STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2019-083
December 2018

FLORIDA STATE UNIVERSITY

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period January 2017 through December 2017, Mr. John Thrasher served as President of Florida State University and the following individuals served as Members of the Board of Trustees:

Edward E. Burr, Chair	Dr. Susan S. Fiorito through 4-25-17 [a]
Leslie Pantin, Vice Chair	Mark Hillis
Dr. Todd Adams from 4-26-17 [a]	Kyle Hill from 3-8-17 [b]
Maximo Alvarez	Craig Mateer
Kathryn Ballard	Nathan Molina through 3-7-17 [b]
William A. Buzzett	Bob Sasser
Emily Fleming Duda	Brent W. Sembler

[a] Faculty Senate President (equivalent to Faculty Senate Chair referred to in Section 1001.71(1), Florida Statutes).
[b] Student Body President.
Note: One Trustee position was vacant during the period.

The team leader was Craig J. Pohlmann, CPA, and the audit was supervised by Edward A. Waller, CPA.

Please address inquiries regarding this report to Jaime N. Hoelscher, CPA, Audit Manager, by e-mail at jaimehoelscher@aud.state.fl.us or by telephone at (850) 412-2868.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

FLORIDA STATE UNIVERSITY

SUMMARY

This operational audit of Florida State University (University) focused on selected University processes and administrative activities and included a follow-up on findings noted in our report No. 2017-086. Our operational audit disclosed the following:

Finding 1: Controls over cash collections need improvement.

Finding 2: Some unnecessary information technology (IT) user access privileges existed that increased the risk that unauthorized disclosure of sensitive student information may occur.

Finding 3: University IT access controls need improvement so that any unnecessary access privileges are detected and timely removed.

Finding 4: The University needs to ensure an IT risk assessment is performed for all University units.

Finding 5: Records documenting the University's direct-support organizations' use of University property, facilities, and personal services could be improved.

BACKGROUND

Florida State University (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate President and Student Body President are also members.

The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the Executive Officer and the Corporate Secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

FINDINGS AND RECOMMENDATIONS

Finding 1: Cash Collections

Effective controls over collections ensure that moneys received are appropriately safeguarded during receipt through deposit at the bank. University personnel have developed policies[1] over collections and collect moneys at various decentralized locations, referred to as cash collections points, located throughout the University. A cash collection point is defined by the University as a department, event,

[1] Policy No. 4-OP-D-2-B, *Cash Management*.

club, or other entity that collects more than $5,000 annually, except for those entities whose collections occur infrequently and are for the recovery of expenditures for telephone, copy, and similar charges.

The University Treasury Management Unit within the Controller Office oversees the 84 cash collection points for student tuition and fees and auxiliary fund revenues. For the 2017-18 fiscal year, the University reported total auxiliary fund revenue of $179 million. University policies require the Controller Office to authorize these collection points before collections begin and to provide guidance to help ensure the accountability and safeguarding of collections. University policies also require that standard control procedures be established at each cash collection point to provide that collections be promptly receipted with a prenumbered receipt, deposits be made daily,[2] and cash collection points be reauthorized[3] every 3 years.

Our discussions with University personnel and review of University records supporting cash collections disclosed that, while 27 cash collection points had been reauthorized within the past 3 years, 57 other collection points operated without reauthorization in the past 3 years. Absent timely reauthorization, the collection points operated without specific authority, increasing the risk for collections to be diverted without timely detection and resolution.

As part of our audit, we also examined University records supporting 30 selected deposits totaling $2.7 million from auxiliary fund collections at the International Programs Department, Leach Center, and Dick Howser Stadium. We found that Leach Center personnel untimely deposited 4 checks, ranging from $780 to $3,301, 3 to18 business days after receipt. Additionally, Leach Center personnel did not prepare a prenumbered receipt for a $906 check that was deposited and, although we requested, University records were not provided to disclose how many days elapsed from receipt of the check until its deposit.

In response to our inquiries, University personnel indicated the Treasury Management Unit was restructured in the 2017-18 fiscal year to allow time to review and reauthorize the cash collection points every 3 years and, because of oversight, collections were not always receipted and timely deposited as required.

Absent timely collection point reauthorizations and promptly recorded receipts and deposits, there is an increased risk that theft could occur without timely detection and resolution.

Recommendation: The University should continue efforts to timely reauthorize cash collection points and ensure all collections are promptly receipted and deposited.

Finding 2: Information Technology User Access Privileges – Student Information

The Legislature has recognized in State law[4] that social security numbers (SSNs) can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining the confidential status of such information. Effective controls restrict individuals from

[2] Policy No. 4-OP-D-2-B states that deposits should generally be made daily and that no collections be held more than 5 business days before being deposited.

[3] According to FSU Policy No. 4-OP-D-2-B, to be reauthorized, a cash collection point must be able to demonstrate a continued ability to follow appropriate control procedures and comply with prescribed cash handling guidelines.

[4] Section 119.071(5)(a), Florida Statutes.

accessing information unnecessary for their assigned job responsibilities and provide for documented, periodic evaluations of employee access privileges to help prevent personnel from accessing sensitive personal information inconsistent with their responsibilities.

According to University personnel and records, the University established a unique identifier, other than the SSN, to identify each student and maintained student information, including SSNs, in the University information technology (IT) system. The University collects and uses student SSNs pursuant to State law for various purposes, such as to register newly enrolled students and to comply with Federal and State requirements related to financial and academic assistance. Student SSNs are also maintained so the University can provide student transcripts to other universities, colleges, and potential employers based on student-authorized requests. For former students who transferred, graduated, or withdrew and prospective students who apply for entrance into the University but do not enroll, the University indefinitely maintains records such as the SSNs of these former and prospective students. Access to student SSNs should only be granted for the performance of administrative, supervisory, or instructional responsibilities that serve a legitimate educational purpose in accordance with applicable Florida Statutes and Federal laws.

To help protect student information from unauthorized disclosure, modification, or destruction, all employees with IT system access are required to sign a protection of information and access agreement form and receive training on records confidentiality. The University established IT procedures to require applicable supervisors and security administrators to document approval of employee access to sensitive data. However, University procedures had not been established to perform periodic evaluations of access to the sensitive personal information of students to ensure that the access was based on a demonstrated need.

As of December 29, 2017, the University IT system contained sensitive personal information for 1 million students, including current, former, and prospective students, and a total of 211 individuals had IT user access privileges to the information, which included student SSNs. University personnel indicated that neither the IT system nor University procedures differentiated current, former, and prospective students. University records also did not demonstrate the public purpose served for maintaining SSNs indefinitely for individuals who had not enrolled in the University.

As part of our audit, we examined University records supporting the access privileges to sensitive personal information of students for 26 selected individuals. We found that 10 of the individuals including an associate vice president, an assistant director, a professor, and a volunteer had unnecessary access to the information. Additionally, we found that while the other 16 selected individuals (programmers, technological specialists, and academic advisors) needed access to current student information, University records did not evidence that these individuals needed continuous access to former or prospective student information.

In response to our inquiry, University personnel indicated that they removed the unnecessary access for the 10 individuals who had the ability to view sensitive personal information of students. Additionally, University personnel indicated that they maintain prospective student information because they have been asked to provide reports to the State on student admission and enrollment patterns in which data for non-enrollees would be requested. Notwithstanding these responses, the existence of unnecessary

access privileges increases the risk of unauthorized disclosure of sensitive personal information and the possibility that such information may be used to commit a fraud against University students or others.

Recommendation: To ensure access to sensitive student information is properly safeguarded, the University should:

- **Document the public purpose served for maintaining that information for individuals who do not enroll in the University. Absent such, the University should discontinue the practice of indefinitely maintaining such information.**
- **Establish procedures that require and ensure documented periodic evaluations of assigned IT user access privileges to determine whether such privileges are necessary and timely remove any inappropriate or unnecessary access privileges detected. Such removal may be achieved by masking the information from individuals who do not need it to perform their assigned duties.**
- **Document the necessity for University personnel who have continuous access privileges to continue these privileges. If an individual only requires occasional access to sensitive personal information, the privileges should be granted only for the time needed.**
- **Upgrade the University IT system to include a mechanism to differentiate current, former, and prospective student information.**

Finding 3: Information Technology User Access Privileges – Enterprise Resource Planning System

Access controls are intended to protect University data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls provide employees access to IT resources based on a demonstrated need to view, change, or delete data and restrict employees from performing incompatible functions or functions inconsistent with their assigned responsibilities.

Our discussions with University personnel and examination of University records disclosed that University personnel documented periodic evaluations of IT access privileges assigned to the University Enterprise Resource Planning (ERP) system finance and human resources (HR) applications based on a demonstrated need. University personnel indicated that, to further reduce the risk of unnecessary or inappropriate access privileges, the Controller Office reviewed all vendor file updates, including specific data elements changed by users, and that independent reconciliations of general ledger detailed transactions to supporting documentation were performed by each department. In addition, the Associate Controller of Disbursement Services evaluated changes to the vendor file to ensure the propriety of the changes.

As part of our audit, from the population of 231 (154 finance and 77 HR) employees with update access to critical roles within the finance and HR applications as of December 2017, we analyzed the IT user access privileges for 26 selected University employees with access privileges to 17 critical finance roles and 14 critical HR roles. We found that 4 employees had finance application access privileges that were unnecessary to perform their assigned functions and allowed them to add or update vendor records and addresses, add and change purchase orders, and approve vouchers for payment. The 4 employees included an IT Director, an Accounts Payable Manager, a Budgeting Director, and a Procurement Support Specialist.

In response to our inquiries, University personnel indicated that the 4 employees had the unnecessary access because the University cross-trained personnel to perform backup services in case of an emergency or personnel turnover. Subsequent to our inquiries, University personnel indicated that the unnecessary access for all 4 employees had been removed.

While our examination of University records supporting selected vendor transactions did not disclose any fraud or errors as a result of the unnecessary access privileges, our procedures do not substitute for management's responsibility to implement adequate controls. Unnecessary or inappropriate access privileges assigned to the ERP system applications increase the risk that unauthorized disclosure, modification, or destruction of University data or IT resources may occur.

Recommendation: The University should continue efforts to appropriately separate incompatible duties associated with the finance application and remove any unnecessary access privileges detected.

Finding 4: Information Technology Risk Assessment

Management of information technology (IT) related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps entity personnel understand the entity's greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction.

IT risk assessments at the unit level, including the identification of risks and the evaluation of the likelihood of threats and the severity of threat impact, help support management's decisions in establishing cost effective measures to mitigate risk and where appropriate, formally accept residual risk. In lieu of IT risk assessments at the unit level, an entitywide comprehensive, written IT risk assessment would evaluate network vulnerability assessments and threats and vulnerabilities at the entity, system, and application levels, and document the range of risks that the entity systems and data may be subject to, including those posed by internal and external users.

University policies[5] require that each University unit[6] conduct an annual risk assessment to evaluate the security and privacy of the unit and provide the results to the Director of the Information Security and Privacy (ISP) Office. The risk assessment information assists the University in managing IT risks facing the University.

For the 2017 calendar year, we requested for examination University records supporting each University unit annual risk assessment and found that, contrary to University policies, 239 (88 percent) of the 273 units did not conduct the assessments. In response to our inquiry, University ISP Office personnel indicated that they contacted all University units to conduct the risk assessments but did not follow-up to ensure the risk assessments were conducted and provided to the ISP Office. Additionally, University

[5] Policy 4-OP-H-5, *Information Security Policy*.

[6] Policy 4-OP-H-5 defines a University unit as a "school or college and any departments or divisions which are a subdivision of a college or school; centers, facilities, labs, libraries, or program within a college or school, or as an independent entity; offices; associations; and administrative units."

personnel indicated that a Universitywide comprehensive, written IT risk assessment had not been performed because each University unit was required to conduct an annual risk assessment.

Absent compliance with University annual risk assessment policies or the conduct of a Universitywide comprehensive, written IT risk assessment, there is an increased risk that all likely threats and vulnerabilities have not been identified, the most significant risks have not been addressed, and appropriate decisions have not been made regarding which risks to accept and which risks to mitigate through appropriate controls.

Recommendation: The University should ensure that an IT risk assessment is conducted for each University unit or revise University policies to require and ensure a Universitywide comprehensive, written IT risk assessment is conducted to provide a documented basis for managing IT-related risks.

Finding 5: Direct–Support Organizations

To promote accountability over University property, facility, and personal service use, it is important that public records prescribe the conditions for such use, document appropriate approval before the use occurs, and demonstrate appropriate use. Such records help document authorization for the use, demonstrate the reasonableness of the value associated with that use, and enhance government transparency.

State law[7] provides that a direct-support organization (DSO) is organized and operated exclusively to receive, hold, invest, and administer property and to make expenditures to, or for the benefit of the University. Additionally, State law[8] authorizes the Board of Trustees (Trustees) to permit the use of University property, facilities, and personal services by a DSO, and requires the Trustees to prescribe by regulation any condition with which a DSO must comply for such use. University regulations[9] establish procedures for the creation, certification, operation, and decertification of University DSOs and the Trustees approved 10 organizations as DSOs. These DSOs routinely provide supplemental resources and education support services to the University.

As part of our audit, we examined University records supporting DSO use of University property, facilities, and personal services. In response to our request, University personnel provided a list of the University facilities used by the DSOs with an annual rent value totaling $525,459 during the 2017 calendar year. Also, according to University personnel, during the 2017 calendar year, the University provided personal services with related costs totaling $5.1 million to the 10 DSOs and the respective DSOs reimbursed the University for $2.4 million of these costs. University personnel indicated that these costs were based on the services of 134 University employees who provided up to 100 percent of their work effort for the DSOs. However, although we requested, University records were not provided to document the actual time and effort of those employees who provided less than 100 percent of their work effort for the DSOs. In addition, we requested Trustees-approved agreements to evidence the basis for reimbursements totaling $557,245 from one of the University's DSOs, the Florida State University Foundation; however,

[7] Section 1004.28(1)(a)2., Florida Statutes.

[8] Section 1004.28(2)(b), Florida Statutes.

[9] University Regulation FSU-2.025, *Direct Support Organizations*, Revised June 10, 2016.

no such agreements were provided. Without such agreements, there is an increased risk of misunderstanding between the University Trustees and a DSO and for over or under reimbursements to occur.

We also noted that, although University regulations establish procedures with conditions for DSO use of University property, facilities, and personal services, University records associated with such use could be improved by obtaining:

- The Trustees' approval of the anticipated DSO use and the estimated value of the associated University resources before the use occurs.
- Confirmations and other documentation from DSO management affirming that University resources were used only for purposes approved by the Trustees.

According to University personnel, the University was unaware of any requirement for the Trustees to document consideration and approval of DSO use of University resources, given that at least one Trustee serves, or appoints a designee to serve, on the executive board of each DSO. Notwithstanding the veracity of this response, approvals by the Board of Trustees and documentation affirming the actual use of University resources would provide additional assurance that DSO use of University resources is consistent with the Trustees' intent and enhance transparency for such use.

Recommendation: We recommend that:

- **The University document University employee actual time and effort provided to the DSOs to support the purpose for and value of such services and the distribution of applicable personal services costs among specific University and DSO activities for employees who work on more than one activity.**
- **The Trustees enter into agreements with DSOs to establish the basis for DSO reimbursements.**
- **The University document the Trustees' consideration and approval of DSO anticipated use of University resources, at least on an annual basis, before the use occurs. To enhance government transparency, Trustees approval documentation should identify the positions of the employees who will provide the personal services, the square footage of the office space and related buildings that will be used by the DSO, and the value of such use.**
- **The University obtain confirmations and other documentation from DSO management affirming that University resources were used only for purposes approved by the Trustees.**

PRIOR AUDIT FOLLOW-UP

The University had taken corrective actions for findings included in our report No. 2017-086.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from February 2018 through August 2018 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.

The objectives of this operational audit were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2017-086.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, weaknesses in management's internal controls; instances of noncompliance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included transactions, as well as events and conditions, occurring during the audit period of January 2017 through December 2017 and selected University actions taken prior and subsequent thereto. Unless otherwise indicated in this report, these records and transactions were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of management, staff, and vendors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed University information technology (IT) policies and procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security, systems development and maintenance, and disaster recovery.
- Evaluated University procedures for maintaining and reviewing employee access to IT data and resources. We examined access privileges to the database and finance and human resources applications during the audit period for 26 of the 231 total employees with such access privileges to determine the access appropriateness and necessity based on the employees' job duties and user account functions and adequacy with regard to preventing the performance of incompatible duties.
- Evaluated University procedures for protecting the sensitive personal information of students, including social security numbers (SSNs). From the population of 211 individuals who had access to student SSNs during the audit period, we examined University records supporting the access privileges granted to 26 employees to determine the appropriateness and necessity of the access privileges based on the employee's assigned job responsibilities.
- Evaluated University security policies and procedures effective during the audit period governing the classification, management, and protection of sensitive and confidential information.
- Evaluated the appropriateness of the University comprehensive IT disaster recovery plan effective during the audit period and determined whether it had been recently tested.
- Reviewed operating system, database, network, and application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Determined whether a written, comprehensive IT risk assessment had been developed for the audit period to document the University risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Examined Board of Trustees (Trustees) board meeting minutes to determine whether Trustees approval was obtained for the University policies and procedures in effect during the audit period and for evidence of compliance with Sunshine Law requirements (i.e., proper notice of meetings, meetings readily accessible to the public, and properly maintained meeting minutes).
- Examined University records for the audit period to determine whether the University informed students and employees at orientation and on its Web site of the existence of the Florida Department of Law Enforcement sexual predator and sexual offender registry Web site and the toll-free telephone number that gives access to sexual predator and sexual offender public information as required by Section 1006.695, Florida Statutes.
- Reviewed the internal audit function to determine whether the University followed professional requirements and provided for peer review of reports issued.
- Examined University records to determine whether the University had developed an anti-fraud policy for the audit period to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we examined University records to determine whether the University had implemented appropriate and sufficient procedures to comply with its anti-fraud policy.
- From the population of payments totaling $34.9 million made during the audit period from the University to its direct-support organizations (DSOs), selected and examined University records

supporting 17 payments totaling $15.6 million to determine whether the transactions were as described by Section 1004.28(1)(a)2. and (2), Florida Statutes.

- Examined University records to determine whether the Trustees had prescribed by regulation, pursuant to Section 1004.28(2)(b), Florida Statutes, the conditions with which the DSOs must comply in order to use University property, facilities, and personal services and whether the Trustees documented consideration and approval of anticipated property, facilities, and personal services provided to the DSOs and the related costs.
- From the population of 7,840 student receivables totaling $3.7 million and recorded as of December 31, 2017, examined documentation related to 33 selected student receivables totaling $14,897 and evaluated the adequacy of the University collection efforts and whether restrictions on student records and holds on transcripts and diplomas were appropriate and enforced for students with delinquent accounts in accordance with Trustees' regulations established pursuant to Section 1010.03(4), Florida Statutes.
- Examined University records to determine whether uncollectible accounts totaling $1.7 million written off during the audit period were properly approved.
- Analyzed payments from tuition differential fees collected during the Spring 2017 and Fall 2017 Semesters to determine whether the University assessed and used tuition differential fees in compliance with Section 1009.24(16)(a), Florida Statutes.
- To determine whether student fees totaling $384 million during the audit period were properly assessed, properly authorized, and correctly recorded in accordance with Trustees' policies and Board of Governors regulations, examined University records for 33 selected students with related fees totaling $223,519. We also determined whether the student status and residency determinations for the selected students complied with Section 1009.21, Florida Statutes.
- From the population of 594 distance learning courses with fee revenue totaling $20.1 million during the audit period, examined University records supporting 30 selected distance learning courses with fee revenue totaling $1.9 million to determine whether distance learning fees were assessed, collected, and separately accounted for in accordance with Section 1009.24(17), Florida Statutes.
- From the population of 84 decentralized cash collection locations, selected 3 locations with collections during the audit period and examined University records supporting collections totaling $2.7 million to determine the effectiveness of University collection procedures and whether the locations were timely reauthorized as cash collection points.
- From the population of 12 contracts for auxiliary operations, which generated revenue totaling $27.1 million for the audit period, examined University records supporting 7 selected contracts, which generated revenue totaling $11.7 million, to determine whether the University properly monitored compliance with the contract terms for fees, insurance, and other provisions. Also, we performed analytical procedures to determine whether University auxiliary services were self-supporting.
- Examined University records for the 19,243 course sections offered during the audit period to determine whether University textbook affordability procedures complied with Section 1004.085, Florida Statutes.
- Examined Board policies, University procedures, and related records for supervisory review and approval of time worked and leave used by exempt employees (i.e., full-time faculty and administrative and professional employees) during the audit period to determine whether supervisory personnel reviewed, and approved employee reports of time worked.
- Reviewed Board policies and University procedures for payments of accumulated annual and sick leave (terminal leave pay) to determine whether the policies and procedures promoted compliance with State law. Specifically, from the population of 531 employees who separated

from University employment during the audit period and were paid $3.5 million for terminal leave, we selected 30 employees with terminal payments totaling $448,636 and examined the supporting records to determine compliance with Section 110.122, Florida Statutes, and Trustees' Policy 4-OP-C-7-E.

- Examined severance pay provisions in 13 employee contracts to determine whether the provisions complied with Section 215.425(4)(a), Florida Statutes, and whether the severance payments totaling $206,322 complied with State laws and Trustees policies.
- Examined University records for 35 administrative employees (including the President) who received compensation totaling $22.5 million during the 2016-17 fiscal year, to determine whether the amounts paid did not exceed the limits established in Sections 1012.975(3) and 1012.976(2), Florida Statutes.
- Evaluated University policies and procedures to ensure health and life insurance was provided only to eligible employees and dependents and that such insurance was timely canceled upon employee termination. Also, we determined whether the University has procedures for reconciling health insurance costs to employee and Trustee-approved contributions.
- Examined University records to determine whether selected expenses were reasonable, correctly recorded, adequately documented, for a valid University purpose, properly authorized and approved, and in compliance with applicable laws, rules, contract terms, and Trustees policies; and applicable vendors were properly selected and carried adequate insurance. Specifically, from the population of expenses totaling $219.3 million for the audit period, we examined University records supporting:
  - 30 selected payments for general expenses totaling $6,664.
  - 31 selected payments for contractual services totaling $7.4 million.
- From the population of 60,766 purchasing card (P-card) transactions totaling $15.1 million during the audit period, examined University records supporting 30 selected P-card transactions totaling $101,761 to determine whether the P-card program was administered in accordance with Trustees policies and University procedures and transactions were not of a personal nature.
- Examined P-card records for the 61 cardholders who separated from University employment during the audit period to determine whether the University timely canceled the cardholders' P-cards.
- From the population of 575 payments totaling $111,847 during the audit period to employees for other than travel and compensation, examined 19 selected payments totaling $22,485 to determine whether such payments were reasonable, adequately supported, for valid University purposes, and whether such payments were related to employees doing business with the University, contrary to Section 112.313(3), Florida Statutes.
- From the population of 244 construction projects with contracts totaling $275.7 million and in progress during the audit period, selected 6 payments totaling $5.6 million related to three construction projects with contract amounts totaling $61.9 million and examined University records to determine whether the payments were made in accordance with contract terms and conditions, University policies and procedures, and provisions of applicable State laws and rules.
- Examined University records to evaluate the propriety of the funding source for the Student Union Expansion Construction Project totaling $127.5 million and whether the contractors for the Project were competitively selected as required.
- Reviewed documentation related to three selected construction projects with construction costs totaling $61.9 million to determine whether the University selected design professionals and construction managers in compliance with State law and adequately monitored the selection of subcontractors and whether design professionals provided evidence of required insurance in

accordance with a Trustees-adopted policy establishing minimum insurance coverage requirements for design professionals.

- Examined a royalty fee contract to determine whether the contract provided for the transfer of royalty fee revenue to a University DSO.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each University on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

FLORIDA STATE UNIVERSITY
OFFICE OF THE PRESIDENT

December 12, 2018

Ms. Sherrill F. Norman, CPA
Auditor General
Claude Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Florida State University's response to your findings and recommendations, for the Operational Audit of Florida State University for the fiscal year ended June 30, 2018, is attached.

We continue to appreciate the work of your staff and your audits, as they assist us in our ongoing efforts to improve our operations. If you have any questions about the responses, please contact Dr. Sam McCall, Chief Audit Officer, at 644-6031 or smmccall@fsu.edu.

Sincerely,

John E. Thrasher
President

Attachment

CC: Sally McRorie
Kyle Clark
Carolyn Egan
Sam McCall
Michael Barrett
Michael Williams

211 Westcott Building, P.O. Box 3061470, Tallahassee, FL 32306-1470
850.644.1085 • Fax 850.644.9936 • www.president.fsu.edu

FLORIDA STATE UNIVERSITY 2018 OPERATIONAL AUDIT
RESPONSES TO AUDITOR GENERAL'S PRELIMINARY AND TENTATIVE FINDINGS

Finding 1: Cash Collections

Auditor's Recommendation:
The University should continue efforts to timely reauthorize cash collection points and ensure all collections are promptly receipted and deposited.

University's Response:
The University will continue to review the established control environment for authorized sites and reauthorize as required by the Cash Management Policy. As of 11/30/2018, 60 of the 67 sites have been certified. The remaining 7 sites are currently under review, which we expect to have completed by 12/31/2018.

Responsible Auditee: Michael Williams, Associate VP for Finance & Administration

Finding 2: Information Technology User Access Privileges – Student Information

Auditor's Recommendation:
To ensure access to sensitive student information is properly safeguarded, the University should:

1. Document the public purpose served for maintaining that information for individuals who do not enroll in the University. Absent such, the University should discontinue the practice of indefinitely maintaining such information.
2. Establish procedures that require and ensure documented periodic evaluations of assigned IT user access privileges to determine whether such privileges are necessary and timely remove any inappropriate or unnecessary access privileges detected. Such removal may be achieved by masking the information from individuals who do not need it to perform their assigned duties.
3. Document the necessity for University personnel who have continuous access privileges to continue these privileges. If an individual only requires occasional access to sensitive personal information, the privileges should be granted only for the time needed.
4. Upgrade the University IT system to include a mechanism to differentiate current, former, and prospective student information.

University's Response:

1. Although FSU needs to retain certain applicant data indefinitely for all applicants, we will implement a practice of removing the applicant's sensitive information for those who do not enroll or become affiliated with the university within two years from the date of the application. This will be implemented by October 31, 2019.
2. Procedures to review user roles with access to sensitive student information will continue to be developed and implemented by the University.
3. The personnel who have the elevated access to view SSN access this information year-round, not just seasonally, therefore taking the access away and adding it back periodically would greatly hinder their day to day business processes. We will document these requirements based on the job duties of the impacted personnel and revoke access when no longer needed by the process listed in the previous recommendation response.

4. The personnel who have access to view Social Security number in the student system are required to reconcile documents and data coming from external sources with the University's own records. Social Security Number is part of the identifying information required for these tasks. These personnel require access to data on all students. Whether the individual is a prospective, current, or past student is not a designation that would be useful for that purpose.

Responsible Auditee: Angela McCausland, Senior ERP Director

Finding 3: Information Technology User Access Privileges – Enterprise Resource Planning System

Auditor's Recommendation:
The University should continue efforts to appropriately separate incompatible duties associated with the finance application and remove any unnecessary access privileges detected.

University's Response:
The University will continue to perform periodic reviews of employee security roles to help minimize the risk of incompatible duties and restrict access based on a demonstrated business need.

Responsible Auditee: Michael Williams, Associate VP for Finance & Administration

Finding 4: Information Technology Risk Assessment

Auditor's Recommendation:
The University should ensure that an IT risk assessment is conducted for each University unit or revise University policies to require and ensure a University-wide comprehensive, written IT risk assessment is conducted to provide a documented basis for managing IT-related risks.

University's Response:
The University will change the FSU Information Security policy by June, 2019 to require risk assessments be completed every 3 years by each university unit. Units will be prioritized using a risk based approach to complete 1/3 of all units within a given year therefore the entire population of units will be completed within 3 years. Risk assessments for the first 1/3 of units will begin in fall of 2019 with a completion of December, 2019. The remaining university units will complete risk assessments in the 2020 and 2021 calendar years. The program will restart in the 2022 calendar year.

Responsible Auditee: Bill Hunkapiller, Director for Information Security and Privacy

Finding 5: Direct-Support Organizations

Auditor's Recommendation:
We recommend that:

- The University employee actual time and effort provided to the DSOs to support the purpose for and value of such services and the distribution of applicable personal services costs among specific University and DSO activities for employees who work on more than one activity.
- The Trustees enter into agreements with DSOs to establish the basis for DSO reimbursements

- The University document the Trustee's consideration and approval of DSO anticipated use of University resources, at least on an annual basis, before the use occurs. To enhance government transparency, Trustees approval documentation should identify the positions of the employees who will provide the personal services, the square footage of the office space and related buildings that will be used by the DSO, and the value of such use.
- The University obtain confirmations and other documentation from DSO management affirming that University resources were used only for purposes approved by the Trustees.

University's Response:
The University complies with applicable requirements of State law regarding accountability over University property, facility and personal service use by Direct-Support Organizations. The University has an existing and long standing regulation governing such use. Regulation 2.025 Direct-Support Organizations stipulates accountability and transparency measures including the review of the annual budget and recommendation to the Board of Trustees for approval, monitor and control the use of University resources by the organization, review and approve quarterly expenditure plans, and review and approval of the independent audits of the organizations. The Board of Trustees' approval of the annual budget includes approval of the anticipated expenditures of personal services and use of University facilities and property by Direct-Support Organizations. The Board of Trustees Chair or their designee serves on each of the Direct-Support Organization Boards to provide further oversight.

University leadership will work with the Direct-Support Organization leadership to evaluate and review the existing procedures and agreements to ensure transparency and accountability over Direct-Support Organization use of University property, facilities, and personal services. Suggested recommendations by the Auditor General to increase transparency will be reviewed while evaluating the efficient use of University and Direct-Support Organization resources.

Responsible Auditee: Michael Williams, Associate VP for Finance & Administration