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

Official Audit Report – Issued April, 15, 2021

Westfield State University

For the period October 1, 2018 through March 31, 2020

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

April 15, 2021

Roy Saigo, PhD, Interim President
Westfield State University
577 Western Avenue
Westfield, MA 01085

Dear Dr. Saigo:

I am pleased to provide this performance audit of Westfield State University. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, October 1, 2018 through March 31, 2020. My audit staff discussed the contents of this report with management of the university, whose comments are reflected in this report.

I would also like to express my appreciation to Westfield State University for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Kevin R. Queenin, Chair of the Board of Trustees

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CTR	Office of the Comptroller of the Commonwealth
EFT	electronic fund transfer
EOTSS	Executive Office of Technology Services and Security
IRS	Internal Revenue Service
MMARS	Massachusetts Management Accounting and Reporting System
OSA	Office of the State Auditor
WSU	Westfield State University

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 Westfield State University (WSU) for the period October 1, 2018 through March 31, 2020.

In this performance audit, we reviewed WSU's information system security awareness training practices to determine whether its system users had completed required information system security awareness training. We also determined whether WSU had complied with its procedures, as well as policies issued by the Office of the Comptroller of the Commonwealth, when processing state vendors' requests to create or change payment information and other information in the state's accounting system, the Massachusetts Management Accounting and Reporting System.

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

Finding 1 **Page 7**	WSU did not always perform or document a verification of vendor/customer information.
Recommendations **Page 8**	1. WSU should amend its procedures to ensure that verification is properly performed before creations or changes are processed and require all personnel to document the measures they take to verify the information vendors provide in requests to create or change information in their files. 2. WSU should implement effective monitoring controls (e.g., a supervisory review process) to ensure that its staff complies with this requirement.
Finding 2 **Page 9**	WSU did not ensure that information system security awareness training was completed as required by the Executive Office of Technology Services and Security.
Recommendations **Page 10**	1. WSU should implement a formal information system security awareness training program requiring new users to receive training and existing users to be retrained annually. 2. WSU should establish monitoring controls to ensure that all of its employees with access to its systems comply with these requirements.

OVERVIEW OF AUDITED ENTITY

Westfield State University (WSU) was established by Section 5 of Chapter 15A of the Massachusetts General Laws and operates under the direction of a board of trustees, the members of which are appointed by the Governor. The board is responsible for reviewing the university's mission, appointing a president, and approving the annual budget. Its officers include a chair, a vice chair, an alumni trustee, a student trustee, a secretary, and other members, as well as the president of the university, who is an ex officio member.

WSU is a member of the Massachusetts public higher-education system, which consists of 15 community colleges, nine state universities, and five University of Massachusetts campuses. WSU is a public institution that offers undergraduate and graduate programs in the liberal arts, sciences, and professional studies. It is a department of the Commonwealth and receives funding through state appropriations, tuition and fees, investment income, capital grants, and other sources. In 2019, WSU received appropriations of $39 million from the Commonwealth. According to its website, for fiscal year 2020, WSU had 5,810 students enrolled in credit and non-credit courses.

Vendor/Customer File Information and Changes

When a state agency enters into contracts with a vendor, the agency must first obtain information, such as the vendor's legal name, address, and electronic fund transfer (EFT) information, from the vendor. EFT information is required for all statewide vendors that receive multiple payments, so that the Commonwealth can transmit payments directly into their bank accounts. When registering a new vendor, a state agency must also obtain from the vendor a completed Internal Revenue Service (IRS) W-9 form ("Request for Taxpayer Identification Number and Certification"), which allows the vendor to provide the state with a unique taxpayer identification number that the vendor needs in order to be paid. Once the agency obtains this information, it is stored in a vendor/customer file in the Massachusetts Management Accounting and Reporting System (MMARS), the official accounting record of the Commonwealth. The agency is responsible for reviewing and updating the information as necessary to ensure that it is accurate. Pursuant to policies issued by the Office of the Comptroller of the Commonwealth (CTR), when a vendor wants to change any of its information in MMARS, it must contact the agency it is working with, inform the agency of the necessary change, and provide documentation to support the change. Once a state agency receives a request to change information in a MMARS

vendor/customer file, it must collect supporting documentation for the change; verify the change with an authorized signatory by phone; process the change; and notify CTR, providing the aforesaid documentation. WSU procedures incorporate these requirements except the documentation of the follow-up with the vendor.

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 Westfield State University (WSU) for the period October 1, 2018 through March 31, 2020.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and where each objective is discussed in the audit findings.

Objective	Conclusion
1. Does WSU comply with its procedures and the "Vendor/Customer File and W-9s" policy issued by the Office of the Comptroller of the Commonwealth (CTR) for making changes to information in state vendor/customer files in the Massachusetts Management Accounting and Reporting System (MMARS)?	**No; see Finding 1**
2. Does WSU adhere to Sections 6.2.3 and 6.2.4 of the Executive Office of Technology Services and Security's "Information Security Risk Management Standard" for information system security awareness training?	**No; see Finding 2**

To achieve our objectives, we gained an understanding of WSU's internal control environment related to the objectives by reviewing policies and procedures, as well as conducting inquiries with WSU officials. In addition, we performed the following procedures to address our audit objectives.

Initially, we requested from WSU a list[1] of all information about the 15 requests made by WSU vendors for creations of, or changes to, vendor/customer files during the audit period. WSU officials told us during discussions that in 2 of these 15 instances, no changes had been made and the requests had been discarded. We confirmed that the 2 discarded files did not appear in the list of vendors in MMARS.

1. The information was not generated by a system; rather, it was produced from university documentation (e.g., Internal Revenue Service W-9 forms submitted by vendors to the university to provide identifying information to help the university prepare information return filings with the Internal Revenue Service).

For the other 13 requests, we confirmed WSU's compliance with its procedures and CTR's "Vendor/Customer File and W-9s" policy. To do this, we reviewed each file to see whether it included the following: a completed Internal Revenue Service (IRS) W-9 form ("Request for Taxpayer Identification Number and Certification"), electronic fund transfer (EFT) forms, information from the IRS website about the vendor (e.g., tax identification number, address, and legal name), a business entity summary[2] from the Secretary of the Commonwealth's website to verify the vendor's information, and a letter to CTR detailing the file creation or change. Using the evidence in each vendor/customer file, we determined whether WSU collected the W-9 and/or EFT forms. In addition, we reviewed each vendor/customer file for evidence of WSU verifying the information on the W-9 or EFT against independent sources (IRS or Secretary of the Commonwealth website) and notifying CTR of the creation or change.

We conducted inquiries with the head of the Human Resources Department, the vice president of administration and finance, and the chief information officer to determine whether information system security awareness training was provided to employees with access to WSU information systems.

Data Reliability

In 2018, OSA conducted an assessment of MMARS (Project #2017-8020-14O) the focus of which was on testing selected system controls, including access controls, application controls, configuration management, contingency planning, and segregation of duties, for the period April 1, 2017 through March 31, 2018. During our current audit, we reviewed policies and procedures for security awareness training and personnel, and we conducted testing to verify that personnel with access to the systems were screened before they were given access.

In addition, WSU compiled for us a list of vendor creations and changes made in MMARS during the audit period, showing the vendor name, date of occurrence, and description for each change. We traced all of the creations and changes from the Commonwealth Information Warehouse[3] vendor table (which contains all vendor information entered in MMARS and provides details on any changes made to vendor information) to the WSU-compiled list for completeness. We also verified the accuracy of the vendor list by tracing the information on the list back to the supporting documentation (i.e., W-9 forms, letters

2. A business entity summary details information about an organization, including tax identification number, legal name, and address.
3. According to the website of the Executive Office for Administration and Finance, the Commonwealth Information Warehouse is a repository of "financial, budgetary, human resource, payroll and time reporting information."

written to CTR detailing the creation or change, and EFT forms). We determined that the list of vendor creations and changes in MMARS was sufficiently reliable for our audit purposes.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. Westfield State University did not always perform or document a verification of vendor/customer information.

For 10 of the 13 vendor/customer creations or changes during our audit period, there was no documentation to substantiate that Westfield State University (WSU) personnel verified the accuracy of information on an Internal Revenue Service W-9 form or electronic fund transfer (EFT) form obtained from the vendor/customer before making or changing entries in the Massachusetts Management Accounting and Reporting System (MMARS). These changes were based on requests to create vendor/customer files or to change vendors' legal names, legal addresses, and/or EFT information.

Additionally, in February 2020, a WSU employee made a change to the banking information in a vendor/customer file without verifying the information in the change request, resulting in WSU transferring $1.75M to an unauthorized account. Upon discovering the transfer, WSU immediately reported it to the Office of the State Auditor in accordance with Chapter 647 of the Acts of 1989, as well as to other proper authorities. WSU recovered all the funds, so there was no loss. WSU officials told us it was their understanding that the event was still under investigation by state and federal authorities.

A lack of documented verification causes a higher-than-acceptable risk of improper payments such as the one discussed above.

Authoritative Guidance

WSU's internal control plan states,

> *Each Commonwealth Department Head (the University President) has the responsibility to ensure that the department conducts all fiscal business in accordance with state finance law, including but not limited to . . . policies and procedures of the Office of the Comptroller (CTR).*

Section 4c of the Office of the Comptroller of the Commonwealth's (CTR's) "Vendor/Customer File and W-9s" policy describes the process that state agency personnel must follow when changing information in vendor/customer files:

> *Verification of [created or modified vendor/customer] information should not be done solely through email, but should be followed up with a phone call and verified with an authorized signatory, or whatever other actions are necessary to document that the Department has*

> *investigated that the . . . change or additional remittance address is appropriate and properly authorized.*

CTR's "Vendor/Customer File and W-9s" policy states,

> *Departments must ensure the legal and remittance address, classification and [Social Security number or employer identification number] are recorded correctly . . . in MMARS.*

Additionally, WSU's "Bank Wire Procedures" require verification, with an authorized signatory of the vendor, of the validity of requested changes to banking information in vendor/customer files:

> *If [banking] information has changed since the last time a [payment] was initiated to the [vendor], Financial Accounting verifies this information with the vendor through means other than email (i.e. a telephone call using publicly published information) not just from the information provided by the requestor.*

Reasons for Issues

WSU officials told us that although there is no documentation, university personnel did verify the accuracy of the 10 vendor-requested creations or changes in question before making the changes in MMARS. However, without documentation, there is nothing to substantiate to what extent, if any, the required verification process was conducted. WSU officials told us they were not aware that the verification needed to be documented. The university's procedures for changes to, or creation of, vendor/customer files do not require personnel to document the measures they take to verify the information a vendor provides in its creation or change request.

WSU also does not have any monitoring controls (e.g., a supervisory review process) to ensure that the verification is performed.

Regarding the instance of an employee not following WSU verification procedures, WSU officials stated that the employee attempted to call the vendor to verify the information, but could not reach anyone, and the employee decided to process the requested change anyway.

Recommendations

1. WSU should amend its procedures to ensure that verification is properly performed before creations or changes are processed and require all personnel to document the measures they take to verify the information vendors provide in requests to create or change information in their files.
2. WSU should implement effective monitoring controls (e.g., a supervisory review process) to ensure that its staff complies with this requirement.

Auditee's Response

The Vendor Review Procedure in Banner [WSU's accounting system] and MMARS has been updated and implemented. This procedure complies with the Commonwealth of Massachusetts, Office of the Comptroller, ***Vendor/Customer File and W-9's Policy****. This procedure also includes steps that document this process coupled with supervisory review.*

The University's procedures have been updated to require actions to be documented on a newly created form entitled ***Vendor Electronic Payment Instructions—Addition/Change Documentation Form****, which requires a review and approval process when updating or adding vendor banking information.*

Auditor's Reply

Based on the reply above, WSU is responding to our concerns.

2. WSU did not ensure that information system security awareness training was completed as required by the Executive Office of Technology Services and Security.

WSU did not ensure that employees who had access to its systems received information system security awareness training as required by the Executive Office of Technology Services and Security (EOTSS). Specifically, WSU did not provide initial information system security awareness training to new employees when they were hired or require employees to receive training each year. WSU officials conducted periodic training using a PowerPoint presentation, but attendance was not required. Without this training, WSU is exposed to a higher risk of cybersecurity attacks, such as the one discussed in the previous finding, and financial and/or reputation losses.

Authoritative Guidance

EOTSS's "Information Security Risk Management Standard" states,

Commonwealth Offices and Agencies must ensure that all personnel are trained on all relevant rules and regulations for cybersecurity. . . .

All new personnel must complete an Initial Security Awareness Training course. . . . All personnel will be required to complete Annual Security Awareness Training.

Reasons for Issues

WSU did not have a formal program requiring new and existing users to take information system security awareness training. Initially, WSU officials told us that training was not required upon hire for

new employees or annually for all employees because they believed they could not require the training in WSU's collective bargaining agreements or policies, since the agreements did not include compensation for the extra time needed for such training. They stated that for this reason, they could not mandate information system security awareness training or implement a formal policy requiring it. However, during the audit, WSU researched this issue and determined that it could require the training of all employees, including those under collective bargaining agreements.

Recommendations

1. WSU should implement a formal information system security awareness training program requiring new users to receive training and existing users to be retrained annually.
2. WSU should establish monitoring controls to ensure that all of its employees with access to its systems comply with these requirements.

Auditee's Response

WSU currently conducts security awareness training with all constituents who are required to attend training for [Payment Card Industry—Data Security Standard] compliance. Knowing more is needed in this area, at onboarding and for periodic review, WSU has purchased and begun the implementation process of a security awareness education program software that will allow for ad-hoc, scheduled, refresher training and compliance monitoring to meet the needs for good security practice, compliance, and the ever-changing security landscape.

Auditor's Reply

Based on the response above, WSU is responding to our concerns.