Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued June 11, 2018

Massachusetts Clean Energy Center

For the period July 1, 2015 through June 30, 2017

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

June 11, 2018

Mr. Matthew Beaton, Secretary
Executive Office of Energy and Environmental Affairs
100 Cambridge Street, Suite 900
Boston, MA 02114

Dear Secretary Beaton:

I am pleased to provide this performance audit of the Massachusetts Clean Energy Center. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2015 through June 30, 2017. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Massachusetts Clean Energy Center for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

BCP	business-continuity plan
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DRP	disaster-recovery plan
DHS	Department of Homeland Security
EOTSS	Executive Office of Technology Services and Security
FBI	Federal Bureau of Investigation
IT	information technology
MassCEC	Massachusetts Clean Energy Center
RETF	Renewable Energy Trust Fund
WTTC	Wind Technology Testing Center

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 Massachusetts Clean Energy Center (MassCEC) for the period July 1, 2015 through June 30, 2017.

In this performance audit, we examined whether (1) MassCEC's Wind Technology Testing Center generated sufficient revenue to cover its expenses; (2) MassCEC had a positive track record of investing in Massachusetts companies (i.e., had invested in companies that were financially viable); (3) MassCEC properly administered the Equity Investment and Venture Debt Investments Programs; (4) MassCEC had adequate internal controls (i.e., policies and procedures) over the processing of wire transfers and internal fund transfers; and (5) MassCEC developed a disaster-recovery plan (DRP)[1] and business-continuity plan (BCP)[2] for its computer operations. Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 6**	MassCEC did not prevent or properly report the theft of $93,679 in public funds.
Recommendations **Page 8**	1. MassCEC should conduct risk assessments and develop written policies and procedures to manage all risks to its operations, including its exposure to cybercrime, and immediately inform its board of directors of any incidents, including security breaches perpetrated against the organization. 2. MassCEC should consider adopting elements of the Committee of Sponsoring Organizations of the Treadway Commission's model in developing control activities to prevent, detect, and mitigate cyber-risks.
Finding 2 **Page 9**	MassCEC did not develop DRPs and BCPs for its computer systems.
Recommendation **Page 10**	MassCEC should assess its computer systems from a risk-management and business-continuity perspective and develop and test an appropriate DRP and BCP. It should reassess such plans at least annually or upon major changes to its operations or overall information-technology environment.

1. A DRP is an information-system-based plan designed to allow for quick recovery of critical systems, applications, and information-technology infrastructure in the event of a large-scale disaster.
2. A BCP is a plan that develops risk-based strategies to mitigate identified potential threats to business operations. At a minimum, it should include a DRP and continuity-of-operations plan.

OVERVIEW OF AUDITED ENTITY

The Massachusetts Clean Energy Center (MassCEC) is an independent governmental entity within, but not under the supervision of, the Executive Office of Energy and Environmental Affairs. It was established by Chapter 23J of the Massachusetts General Laws and began operations in 2009. MassCEC is governed by a 12-member board of directors. Seven of the board members are ex officio; the rest are from the private and public sectors and are appointed by the Governor. The board has three committees: the Audit Committee, the Compensation Committee, and the Investments Committee. By statute, the board is chaired by the Secretary of Energy and Environmental Affairs. The board meets seven times each year to vote on programmatic and fiscal decisions and is governed by bylaws that are reviewed and updated as needed. During our audit period, MassCEC had 60 employees in its six departments: Corporate, Innovation and Industry Support, Investments, Offshore Wind, Renewable Energy Generation, and the Wind Technology Testing Center (WTTC). MassCEC's main office is at 63 Franklin Street and WTTC is at 80 Terminal Street in Boston.

According to its website,

> *MassCEC's mission is to grow the state's clean energy economy while helping to meet the Commonwealth's clean energy, climate and economic development goals. . . .*
>
> *MassCEC funds more than 40 programs including incentives for clean energy technology installations, financing for early stage companies and technology development as well as investments in training programs to build a clean energy workforce. . . .*
>
> *MassCEC fosters collaboration among the industry, state government, research universities and the financial sector to advance the state's clean energy economy.*

In November 2009, An Act Relative to Clean Energy transferred the state's Renewable Energy Trust Fund (RETF) from the Massachusetts Technology Park Corporation to MassCEC. The RETF is funded by a renewable-energy surcharge of $0.0005 per kilowatt-hour paid by ratepayers of public and participating municipal electric utilities in Massachusetts. Proceeds from the surcharge totaled $22,784,856 in 2016 and $22,649,352 in 2017, representing approximately $0.29 per month paid by each residential customer. MassCEC uses the proceeds from the RETF to fund its operations.

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 Massachusetts Clean Energy Center (MassCEC) for the period July 1, 2015 through June 30, 2017.

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 the Wind Technology Testing Center (WTTC) generate sufficient revenue to cover operating expenses?	**Yes**
2. Did MassCEC have a record of investing in financially viable Massachusetts companies?	**Yes**
3. Does MassCEC properly administer the Equity Investment and Venture Debt Investments Programs?	**Yes**
4. Does MassCEC have adequate internal controls, including policies and procedures, over the processing of wire transfers and internal fund transfers?	**No; see Finding 1**
5. Did MassCEC have a disaster-recovery plan (DRP) and business-continuity plan (BCP) in place for its computer operations?	**No; see Finding 2**

To achieve our audit objectives, we gained an understanding of MassCEC's internal control environment related to our audit objectives by reviewing applicable laws, agency policies, and procedures, as well as conducting inquires with MassCEC management regarding investment performance. We evaluated the design and tested the operating effectiveness of controls over WTTC; investments made in clean energy companies in Massachusetts; the administration of the Equity Investment and Venture Debt Investments Programs; the processing of wire transfers and internal fund transfers; and the existence of

a DRP and BCP for MassCEC's computer operations. In addition, the audit team performed the following procedures:

- To determine whether WTTC generated sufficient revenue to cover its operating expenses, we compared the financial statements and annual budgets of WTTC to the audited financial statements of MassCEC for fiscal years 2016 and 2017. We verified actual rent paid using the monthly bank statements for the audit period and reviewed the depreciation schedules[3] of assets and the allocation of MassCEC expenses. We also attended a MassCEC Audit Committee meeting during which the independent external auditors presented an analysis of WTTC's financial position.

- To determine whether MassCEC had a record of investing in financially viable Massachusetts companies, we reviewed all 14 contract agreements of the companies in which MassCEC invested during the audit period. We reconciled MassCEC's list of investments in companies during our audit period to its audited financial statements to confirm our population of investments. We verified with the Office of the Secretary of the Commonwealth (Corporations Division) that each of these companies was headquartered in Massachusetts. We reviewed the audited financial statements for the companies in which MassCEC invested to identify revenue growth and declines during the audit period.

- We examined reports MassCEC prepared that provided performance metrics for investments made during fiscal years 2016 and 2017. We verified information in supporting documentation regarding companies invested in by MassCEC, such as the total number of employees, the total funding raised from other investors, the valuations performed by MassCEC, the total revenue generated, and MassCEC's investment returns on these companies.

- We reviewed the agency's financial records related to investments that were written down as uncollectable during our audit period, prepared an analysis of gains and losses, and reconciled the investments to MassCEC's audited financial statements. We interviewed MassCEC's director of investments to discuss the agency's investment portfolio performance.

- To determine whether MassCEC properly administered its Equity Investment and Venture Debt Investments Programs, we reviewed all the awards made by MassCEC through these programs during the audit period and confirmed that they received proper approvals from the agency's chief executive officer, chief financial officer, general counsel, managing director of investments, board of directors, and/or investment committee in accordance with the agency's bylaws.

- We verified that each of the 14 companies MassCEC invested in during our audit period certified that its financial statements were presented in accordance with generally accepted accounting principles.

- To determine whether MassCEC had adequate internal controls, including policies and procedures, over the processing of internal fund transfers, we selected a sample of 8 out of 24 months of internal fund transfers during the audit period and verified that MassCEC's controller had approved these transactions via electronic signature. We reviewed all fund transfers to

3. A depreciation schedule is a detailed report of fixed assets that shows annual and accumulated reductions in their value.

ensure that all transfers were performed and no funds were misappropriated. We then reviewed all supporting documentation, including letters from the Massachusetts Department of Energy Resources related to the dispersal of Alternative Compliance Payments,[4] internal emails, minutes of board meetings (if applicable), spreadsheets, and invoices, to confirm that the controller had properly authorized the transactions.

- We chose a sample of 20 out of the 75 wire transfers that were performed during the audit period to determine whether MassCEC's controller and personnel at the appropriate level of management (chief financial officer, chief executive officer, and chief operating officer) had approved each transaction and whether each transaction had the appropriate supporting documentation.

- To assess the adequacy of system availability, we determined whether formal (i.e., documented, tested, and board-approved) planning had been performed to develop and maintain a DRP and BCP to resume computer operations should the network application systems become inoperable or inaccessible. We also determined whether mission-critical application systems had been assessed for security vulnerabilities and whether risks to computer operations had been evaluated by MassCEC's management in conjunction with the agency's Information Technology Department (within its Corporate Department).

We used data from MassCEC's Great Plains accounting and customer relationship management system to review equity investment and venture debt activity, internal and external bank transfers, and user access security during our audit period. We reviewed the controls in place for access to the data, program changes, and computer operations. We compared system reports to the audited financial statements, traced system financial information to bank statements and invoices, and determined that the data from these systems were sufficiently reliable for the purposes of our audit.

We used nonstatistical sampling to help achieve our audit objectives and therefore did not project our results to the various populations.

4. Retail electricity suppliers can make Alternative Compliance Payments to the Massachusetts Department of Energy Resources, collected by MassCEC to comply with the Massachusetts Renewable Energy Portfolio Standard and Alternative Energy Portfolio Standard regulations.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Massachusetts Clean Energy Center did not prevent or properly report the theft of $93,679 in public funds.

The Massachusetts Clean Energy Center (MassCEC) did not have effective internal controls (i.e., policies and procedures) in place for the wire transfer of agency funds. As a result, a cyberscammer was able to get a MassCEC official to transfer $93,679 in public funds to an account the scammer controlled. Most of these funds were not recovered, so the agency was unable to use them to further its mission of promoting clean energy technology, projects, and companies.

Further, MassCEC management did not inform the agency's board of directors of this theft in a timely manner. Specifically, although the theft occurred on January 9, 2017 and was detected by MassCEC on February 3, 2017, MassCEC management did not inform its board of the theft until September 15, 2017. As a result, the board could not provide timely guidance regarding any measures that should be taken to address the problem and prevent this from happening in the future.

In addition, although MassCEC verbally contacted the Commonwealth's Office of the Attorney General and the Boston Police Department about this matter, it never formally filed a criminal complaint concerning the theft. Although MassCEC eventually recovered $25,261 of the stolen funds from the bank where they had been deposited, if the agency had officially requested the assistance of law enforcement, it might have been able to prosecute the perpetrator and recover additional funds.

Authoritative Guidance

The most widely used framework for internal controls in the United States was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and represents best practices that should be used by organizations such as MassCEC in their development of effective internal control systems. The COSO document *Internal Control—Integrated Framework* adopted the concept of enterprise risk management, a key element of which is an organization's identification and assessment of the risks inherent to its operations that could prevent the accomplishment of its mission and goals and the controls in effect to mitigate those risks.

COSO specifically refers to cyber-risks and methods to prevent and detect fraud in its 2015 report *COSO in the Cyber Age:*

> *When a company manages cyber risk through a COSO lens, it enables the board of directors and senior executives to better communicate their business objectives, their definition of critical information systems, and related risk tolerance levels. This enables others within the organization, including [information technology, or IT] personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, the likely attack methods, and the points of intended exploitation. In turn, appropriate control activities can be put in place to address such risks. . . .*
>
> *Because cyber risk exposure can come from many entry points, both internal and external to the organization, preventive and detective controls should be deployed to mitigate cyber risks. . . .*
>
> *Effective communication between the board of directors and management, including senior executives and operational management, is critical for the board to exercise its internal control oversight responsibilities.*

In addition, the federal Department of Homeland Security (DHS) provides guidance on reporting cybercrimes and suggests reporting such incidents to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center. In its bulletin Cyber Incident Reporting, published September 22, 2016, DHS advises victims to "report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to the FBI Field Office Cyber Task Forces."

Reasons for Issues

Although MassCEC management did perform a risk assessment of its business activities to identify any potential risks, it did not consider cyberthreats as part of that overall assessment. Conducting a risk assessment regarding cyberthreats would have allowed MassCEC to identify the need to develop effective internal controls (i.e., policies and procedures) to mitigate risks in this area and prevent the improper transaction from occurring.

MassCEC did not have written policies and procedures in place to promptly notify the board of directors of incidents or actions such as thefts or breaches of information security controls within a specific timeframe. Furthermore, MassCEC management said that they were unaware of the guidelines promulgated by DHS regarding reporting cybercrimes to the FBI's Internet Crime Complaint Center.

According to MassCEC management, they believed they had fulfilled their obligations to report the theft by verbally contacting the Massachusetts Office of the Attorney General and the Boston Police Department.

Recommendations

1. MassCEC should conduct risk assessments and develop written policies and procedures to manage all risks to its operations, including its exposure to cybercrime, and immediately inform its board of directors of any incidents, including security breaches perpetrated against the organization.

2. MassCEC should consider adopting elements of the COSO model in developing control activities to prevent, detect, and mitigate cyber-risks.

Auditee's Response

MassCEC takes the stewardship of public funds very seriously. Upon discovering the fraudulent activity, management immediately contacted its bank and successfully recovered $25,261, or 27% of the funds. In February 2017 when the event was identified, management conducted an immediate review and enhancement of internal controls. Additional layers of IT security and enhanced internal controls around wire transfers were implemented quickly to prevent and detect fraud from occurring in the future. Examples of these additional internal controls include requiring employees take an IT security training course annually, additional verification steps for vendor banking information for wire transfers, and the installation of software that blocks known fraudulent websites.

MassCEC has in place a risk assessment that identifies potential risks to the organization and internal controls and procedures to mitigate those risks, which is periodically reviewed and updated. Management will enhance this risk assessment to include cyber security. MassCEC management will continue to monitor the ongoing trends and constantly changing cyber threat environment and will further enhance our internal controls and procedures as appropriate to mitigate the risks of future events. As recommended by the auditor, MassCEC will consider adopting elements of the COSO model, including incorporating the general framework into our existing risk assessment model and in developing control activities to prevent, detect and mitigate risk.

With respect to the issue of reporting, we are committed to taking more timely action to notify the members of our Board of Directors, should similar incidents occur in the future. However, we wish to clarify that, in response to the incident at issue, MassCEC did notify the Chair of the Audit Committee and the office of our Board Chair in July 2017, prior to the full Board notification in September 2017.

MassCEC has also enhanced our existing policies and procedures to require timely reporting of all thefts of funds or property to relevant authorities and our Board of Directors. The enhanced policy requires management to immediately inform the Chief Executive Officer upon discovery of a fraudulent event or theft, and the Chief Executive Officer and/or Chief Financial Officer to inform the Board of Directors and relevant authorities in a timely manner. For cybercrime events, the policy requires management to report the incident to the Federal Bureau of Investigation's Internet Crime Complaint Center.

2. MassCEC did not develop disaster-recovery and business-continuity plans for its computer systems.

Although MassCEC stores backup copies of its own network-based information both on site and off site, it did not have a documented and tested disaster-recovery plan (DRP) or business-continuity plan (BCP) for restoring system functionality if its computer systems were rendered inoperable or inaccessible.

The lack of a documented, tested, and approved plan to address the resumption of system functionality may significantly affect MassCEC's efforts to properly recover and restore mission-critical and confidential data. Further, without such a plan, MassCEC could experience delays in reestablishing mission-critical software for processing transactions, financial data, and sales and marketing performance data. Recovery tests are a key component of an effective BCP.

Authoritative Guidance

The Enterprise Business Continuity for IT Management Policy issued June 5, 2013 by the Executive Office of Technology Services and Security (EOTSS) states,

> 1. *Agencies are required to develop, implement, test and maintain a Business Continuity Plan (BCP) for all Information Technology Resources (ITR) that deliver or support core Critical Business Functions on behalf of the Commonwealth of Massachusetts. . . .*
>
> 8. *Agencies are required to document, implement and annually test plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters.*

In addition, EOTSS's Enterprise Information Security Policy requires agencies to do the following:

> *Document, implement and annually test plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters via adoption of:*
>
> - *Continuity of operations plan and*
> - *A disaster recovery plan.*

Although MassCEC may not specifically be required to follow these policies, they represent a best practice that should be followed by all Commonwealth government organizations, including MassCEC.

Reasons for Issues

MassCEC's management said they believed that the agency's plan for storing backup data off site, described in its internal control plan, was sufficient documentation for the restoration of its computer systems. However, MassCEC's plan did not contain the elements that a BCP or DRP is required to include.

Recommendation

MassCEC should assess its computer systems from a risk-management and business-continuity perspective and develop and test an appropriate DRP and BCP. It should reassess such plans at least annually or upon major changes to its operations or overall IT environment.

Auditee's Response

MassCEC is committed to strengthening our IT operations, and has continually enhanced our IT environment, policies and procedures over the last several years. As previously discussed with the audit team, MassCEC has disaster recovery and offsite data backup procedures which have been documented and are periodically tested. We acknowledge that certain elements were not documented in a centralized policy. In response to the state auditor's recommendation, management is in the process of enhancing the current backup and disaster recovery procedures by formalizing them into a centralized business continuity and disaster recovery plan in order to ensure more effective communication and implementation throughout the entire organization. This enhancement will include a requirement to assess the plans at least annually or upon a significant change to the overall IT environment.

APPENDIX

Departments within the Massachusetts Clean Energy Center

- The Corporate Department of the Massachusetts Clean Energy Center is composed of legal, finance, human resources, information technology, operations, communications, and administrative personnel.

- The Innovation and Industry Support Department helps clean energy companies develop technologies and meet the workforce needs of the industry.

- The Investments Department is responsible for direct equity and venture debt investments in clean energy companies in Massachusetts.

- The Offshore Wind Department conducts projects and research to further the offshore industry and manages the New Bedford Marine Commerce Terminal, a 21-acre facility in the Port of New Bedford for accommodating cargo vessels and supporting offshore wind projects.

- The Renewable Energy Generation Department promotes renewable-energy deployment.

- The Wind Technology Testing Center provides certification testing for wind turbine blades.