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

Official Audit Report – Issued March 19, 2019

Commonwealth Corporation

For the period July 1, 2015 through June 30, 2018

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

March 19, 2019

Ms. Rosalin Acosta, Chair of the Board of Directors
Commonwealth Corporation
2 Oliver Street
Boston, MA 02190

Dear Ms. Acosta:

I am pleased to provide this performance audit of Commonwealth Corporation. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2015 through June 30, 2018. 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 Commonwealth Corporation 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

CEO	chief executive officer
CommCorp	Commonwealth Corporation
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CTR	Comptroller of the Commonwealth
EOAF	Executive Office for Administration and Finance
IT	information technology
PII	personally identifiable information
WTFP	Workforce Training Fund Program

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 Commonwealth Corporation (CommCorp) for the period July 1, 2015 through June 30, 2018. In this performance audit, we examined certain activities of CommCorp's administration of the General Program within its Workforce Training Fund Program, its protection of personally identifiable information in its records, and its compliance with the General Laws regarding providing its financial records to the Secretary of Administration and Finance for public disclosure.

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

Finding 1 **Page 7**	CommCorp did not adequately protect confidential employee information.
Recommendations **Page 8**	1. CommCorp should develop policies and procedures that require periodic security awareness training for all employees. 2. CommCorp should consider adopting security practices outlined by the Committee of Sponsoring Organizations of the Treadway Commission to enhance its control activities to prevent, detect, and mitigate cyber-risks.
Finding 2 **Page 9**	CommCorp did not submit required payroll and expenditure information to the Commonwealth to be made available to the public on a searchable website.
Recommendations **Page 9**	1. CommCorp should contact the Comptroller of the Commonwealth (CTR) to obtain an understanding of how to submit information to the Executive Office for Administration and Finance for posting to CTR's searchable website and submit all the required information for fiscal and calendar years 2016 and 2017 as well as any deficient fiscal and calendar years before our audit period. 2. CommCorp should develop and implement policies and procedures for collecting the required payroll and expenditure information and submitting it to the Secretary of Administration and Finance for posting to CTR's website. CommCorp should also establish monitoring controls to ensure that the policies and procedures are adhered to.

OVERVIEW OF AUDITED ENTITY

Commonwealth Corporation (CommCorp) is a quasi-public agency that was established in 1996 through the merger of two Massachusetts nonprofit organizations: the Industrial Service Program and the Bay State Skills Corporation. The agency was then known as the Corporation for Business, Work and Learning until March 2001, when it began doing business under the name "Commonwealth Corporation" by a resolution of its board of directors. The Legislature formally approved the name change in September 2004.

The agency is responsible for administering and delivering a wide range of publicly and privately funded programs. According to CommCorp's website, its primary goals are as follows:

- *to build regional industry training partnerships that prepare youth and unemployed workers for jobs in demand that lead to higher rates of employment;*
- *to upgrade the skills of underemployed workers to meet specific employer skill demands leading to job retention, upgrades and wage gains, and;*
- *to increase the share of youth engaged in education and employment pathways preparing them for post-secondary education and careers.*

CommCorp is governed by a 19-member board of directors that includes leaders from the private sector, organized labor, academia, and government.

CommCorp is responsible for administering the Workforce Training Fund Program's (WTFP's) General Program Training Grant through an annual contract with the Executive Office of Labor and Workforce Development. The program's purpose is to enhance business productivity and competitiveness by providing resources to medium-sized and small businesses to upgrade their workforces' skills. It is funded by the Commonwealth through unemployment tax payments, which are deposited in the Unemployment Insurance Trust Fund. The funds are distributed back to businesses that apply and are selected for funding for employee training grants. The trust fund pays 50% of the total cost of a selected business's employee training programs; the business is responsible for the other 50%. CommCorp works with the Workforce Training Fund Advisory Board, an independent board composed of Massachusetts employers, nonprofit organizations, labor organizations, and experts in workforce training, to select the grant recipients. The table below shows the amounts of the training grants CommCorp awarded through the WTFP General Program during the audit period.

Fiscal Year	Total Number of Recipients	Total Amount Awarded
2016	185	$18,160,351
2017	206	$17,954,768
2018	152	$16,884,235

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 Commonwealth Corporation (CommCorp) for the period July 1, 2015 through June 30, 2018.

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. Does CommCorp administer the Workforce Training Fund Program's (WTFP's) General Program in such a way that CommCorp can effectively achieve the stated goals of awarding and monitoring grants to projects that will upgrade workers' skills, increase productivity, and enhance the competitiveness of Massachusetts businesses?	**Yes**
2. Does CommCorp properly administer the dissemination of personally identifiable information (PII)?	**No; see Finding 1**
3. Does CommCorp post payroll and expenditure information to the Commonwealth's CTHRU website[1] as required by Section 14C of Chapter 7 of the General Laws?	**No; see Finding 2**

To achieve our objectives, we gained an understanding of CommCorp's internal control environment as it relates to our audit objectives by reviewing applicable laws and agency policies and procedures and by conducting inquires with management regarding the administration of the WTFP General Program. We evaluated the design and tested the operating effectiveness of CommCorp's controls over WTFP General Program Training Grant activity.

We also performed the following procedures.

1. CTHRU is a Web-based application provided by the Comptroller of the Commonwealth to allow public access to state spending and payroll data. Payroll information is posted by calendar year, whereas expenditures are posted by fiscal year.

- To determine whether CommCorp had adequately selected and awarded grants to eligible businesses, we selected a random nonstatistical sample of 27 out of 160 WTFP General Program grantees that were awarded grants during our audit period and assessed the information they provided in applying for grants to determine whether they met program eligibility requirements.

- To determine whether CommCorp actively monitored individual grant awards after they were distributed to recipients, we obtained a list of all WTFP General Program grants awarded and closed out[2] before grant completion during the audit period. We selected a random nonstatistical sample of 27 out of 160 WTFP General Program grants that were issued and closed during our audit period and reviewed each grant to determine whether the goals regarding job creation and business productivity were achieved. We obtained and reviewed records of all WTFP General Program site visits to grantee businesses by CommCorp's program managers during the audit period.

- To determine whether CommCorp properly administered the dissemination of PII, we reviewed policies and procedures for information technology (IT) security, conducted interviews with members of senior management who were responsible for protecting confidential information, and further reviewed the support for security awareness training provided during the audit period.

- Regarding the data breach[3] that occurred on March 19, 2018, we interviewed key managers involved, including the president / chief executive officer, the chief financial officer, and the IT specialist. We then reviewed supporting documentation of CommCorp's response to the data breach, including internal and external notification letters sent to employees and outside agencies.

- We examined the state's publicly available, searchable website CTHRU to determine whether it included data for CommCorp expenditures, including payroll, to ensure transparency with regard to the agency's spending. We conducted interviews with senior management and documented their methods of reporting financial and payroll information as required.

We used data from CommCorp's grant management system (Salesforce) to select our test sample in reviewing grant performance. We reviewed the controls in place for access to the data, program changes, and personnel screening. We further compared a random sample of 20 Fiscal Status Reports[4] from Salesforce to the Fiscal Status Reports from AccuFund, CommCorp's accounting and reporting system. We determined that the data from Salesforce were sufficiently reliable for the purposes of our audit.

2. Closing out is the final step in the grant distribution process, whereby the recipient receives the grant, having satisfied WTFP General Program requirements.
3. A data breach occurs when someone gains unauthorized access to confidential information.
4. These required quarterly financial reports are submitted electronically by WTFP General Program grantees to CommCorp to provide information on the current status of grant spending activities.

Where sampling was used, we used nonstatistical judgmental samples; therefore, we could not project the results of our tests to the entire population.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. Commonwealth Corporation did not adequately protect confidential employee information.

Commonwealth Corporation (CommCorp) did not adequately ensure that it protected its employees' personally identifiable information. On March 19, 2018, a hacker impersonating CommCorp's president / chief executive officer (CEO) gained unauthorized access to CommCorp's email system. The hacker accessed payroll data from 164 current and former employees' federal W-2 forms for the period 2008 through 2017. Although the data were protected by encryption[5] software, a payroll employee emailed the encryption password to the hacker. The hacker also attempted to transfer $3,500 from an online bank account, which alerted CommCorp management to the breach of its systems by an unauthorized party. Upon realizing that its systems had been compromised, CommCorp management notified the board of directors and the Executive Office of Labor and Workforce Development, which in turn notified the Governor's Office, the Attorney General's Office, the Executive Office of Technology Services and Security, the Office of the Secretary of the Commonwealth, and the Office of Consumer Affairs and Business Regulation. In addition, CommCorp notified the Internal Revenue Service and the Federal Bureau of Investigation; it also sent written notifications to all current and former employees affected by the breach and committed to providing identity theft monitoring services for three years to all affected individuals. Current and former employees affected by this breach may be at risk of fraud.

Authoritative Guidance

According to CommCorp's "Internal Policies and Procedures Password Policy," dated October 11, 2016, "Passwords must not be inserted into email messages."

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 CommCorp in their development of effective internal control systems, including controls over information security 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

5. Encryption software is an extra security measure used to prevent unauthorized disclosure of sensitive information.

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] 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 into 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.*

Reasons for Issues

According to CommCorp management, a payroll employee believed that the hacker was actually the president / CEO and forwarded the information that the hacker requested. In addition, we found that CommCorp had not developed policies and procedures that required employees to participate in computer security awareness training.

Recommendations

1. CommCorp should develop policies and procedures that require periodic security awareness training for all employees.
2. CommCorp should consider adopting security practices outlined in the COSO model to enhance its control activities to prevent, detect, and mitigate cyber-risks.

Auditee's Response

> *Commonwealth Corporation takes the protection of personally identifiable information seriously. We have updated our Information Technology policies and procedures to strengthen policy and practice regarding the use and protection of personally identifiable information. Updated policies have been distributed to staff and are now included in new hire orientation. Our updated procedures include mandatory annual Information Technology security training for all staff. This training has already been conducted for all current staff on December 20, 2018 and January 14, 2019.*

2. CommCorp did not submit required payroll and expenditure information to the Commonwealth to be made available to the public on a searchable website.

During our audit period, CommCorp submitted incomplete payroll and expenditure information (payroll data and financial statements) to the Executive Office for Administration and Finance (EOAF) to be made available to the public on a searchable website. Specifically, for calendar year 2016, there was no CommCorp payroll information on the CTHRU website, nor was there any expenditure or payroll information for fiscal and calendar year 2017. As a result, CommCorp did not allow the Commonwealth to give the public a sufficient level of transparency regarding CommCorp's operations, including its overall financial health and the nature and extent of its expenses.

Authoritative Guidance

Section 14C of Chapter 7 of the Massachusetts General Laws requires agencies, including quasi-public independent entities such as CommCorp, to report their "appropriations, expenditures, grants, subgrants, loans, purchase orders, infrastructure assistance and other forms of financial assistance" to the Secretary of EOAF for inclusion on the Comptroller of the Commonwealth's (CTR's) searchable website. Section 14C(e) states, "All agencies shall provide to the secretary all data that is required to be included in the searchable website not later than 30 days after the data becomes available to the agency."

Reasons for Noncompliance

According to CommCorp management, they were aware of the financial reporting requirements but not the procedures they needed to follow to meet them. In addition, CommCorp had not established policies and procedures regarding the submission of this information to EOAF for inclusion on CTR's searchable website.

Recommendations

1. CommCorp should contact CTR to obtain an understanding of how to submit information to EOAF for posting to CTR's searchable website and submit all the required information for fiscal and calendar years 2016 and 2017 as well as any deficient fiscal and calendar years before our audit period.

2. CommCorp should develop and implement policies and procedures for collecting the required payroll and expenditure information and submitting it to the Secretary of EOAF for posting to CTR's

website. CommCorp should also establish monitoring controls to ensure that the policies and procedures are adhered to.

Auditee's Response

Throughout the audit period Commonwealth Corporation maintained several years of audited financial statements on our website. Commonwealth Corporation has been engaged with the Office of the Comptroller since April 2018 to ensure the submission and posting of all required financial information. Payroll data for ten years, 2009–2018, are now posted on the Comptroller's CTHRU searchable website. We are actively working with the Office of the Comptroller to upload financial expenses to the CTHRU website.

Commonwealth Corporation has developed policies and procedures to ensure payroll and expense data are uploaded to the Commonwealth's CTHRU searchable website every year. The policies and procedures include the responsibility of the Director of Human Resources to serve in a monitoring capacity to ensure adherence to the policy and procedures.