker Hill, Cape Cod, Greenfield, Holyoke, Massachusetts Bay, Massasoit, Middlesex, Mount Wachusett, North Shore, Northern Essex, Quinsigamond, Roxbury, and Springfield Technical.
2. The state universities are Bridgewater, Fitchburg, Framingham, Salem, Westfield, and Worcester, as well as the Massachusetts College of Art and Design, the Massachusetts College of Liberal Arts, and the Massachusetts Maritime Academy.

MSCBA is governed by a nine-member board, the members of which are appointed by the Governor. Three members of the board must also be members of the state's Board of Higher Education. It is also governed by various state procurement laws and regulations; the trust agreements for all bonds that MSCBA issues; and the Contract for Financial Assistance, Management and Services between MSCBA and the Board of Higher Education, which acts on behalf of the community colleges and universities served by MSCBA. Further, the Secretary of Administration and Finance and the State Treasurer and Receiver General must approve the sale of all bonds and notes issued by MSCBA to fund its projects. MSCBA's board appoints an executive director who is responsible for overseeing the day-to-day operations of MSCBA.

The Commonwealth does not appropriate any state funding for MSCBA, nor does it guarantee the bonds issued by MSCBA for its building projects. Instead, all revenue used to support the design, construction, and operation of MSCBA facilities is generated through rents and fees paid by students for the use of these facilities and related services. According to the MSCBA fiscal year 2023 audit report that was completed by an independent auditor, MSCBA's principal amount of outstanding bond debt, as of June 30, 2023, was $1.135 billion. For the fiscal year that ended June 30, 2023, MSCBA spent $30,323,667 on land, construction, buildings, improvements, furnishings, and equipment for MSCBA capital assets at community colleges and universities.

MSCBA is located at 10 High Street in Boston and had 14 employees as of June 30, 2024.

Supplier Diversity Program

MSCBA voluntarily participates in the Supplier Diversity Office's (SDO's) Supplier Diversity Program (SDP). According to the Supplier Diversity Office Comprehensive Annual Report Fiscal Year 2023, "the role of the SDO is to certify, provide resources for, and support a wide range of diverse and small businesses in competing for contracts being bid across the Commonwealth."

Through consultation with the Office for Access and Opportunity and Community Affairs, which falls under the Office of the Governor, SDO sets annual benchmark percentages for spending by SDP participants with

minority-owned,[3] woman-owned, and veteran-owned businesses.[4] The annual spending benchmarks are expressed as a percentage of the discretionary budget for each participating state agency.

For fiscal years 2023 and 2024, SDO set the spending benchmarks[5] outlined in the table below.

Business Certification Category	Spending Benchmark (Percentage of State Agency's Discretionary Budget)
Minority-Owned Business	8%
Women-Owned Business	14%
Veteran-Owned Business	3%

During the audit, MSCBA officials told us that they determine discretionary spending by identifying expenditures linked to specific job codes within various projects. This includes costs for building construction such as materials, labor, and permits; design services, which cover architectural and interior design; and project management, which involves coordinating budgets, schedules, and resources to ensure the successful completion of projects.

MSCBA voluntarily submits a narrative describing its efforts to meet the spending benchmarks and to advance diversity and inclusion in its procurement, which SDO includes as part of its annual report. According to the Supplier Diversity Office Comprehensive Annual Report Fiscal Year 2023,

> *[MSCBA] is committed to fostering, cultivating, and preserving a culture of diversity, equity, and inclusion. [MSCBA] partners with the Commonwealth's Supplier Diversity Office, other state entities, and industry associations to strengthen the diverse workforce within the Commonwealth.*
>
> *In addition to adopting the Commonwealth's diversity goals for hiring design and construction firms, the MSCBA continues to reach out to the subcontractor community by engaging Minority Business Enterprises, Women Owned Business Enterprises, and Veteran-Owned Business Enterprises in a web-based trade contractor prequalification process where they are awarded additional credit toward becoming prequalified to bid on MSCBA projects.*

3. According to the Supplier Diversity Office Comprehensive Annual Report Fiscal Year 2023, SDO defines a minority-owned business "as a business that is owned by a racially or ethnically diverse individual. While the [term is] meant to define an ethnically or racially diverse individual or business . . . [it is] not meant to denote a smaller or lesser status of the individuals or businesses included in this definition." We use this terminology here because it is a defined term used by the auditee.
4. The percentage for veteran-owned businesses combines the requirement for veteran- and service-disabled veteran–owned businesses. For more information about veteran- and service-disabled veteran–owned businesses, see SDO's Comprehensive Annual Report for Fiscal Year 2023.
5. Effective July 1, 2024, spending benchmarks for businesses owned by LGBTQ individuals and individuals with disabilities were incorporated into the Commonwealth's Supplier Diversity Program. This change occurred outside of the audit period and was therefore not included in the scope of our audit.

Building Safety

Staff members of community colleges and universities manage the day-to-day operations of buildings owned by MSCBA. According to the Contract for Financial Assistance, Management and Services, dated February 1, 2003, between MSCBA and the Board of Higher Education, each community college and university is required to operate and maintain the buildings located on its campus and to keep them in good order and repair. Universities collect rents and fees from students for the use of the buildings; procure all necessary equipment, materials, and supplies for upkeeping buildings; and make necessary repairs—all of which are similar to the responsibilities that a property manager has. As the legal owner of the properties, MSCBA remains accountable for the overall condition of the properties and provides the financing for upkeep and repairs.

MSCBA assigns a project manager to each campus to help oversee building maintenance. These project managers stay in contact with campus facilities staff members and keep track of any deferred maintenance needs. Project managers meet with campus facility staff members regularly to identify any issues, needed repairs, or renovation requests.

MSCBA has a number of requirements to which community colleges and universities must adhere. For example, each year, MSCBA requires community colleges and universities to confirm that they have active service contracts for key systems in MSCBA-owned buildings on their campuses, such as boilers, elevators, fire escapes, fire alarms, fire suppression systems, and generators. In order to confirm that they hold these active contracts, community colleges and universities submit copies of the contract tracking sheets to MSCBA. Universities must also certify that the annual Certificates of Occupancy are on file for residential buildings. Additionally, community colleges and universities must notify MSCBA of any deficiencies or violations that need to be addressed as soon as they are identified—for example, sprinkler systems that need to be updated or issues identified during building system maintenance inspections. Community colleges and universities submit this information via email using a Service Contract Tracking Sheet provided by MSCBA.

Business Continuity and Internal Control Plans

During our prior audit (Audit No. 2018-0209-3A), we found that MSCBA had not developed an effective business continuity plan (BCP) or conducted testing of its disaster recovery plan in accordance with the Executive Office of Technology Services and Security's (EOTSS's) Business Continuity and Disaster

Recovery Standard IS.005.[6] This standard required that Commonwealth agencies have a plan to keep essential business functions running, especially during disruptions. The BCP should focus on the most likely and most impactful risks to information security, identify key functions, and include ways to keep those functions going if systems or environments fail. Additionally, the BCP must be tested every year to check for any overlooked issues or necessary updates, including changes to equipment or staff members. Although MSCBA is not required to follow these standards, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Additionally, during our prior audit (Audit No. 2018-0209-3A), we found that MSCBA's system of internal controls needed improvement. Specifically, we found that MSCBA had not developed an internal control plan (ICP) that clearly summarized (1) all of the risks that could potentially prevent it from achieving its financial, operational, and compliance goals and (2) the internal controls that MSCBA had in place to mitigate these risks. While our report acknowledged that MSCBA had documented policies and procedures, primarily related to its financial operations, these controls were limited to specific areas and did not form a comprehensive ICP. In our prior audit, we recommended that MSCBA conduct an agency-wide risk assessment and develop internal controls to mitigate identified risks and achieve organizational goals.

While there are no specific legal or regulatory requirements related to MSCBA's system of internal controls, Chapter 647 of the Acts of 1989 requires state agencies to develop and clearly document internal control systems in accordance with the guidelines established by the Office of the Comptroller of the Commonwealth (CTR). These guidelines require that an ICP be based on an agency-wide risk assessment and be revised annually. Although MSCBA is not required to follow these standards, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, we consider them best practices.

6. EOTSS has since changed the titles and numbers of at least some of its policies and standards between the end of the audit period and the publication of this report. In this report, we reference the titles and numbers of EOTSS's policies and/or standards as they were during the audit period (unless stated otherwise).

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of certain activities of the Massachusetts State College Building Authority (MSCBA) for the period July 1, 2022 through June 30, 2024.

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 MSCBA have a process in place to ensure that it met the fiscal year 2023 and 2024 benchmarks set by the Supplier Diversity Office (SDO) for contracting with minority-, women-, and veteran-owned businesses?	**No; see Finding 1**
2. To what extent did MSCBA ensure that its residential buildings on university campuses met the minimum public health and safety requirements, in accordance with Section 101.3 of Title 780 of the Code of Massachusetts Regulations (CMR) and MSCBA's established procedures for monitoring its properties?	**To a satisfactory extent**
3. Did MSCBA take corrective actions to address the issue identified in the prior OSA audit (Audit No. 2018-0209-3A) regarding its business continuity plan (BCP)?	**Partially; see Finding 2**
4. Did MSCBA take corrective actions to address the issue identified in the prior OSA audit (Audit No. 2018-0209-3A) regarding its internal control plan (ICP)?	**Partially; see Finding 3**

To accomplish our audit objectives, we gained an understanding of the aspects of MSCBA's internal control environment relevant to our objectives by reviewing applicable policies and procedures, reviewing relevant contracts, and interviewing officials at MSCBA and two state universities. We evaluated the design and implementation of the internal controls related to our audit objectives. We also tested the operating effectiveness of controls related to the verification of service contracts for key safety systems in MSCBA-owned buildings. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

Supplier Diversity Program

To determine whether MSCBA had a process in place to ensure that it met the fiscal year 2023 and 2024 benchmarks set by SDO for contracting with minority-, women-, and veteran-owned businesses, we took the following actions. First, we obtained a list of all 3,947 expenses, totaling $104,299,510, recorded by MSCBA during the audit period in its accounting and project management system. From this data, we identified MSCBA's discretionary spending for fiscal years 2023 and 2024 as $43,968,982 and $41,582,622, respectively, totaling 2,752 transactions. We then determined how much of the identified discretionary spending was directed to certified minority-, women-, and veteran-owned businesses. To do this, we cross-referenced the vendors in the discretionary spending dataset with SDO's directory of certified businesses. We calculated the total dollar amount and the percentage of discretionary spending awarded to diverse vendors during the audit period and compared it to the applicable SDO benchmarks for fiscal years 2023 and 2024.

Based on the results of our testing, we determined that MSCBA did not have a process in place to ensure that it met the benchmarks set by SDO for contracting with minority-, women-, and veteran-owned businesses during the audit period. Also, although MSCBA met the SDO benchmark for contracting with veteran-owned businesses, it did not meet the spending benchmarks for minority- and women-owned businesses. See Finding 1 for more information.

Residential Building Safety

To determine to what extent MSCBA ensured that its residential buildings on university campuses met the minimum public health and safety requirements, in accordance with 780 CMR 101.3 and MSCBA's established procedures for monitoring its properties, we took the actions described below.

We selected a random, nonstatistical[7] sample of 20 MSCBA-owned residential properties from a population of 54 for our testing. For each property in our sample, we verified that the respective state university submitted the required Service Contract Tracking Sheet to MSCBA. We reviewed the tracking sheets submitted by the university facilities staff members to ensure that they were fully completed and that they provided vendor information for all applicable building systems. We requested executed vendor agreements and Certificates of Occupancy for each property and the service contracts listed on the

7. Auditors use nonstatistical sampling to select items for audit testing when a population is very small, the population items are not similar enough, or there are specific items in the population that the auditors want to review.

tracking sheets in our sample. We examined each contract to ensure that it corresponded with the correct property and vendor listed on the tracking sheet, and we ensured that the contract dates were active during the audit period. In addition, we confirmed that the sampled universities maintained a valid Certificate of Occupancy on file for each property.

We did not identify any exceptions in our testing. Therefore, we concluded that, during the audit period, MSCBA ensured that its residential buildings on university campuses met the minimum public health and safety requirements, in accordance with 780 CMR 101.3 and MSCBA's established procedures for monitoring its properties.

BCP

During our prior audit (Audit No. 2018-0209-3A), we found that MSCBA had not developed an effective BCP or conducted testing of its disaster recovery plan in accordance with the Executive Office of Technology Services and Security's (EOTSS's) Business Continuity and Disaster Recovery Standard IS.005. To determine whether MSCBA took corrective actions to address the issue identified in our prior audit (Audit No. 2018-0209-3A) regarding its BCP, we interviewed knowledgeable MSCBA staff members and inspected MSCBA's BCP to confirm that a plan was in place during this report's audit period and that it complied with EOTSS's Business Continuity and Disaster Recovery Standard IS.005. Additionally, we reviewed documented test results to determine whether MSCBA's disaster recovery plan was tested annually during the audit period.

Based on the results of our testing, we determined that MSCBA's BCP did not include all required elements. See Finding 2 for more information.

ICP

During our prior audit (Audit No. 2018-0209-3A), we found that MSCBA had not developed an ICP that clearly summarized all of MSCBA's risks and the internal controls that it had in place to mitigate them. To determine whether MSCBA took corrective actions to address the issue identified in our prior audit (Audit No. 2018-0209-3A) regarding its ICP, we interviewed knowledgeable MSCBA staff members and inspected the agency's ICP that was in effect during this report's audit period to determine whether it had been updated to include an agency-wide risk assessment, as recommended in our prior audit. Additionally, we examined the ICP to assess whether it complied with the Office of the Comptroller of the Commonwealth's

(CTR's) guidelines, which require inclusion of the eight components of the Committee of Sponsoring Organizations of the Treadway Commission's enterprise risk management framework.

Based on the results of our testing, we determined that MSCBA's ICP does not meet all of the requirements of CTR's guidelines. See Finding 3 for more information.

We used nonstatistical sampling methods for testing and therefore did not project the results of our testing to any population.

Data Reliability Assessment

To determine the reliability of the list of expenses that we obtained from MSCBA's accounting and project management system, we conducted interviews and system walkthroughs with MSCBA management and staff members who were knowledgeable about and responsible for overseeing the data. We also checked the list to ensure that there were no duplicates or missing data, and that all of the data corresponded to dates within the audit period. To confirm the completeness of the list of expenses, we selected a random sample of 20 purchase orders we inspected from MSCBA's physical files and traced vendor names, purchase order numbers, and payment amounts to the list of expenses we received. To confirm the accuracy of the list of expenses, we selected a random sample of 20 expenses from the list and traced vendor names, payment dates, and payment amounts to invoices that we inspected from MSCBA's records.

We also reviewed select system controls related to security management, access controls, configuration management, segregation of duties, and contingency planning. Through this testing, we found that MSCBA has not established adequate internal controls over its accounting system. See Finding 4 for more information regarding the results of our review of the information system controls.

Further, we conducted a Benford's Law test[8] on the list of overall expenses to detect any indication of fraud or tampering with general ledger expenses that would compromise data integrity, and we found no indication of such activity.

8. Benford's Law is a statistical principle that predicts how often each digit (one through nine) appears as the leading digit in naturally occurring numerical data. Significant deviations from this distribution may indicate irregularities or potential manipulation and can be used as a tool for data analysis in audits.

To determine the reliability of the list of properties owned by MSCBA that was provided to us, we interviewed MSCBA officials who were knowledgeable about the list. We checked the list for blank and duplicate records. We also confirmed that final construction dates for all listed properties occurred before the start of the audit period. Additionally, we verified the list of properties against community college and university records and MSCBA contracts. Finally, we reconciled the list of residential properties with MSCBA's Annual Report Fiscal Year 2023.

Based on the results of the data reliability assessment procedures described above, we determined that the information we obtained was sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts State College Building Authority did not ensure that it met the annual benchmarks for diverse supplier spending set by the Supplier Diversity Office.

The Massachusetts State College Building Authority (MSCBA) did not have processes to ensure that it met the annual benchmarks for diverse supplier spending set by the Supplier Diversity Office (SDO). During the audit period, MSCBA did not meet discretionary spending benchmarks for minority-owned and women-owned businesses.

MSCBA's spending on minority-owned businesses was only 0.2% in both fiscal years 2023 and 2024, far below the 8% benchmark. Similarly, spending on women-owned businesses was 1.2% in fiscal year 2023 and 2.1% in fiscal year 2024, well below the 14% benchmark. The table below summarizes MSCBA's benchmark attainment during fiscal years 2023 and 2024.

	Fiscal Year 2023	Fiscal Year 2024
Total Discretionary Budget	$43,968,982	$41,582,622
Minimum Amount MSBCA Needed to Spend to Meet the Minority-Owned Business Benchmark (8%)	$3,517,519	$3,326,610
Amount Spent	$89,489 (0.2%)	$74,366 (0.2%)
Minimum Amount MSBCA Needed to Spend to Meet the Women-Owned Business Benchmark (14%)	$6,155,657	$5,821,567
Amount Spent	$530,638 (1.2%)	$890,001 (2.1%)
Minimum Amount MSBCA Needed to Spend to Meet the Veteran-Owned Business Benchmark (3%)	$1,319,069	$1,247,479
Amount Spent	$2,813,780 (6.4%)	$1,456,939 (3.5%)

MSCBA has demonstrated a commitment to promoting diversity in its procurement process by voluntarily participating in the Supplier Diversity Program (SDP). However, because MSCBA did not have an established process for meeting these spending benchmarks, MSCBA limited its ability to evaluate and improve the effectiveness of its efforts to promote diversity in its procurement process.

Authoritative Guidance

SDO's "The Commonwealth of Massachusetts Diverse and Small Business Program Policies for Goods and Services Procurements" states,

> *Annual benchmarks for departmental supplier diversity and small business spending are set by the SDO and are subject to approval by the Secretary for Administration and Finance and the Governor's Office for Access and Engagement. The benchmark spending amounts are based on applying current benchmark percentages to each department's discretionary budget and, at the end of each fiscal year, to its discretionary spending.*

Program	Certification Type	Benchmark Percentage
Supplier Diversity Program (SDP)	*Minority Business Enterprise (MBE)*	*8%*
	Woman Business Enterprise (WBE)	*14%*
	Veteran Business, including Veteran Business Enterprise (VBE) and Service-Disabled Veteran-Owned Business Enterprise (SDVOBE)	*3%*

Reasons for Issue

According to MSCBA officials, MSCBA's ability to meet SDO's annual spending benchmarks is constrained by procurement regulations that require contracts to be awarded to the lowest eligible and responsible bidder. Specifically, for construction projects, MSCBA must follow the bidding procedures outlined in Chapter 149 of the Massachusetts General Laws, which mandate contract awards based solely on price. As a result, even when a certified diverse business submits a bid, MSCBA cannot prioritize that vendor if a lower bid is received from a nondiverse business.

Recommendations

1. MSCBA should develop, document, and implement policies and procedures to effectively monitor the extent to which it achieves SDO annual benchmarks for diverse supplier spending. These policies should incorporate the updated requirements of the SDP, which, effective July 1, 2024, include spending benchmarks for businesses owned by LGBTQ individuals and individuals with disabilities.
2. MSCBA should develop strategies aimed at enhancing the participation of diverse businesses in its procurement process. This could include expanding targeted outreach to certified diverse vendors to increase their participation as both prime contractors and subcontractors.

Auditee's Response

> *As correctly noted by the [Office of the State Auditor], the Authority is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency and, therefore, not subject to the SDO annual benchmarks. However, as supporting supplier diversity is*

important to the Authority's mission in serving the Commonwealth's campuses, the Authority has established a long-standing practice of setting goals for diversity and specifically supporting diversity of the Commonwealth's workforce.

Moving forward, the Authority intends to improve its process for monitoring and reporting of direct and indirect spending on a fiscal year basis; consider amending existing contracts when new diversity benchmarks are released by the state; expand outreach to diverse vendors in non-construction cost categories of work; and consider incorporating additional spending benchmarks for businesses owned by LGBTQ individuals and individuals with disabilities. Lastly, the Authority may establish its own process for expanding its sources of information in determining the pool of available minority- and women-owned businesses in accordance with [Section 6(c) of Chapter 7C of the General Laws].

Additionally, the Authority continues to reach out to the subcontractor community by engaging Minority-, Woman, and Veteran-Owned Business Enterprises in a web-based trade contractor prequalification process where they are awarded additional credit toward becoming prequalified to bid on Authority projects. Along with such [minority-owned / women-owned business enterprise] goals, the Authority has also adopted workforce participation goals to ensure opportunities for minorities and women to participate in the Authority's construction projects.

Auditor's Reply

Based on its response, MSCBA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

2. The Massachusetts State College Building Authority's business continuity plan was missing critical components.

In our previous audit (Audit No. 2018-0209-3A), we reported that MSCBA had not developed a business continuity plan (BCP). During the current audit, we found that MSCBA has since developed a BCP, but it did not meet the requirements outlined by the Executive Office of Technology Services and Security (EOTSS). Specifically, MSCBA's BCP did not have the following critical components:

- a detailed inventory of critical information assets;
- a clear definition of mission-essential functions;
- identification of and management procedures for risks associated with the potential loss or disruption of essential business processes and information assets;
- an analysis of critical business processes;
- an assessment of likely disruptive events;
- insights from business impact analyses and risk assessments; and
- documentation of an order of succession, delegation of authority, and a list of essential records.

Without a comprehensive BCP, MSCBA cannot ensure that it has adequate procedures in place to protect critical information assets or to recover essential operations in the event of a disruption or disaster.

Authoritative Guidance

According to Section 6.1 of EOTSS's Business Continuity and Disaster Recovery Standard IS.005,

> *Commonwealth Agencies and Offices must establish a Business Continuity Program*
>
> *6.1.1.2 Perform a **risk** assessment of critical **information assets**: Establish **controls** to identify, contain and mitigate the **risks** associated with the loss or disruption of critical business processes and **information assets**. . . .*
>
> *6.1.1.4 Develop business continuity plans (BCP): Commonwealth Agencies and Offices will 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. . . .*
>
> *6.1.1.4.3 BCPs must be updated whenever a major organizational change occurs or at least annually, whichever comes first. . . .*
>
> *6.1.1.4.4.1 Identify essential mission and business functions and a plan for maintaining these functions in the event of system or environment compromise, disruption, or failure. . . .*
>
> *6.1.1.4.6.1 Perform annual tests of the BCPs to identify incorrect assumptions, oversights, and account for updates to equipment or **personnel** changes. Test results will be reported to senior management, **the Commonwealth [chief information security officer]**, or his or her designee, and the Security Office.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reasons for Issue

MSCBA officials stated that they were in the process of developing the BCP when the COVID-19 pandemic began. The unexpected pandemic required the agency to shift its focus, delaying completion of its BCP.

Recommendation

MSCBA should update its BCP to include all critical components outlined by EOTSS.

Auditee's Response

The Authority has made significant progress on the development of a BCP since the [Office of the State Auditor's (OSA's)] 2018 audit (Audit No. 2018-0209-3A). Many of the elements of business continuity that relate to technology cited in OSA's 2018 report have been rectified. For example, the Authority completes an annual disaster recovery drill, performed by its external [information technology) network support provider. As noted in the OSA's 2018 report and during discussions regarding the OSA's 2024 audit of the Authority, these disaster recovery drills are performed annually to ensure that all information assets are safeguarded and recoverable should a disruption to access occur. These annual drills have successfully recovered all Authority information assets for seven (7) consecutive years since 2018. Moreover, the Authority is committed to continuing to develop and refine the BCP so that it is continually focused on improving the Authority's response in the event of a disruption or disaster.

Auditor's Reply

We acknowledge MSCBA's efforts in developing a BCP since our prior audit and commend its consistent annual testing of its disaster recovery plan. However, as noted above, MSCBA's BCP remains incomplete and does not fully align with the requirements established by EOTSS. While disaster recovery is a key element of business continuity, a comprehensive BCP must also address organizational mission-essential functions, risk management procedures, business impact analysis, and succession planning—among other critical areas—which we found are still lacking in the current plan.

We encourage MSCBA to fully implement our recommendation and expand the scope of its BCP to ensure compliance with EOTSS standards, strengthening its ability to withstand and recover from operational disruptions.

3. The Massachusetts State College Building Authority's internal control plan was not based on an agency-wide risk assessment and was missing key elements of enterprise risk management.

In our previous audit (Audit No. 2018-0209-3A), we found that MSCBA had not developed a comprehensive internal control plan (ICP) that identified all agency risks and related controls. While some policies and procedures were documented, they primarily addressed financial operations and therefore did not constitute a comprehensive ICP.

In the current audit, we again identified deficiencies in MSCBA's ICP. Specifically, the ICP was not based on an agency-wide risk assessment, which is a critical element for identifying and addressing potential risks across all aspects of MSCBA's business operations. Similarly to what we found in our prior audit, the

ICP remained focused primarily on financial and accounting functions. Additionally, MSCBA's ICP did not incorporate all critical components of enterprise risk management as outlined by the Office of the Comptroller of the Commonwealth's (CTR) *Internal Control Guide.*

Without a sufficiently developed ICP based on an agency-wide risk assessment, MSCBA is limited in its ability to identify vulnerabilities, which could prevent it from achieving organizational goals.

Authoritative Guidance

There are no specific legal or regulatory requirements related to MSCBA's internal control system; however, according to Chapter 647 of the Acts of 1989, state agencies are required to develop and clearly document internal control systems in accordance with guidelines established by CTR. These guidelines require an ICP to be based on a risk assessment and revised annually. Although MSCBA is not required to follow these standards, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, we consider them best practices.

CTR's *Internal Control Guide* states,

> *Your department is obligated to review and update your Internal Control Plan on an annual basis, as well as whenever there is a new objective, risk, or management structure. . . .*
>
> *An internal control plan should have a statement of awareness and compliance with [the General Laws] Chapter 647 guidelines in addition to the [Committee of Sponsoring Organizations'] eight [enterprise risk management framework] components.*

Reasons for Issue

MSCBA has not developed policies and procedures to ensure that it creates and annually reviews a comprehensive ICP that addresses all of MSCBA's operations. According to MSCBA officials, although MSCBA staff members independently monitor various documents related to internal controls, MSCBA does not have the staff capacity to consolidate these efforts into a centralized ICP.

Recommendations

1. MSCBA should develop an ICP based on a current agency-wide risk assessment that includes all aspects of its business activities. MSCBA should ensure that its ICP includes all the critical components of enterprise risk management.
2. After completing its ICP, MSCBA should ensure that the ICP is communicated to all employees, used within its operations, and reviewed and updated at least annually.

Auditee's Response

The Authority has written policies and procedures for specific operations, and finance and accounting internal controls are reviewed annually both internally and by the Authority's external audit firm. Although these documents do not take the form of a singular document or plan, they collectively direct and guide day-to-day internal operations of the Authority. The Authority will review its internal controls documents, as well as suggested guidance from CTR and other authorities, consistent with the Committee of Sponsoring Organizations (COSO) framework to further develop a single comprehensive plan for all the critical components of enterprise risk management.

Auditor's Reply

Based on its response, MSCBA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

4. The Massachusetts State College Building Authority had inadequate information system general controls over its accounting and project management system.

MSCBA did not have adequate information system general controls over its accounting and project management system. Specifically, we identified issues with management of employee access rights, employee cybersecurity awareness training, background checks, revocation of employee access rights, session lock mechanisms, configuration management, and audit log reviews**.**

a. The Massachusetts State College Building Authority did not adequately manage employee access rights.

MSCBA did not have documented management approval for its employees' access rights to its accounting and project management system for 12 (80%) out of 15 users in the population of employees who were active during the audit period.

Without management approval, MSCBA does not have sufficient verification that system users were approved to access the system at all or that user accounts were limited to the fewest privileges necessary for the employees' job duties.

Authoritative Guidance

Section 6.1 of EOTSS's Access Management Standard IS.003 states,

> *6.1.5 Request access privileges: **User** requests for access privileges will follow a formal process. . . .*

*6.1.5.2 **User** registration and revocation procedures will be implemented for all **information systems** and services.*

*6.1.5.3 **User** access requests will be recorded (paper or tool-based), include a business justification for access, and be approved by the requestor's supervisor and the appropriate **Information Owner** or authorized delegate.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

MSCBA did not have documented policies and procedures regarding recording and maintaining user access request approvals for its accounting and project management system during the audit period.

b. The Massachusetts State College Building Authority could not provide evidence that its employees completed cybersecurity awareness training.

MSCBA was unable to produce any attendance records or certificates of completion to verify that accounting and project management system users received cybersecurity awareness training during the audit period.

If MSCBA does not ensure that its employees complete cybersecurity awareness training, then it is exposed to an increased risk of cyberattacks and financial and/or reputational losses.

Authoritative Guidance

According to Section 6.2 of EOTSS's Information Security Risk Standard IS.010,

*6.2.3 New Hire Security Awareness Training: 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.*

*6.2.4 Annual Security Awareness Training: All **personnel** will be required to complete Annual Security Awareness Training.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still

recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

MSCBA did not have documented policies and procedures that required newly hired employees to complete cybersecurity awareness training within 30 days of their orientation or that required existing employees to complete annual refresher cybersecurity awareness training.

c. The Massachusetts State College Building Authority was missing documentation for a completed background check.

One (7%) out of 15 system users was missing documentation confirming that MSCBA had completed a required background check on them before they gained access to MSCBA's accounting and project management system.

Without proper screening, MSCBA assumes a higher-than-acceptable risk of hiring individuals who may pose security threats to its systems and data.

Authoritative Guidance

According to Section C of MSCBA's *Employee Handbook*, "The Authority will complete background checks for criminal records and social security verification for existing employees every five years and for new employees within 90 days of their start date."

Reason for Issue

According to MSCBA officials, the one employee in our sample who was missing documentation for a completed background check was a post-retiree state employee who was returning to work part-time, and the background check was not performed.

d. The Massachusetts State College Building Authority did not promptly revoke access rights to its accounting and project management system.

MSCBA did not promptly revoke access rights to its accounting and project management system for the one former user whose employment ended during the audit period.

If MSCBA does not promptly revoke former employees' access rights to its system, then there is an increased risk that former employees could improperly access and/or change information in the system.

Authoritative Guidance

According to Section 6 of EOTSS's Access Management Standard IS.003,

> *6.1.8.3 If the termination date of a user is known in advance, the respective access privileges—specifically those with access to confidential information—will be configured to terminate automatically.*
>
> *6.1.8.3.1. If not, access must be manually removed within 24 business hours.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

According to MSCBA officials, the terminated employee whose access was not revoked was on a six-month leave of absence before their employment was terminated.

e. The Massachusetts State College Building Authority did not have session lock mechanisms in place.

MSCBA did not implement session lock mechanisms on its network or within its accounting and project management system. For instance, there was no established protocol for defining a specific duration of user inactivity that would trigger an automatic session lock.

If MSCBA does not have session lock mechanisms in place, then employees may remain logged on indefinitely, increasing the risk of unauthorized access and reducing the organization's ability to effectively monitor and control system activity.

Authoritative Guidance

According to Section 6 of EOTSS's Access Management Standard IS.003,

*6.3.6 An automatic screen saver lock will be configured to become active no more than five (5) minutes after inactivity for workstations used by **personnel** with access to any Commonwealth network and **information system**.*

6.3.6.1 Put devices into sleep or locked mode any time they are not in active use.

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

MSCBA officials could not explain why they do not have a policy for session timeouts for its network or accounting and project management system.

f. The Massachusetts State College Building Authority did not have a documented configuration management policy.

MSCBA did not have a documented configuration management policy for its accounting and project management system to address how changes are processed before they are implemented. The configuration policy should include a testing plan, results of the testing plan, and the process to approve the changes to MSCBA's accounting and project management system. Configuration management ensures that system settings, updates, and security patches are consistently applied.

Without a configuration management policy, MSCBA makes its accounting and project management system vulnerable to misconfigurations, security threats, and performance issues.

Authoritative Guidance

According to Section 6 of EOTSS's Operations Management Standard IS.012,

*6.3 Commonwealth Agencies and Offices must establish controls to maintain the integrity of **information systems**, including: . . .*

*6.3.3. Create, maintain, and update standard operating **procedures** . . . for the secure configuration of **information systems**. Assess compliance with configuration requirements at least annually.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still

recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

MSCBA officials could not explain why MSCBA does not have established controls to ensure that procedures are in place to safeguard its accounting and project management system.

g. The Massachusetts State College Building Authority did not have established procedures to review audit logs.

MSCBA did not establish procedures to conduct regular reviews of audit logs for its accounting and project management system. Our testing found that user activity logs were not reviewed periodically but rather only when issues emerged, which limits the organization's ability to detect unauthorized access or suspicious activity.

If MSCBA does not run regular audit logs of its accounting and project management system, then it exposes itself to a higher-than-acceptable risk of unauthorized user activity. It also exposes itself to a higher-than-acceptable risk that security incidents and policy violations go undetected by MSCBA management.

Authoritative Guidance

According to Section 6 of EOTSS's Logging and Event Monitoring IS.011,

> *6.1.6 **Log** review and reporting*
>
> *Commonwealth Agencies and Offices must ensure that **logs** are periodically reviewed by personnel from the Enterprise Security Office (or **personnel** with a security role in the **agency**) to detect anomalous **events** and apply resolution in a timely manner.*

Although MSCBA is not required to follow this standard, since it is not a Commonwealth agency within the executive branch and is instead categorized as a quasi-governmental agency, EOTSS still recommends that non-executive branch state agencies follow these standards. We also consider them best practices.

Reason for Issue

MSCBA does not have a written policy to ensure that logs are run on a regular basis to track user activity.

Recommendations

1. MSCBA should ensure that documented records are kept to evidence supervisory approval for system user rights for its accounting and project management system.

2. MSCBA should develop and implement policies and procedures to ensure that all employees receive cybersecurity awareness training within 30 days of orientation and annually thereafter. Also, MSCBA should maintain certificates of completion of these trainings for all of its employees.

3. MSCBA should ensure that all employees with access to confidential information undergo background checks, as required by its policy. MSCBA should maintain documentation of these screenings to ensure accountability and compliance.

4. MSCBA should ensure that system privileges are revoked within 24 business hours of termination. Additionally, MSCBA should consider temporarily suspending employees' privileges when they are on leaves of absence.

5. MSCBA should configure both its network and its accounting and project management system to lock out after a five-minute period of inactivity.

6. MSCBA should establish controls to ensure that configuration management procedures are in place to safeguard its accounting and project management system.

7. MSCBA should ensure that audit logs are run for its accounting and project management system on a regular basis, so that system user activity is tracked.

Auditee's Response

1. ***Supervisory review / approval of user access***—*The Authority, through its [information technology (IT)] vendor, currently utilizes forms to establish and terminate user access for its network. Separately, there is a process in place for establishing new employees' access to . . . the Authority's accounting and project management software, however, because network access is required to access [this software], there is a secondary level of control. The Authority acknowledges that it can improve the documentation of this portion of the process and is currently investigating and discussing further enhancements to the Authority's existing processes.*

2. ***Cybersecurity Training***—*Since 2021, the Authority has provided cybersecurity awareness training annually for its employees. These trainings were conducted by the Authority's IT Network Service Provider . . . at an annual "All Staff" meeting. Consistent [with the Office of the State Auditor's (OSA's)] review, the Authority has adopted a more structured and documented approach. Since the informal exit conference with the OSA, the Authority has retrained all staff via its provider's Learning Management System and has current certificates of completion. Existing employees will continue to complete such training annually and new staff members will be required to complete such training within 30 days of hire.*

3. ***Employee Background Checks***—*The Authority's policy is to ensure that all employees undergo appropriate background checks during the hiring process. The omission of a singular employee was in error.*

4. ***Employee Access Changes upon Leave or Termination****—The Authority regards access to the network and its security as a critical component to minimizing risk and routinely ensures that system privileges are revoked within 1 business day of an employee's leave or termination. Moving forward, the Authority will make operational changes to ensure timely revocation of access for separated employees.*

5. ***Inactivity Lockout****—Since the OSA informal exit conference, based on the recommendation of its IT network service provider . . . the Authority has implemented a procedure by which automatic lockout is initiated after 15 minutes of inactivity. The 15-minute lockout standard is based upon the nationally recognized NIST (National Institute of Standards and Technology) recommendation.*

6. ***Network Access / Configuration & Accounting / Project Management . . . Configuration****—The Authority will work with its IT consultants and vendors to develop an IT Configuration Management Plan.*

7. ***Audit Logs for the Accounting / Project Management . . . system****—As previously noted, the Authority considers system access a critical component to minimizing risk and will investigate what reports, logs, and / or other tools are available to provide additional review capabilities of user activity to enhance internal controls.*

Auditor's Reply

Based on its response, MSCBA is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.