



STATE OF ILLINOIS
**OFFICE OF THE
AUDITOR GENERAL**

William G. Holland, Auditor General

SUMMARY REPORT DIGEST

SOUTHERN ILLINOIS UNIVERSITY

**Compliance Examination (In Accordance with the
Single Audit Act and OMB Circular A-133)**

For the Year Ended: June 30, 2013

Release Date: May 22, 2014

Summary of Findings:

• Compliance Examination	18
• Financial Audit (previously reported 1-23-14)	<u>1</u>
Total findings:	19
Total last report:	15
Repeated from last audit:	6

SYNOPSIS

This digest covers our compliance examination and OMB A-133 federal single audit of Southern Illinois University (the "University") for the year ended June 30, 2013. A financial audit covering the year ending June 30, 2013 was previously released on January 23, 2014. In total this report contains nineteen findings, one of which was also reported in the Financial Audit which was released on January 23, 2014.

- The University had inaccurate reporting of volunteer hours used to meet matching requirements for the Head Start program.
- The University lacked security and control of confidential information.
- Computers and related items were not able to be located during the University's annual inventory.
- The University's internal controls failed to timely identify the theft of cash in two instances.

{Financial data and activity measures are summarized on the reverse page.}

SOUTHERN ILLINOIS UNIVERSITY
COMPLIANCE EXAMINATION AND SINGLE AUDIT
For the Year Ended June 30, 2013

COMPARATIVE SCHEDULE OF INCOME FUND REVENUES AND EXPENDITURES (Amounts in Thousands)	FY 2013	FY 2012
INCOME FUND REVENUES		
Student tuition and fees, net.....	\$ 212,423	\$ 211,341
Investment income and other.....	381	1,033
Sales and services.....	58	88
Total Revenues.....	<u>212,862</u>	<u>212,462</u>
INCOME FUND EXPENDITURES		
Personal services.....	110,930	116,300
Contractual services.....	38,052	28,848
Transfers.....	14,881	21,310
Awards and grants.....	13,155	10,774
Equipment.....	8,115	10,717
Scholarships, fellowships and waivers.....	8,050	7,473
Commodities.....	6,711	5,274
Travel.....	2,121	2,062
Social security.....	1,849	2,050
Other.....	3,786	2,773
Total Expenditures.....	<u>207,650</u>	<u>207,581</u>
Excess of Revenues over Expenditures.....	<u>\$ 5,212</u>	<u>\$ 4,881</u>
APPROPRIATIONS & EXPENDITURES		
	FY 2013	FY 2012
Education Assistance Fund-007.....	\$ 204,693,702	\$ 218,231,500
Capital Development Fund-141.....	10,287,866	230,615
General Professions Dedicated Fund-022.....	1,250,000	1,250,000
State College & University Trust Fund-417.....	22,000	20,000
Total Expenditures.....	<u>\$ 216,253,568</u>	<u>\$ 219,732,115</u>
Lapsed/Re-appropriated balances.....	7,146,017	17,433,785
Total Appropriation.....	<u>\$ 223,399,585</u>	<u>\$ 237,165,900</u>
EMPLOYMENT STATISTICS (UNAUDITED)		
	FALL 2012	FALL 2011
Faculty.....	2,123	2,171
Graduate assistants.....	992	1,019
Civil service.....	3,530	3,571
Administrative and Professional staff.....	1,466	1,528
Total Employees.....	<u>8,111</u>	<u>8,289</u>
ENROLLMENT STATISTICS (UNAUDITED)		
	FALL 2012	FALL 2011
Fall term enrollment (full-time equivalents).....	27,151	27,792
COST PER STUDENT (UNAUDITED)		
	FY 2013	FY 2012
Cost per full time equivalent student.....	\$ 40,996	\$ 38,500
PRESIDENT		
During Examination Period: Dr. Glenn Poshard		
Currently: Dr. Randy J. Dunn		

**FINDINGS, CONCLUSIONS, AND
RECOMMENDATIONS**

**ERRORS IN REPORTING VOLUNTEER HOURS TO
MEET HEAD START MATCHING REQUIREMENTS**

**Inaccurate reporting of volunteer
hours**

The University failed to perform internal control procedures over compliance with matching requirements resulting in inaccurate reporting of volunteer hours used to meet matching requirements for the Head Start program.

**Reports lacked evidence of review
and approval**

At both the Carbondale and Edwardsville campuses there were instances in which reports prepared to summarize volunteer timesheets were not mathematically accurate and/or lacked evidence of review and approval.

**Errors noted in reports and time
sheets**

Our tests involved reviewing 40 volunteer time sheets for each Carbondale and Edwardsville campus over 4 different months at various centers served by the Head Start program. We noted errors in the monthly reports and individual volunteer time sheets for Edwardsville and one error in the individual volunteer time sheet for Carbondale. Additionally, these monthly reports were not reviewed in a timely manner.

**Errors due to an oversight and
vacancy in Edwardsville accountant
position**

According to University officials, the individual time sheet errors were not caught due to an oversight. On the Edwardsville campus the accounting position at the Head Start office was vacant and was not filled until October 2012, when a new accountant was hired. The individuals assigned by the East St. Louis Director to carry out those functions at that time did not perform the required reviews. (Finding 3, pages 21-22)

We recommended the University follow the procedures that have been established regarding reviewer monitoring of responsibilities and maintenance of proper documentation.

University agrees with auditors

University officials accepted our recommendation and indicated that at SIUE monitoring and review procedures for the volunteer hours used to meet matching for the Head Start program were implemented in October 2012. At SIUC accounting staff have been directed to ensure that procedures are followed and that all volunteer time sheets are checked for signatures.

**NEED TO IMPROVE CONTROLS OVER ACCESS TO
AND DISPOSAL OF CONFIDENTIAL INFORMATION**

The University has weaknesses regarding the security and control of confidential information.

University-wide procedures lacking

The University lacked University-wide procedures for addressing the security and disposal of confidential

information and had not performed a formal risk assessment for identifying all confidential information and assessing existing security over access to confidential information.

During our review, we noted:

Confidential information not adequately protected

- Confidential information, including protected health information, was found within a waste can at one School of Medicine employee's desk.
- The University had not ensured all confidential information in electronic form was adequately protected (i.e. encrypted or redacted).

Security breaches

- The University had three security incidents that exposed data and three additional security incidents that may have exposed data.

Confidential information exposed

Of the six incidents, the University had determined three of the incidents were compromises and breach notifications were not necessary. Of the three classified as breaches, at the time of our review, required notifications were only sent with regard to the SIUE breach involving student information (names, SSN's and/or grades) on 1,577 students. A faculty member placed his grade-book on the University's website. Upon identification, the file was immediately removed from the website and notification process initiated.

Hard drives infected with Malware

Two other breaches (in August and September 2012) at SIUC involved hard drives infected with malware that contained personal information (names and SSN's) for approximately 107 students. SIUC initially determined these incidents were compromises and notification was not required. However, after management determined the drives were no longer available for full analysis to confirm the lack of a breach, they planned to send notification letters to the affected students.

University officials stated that the University-wide security policies and formal risk assessment will be addressed when the campuses fill their information security positions. Furthermore, the SIUC incidents are partially a result of constrained resources with almost 40 unfilled IT positions and less than half the IT staff as the average of its peers (according to the Educause Core Data Survey). The SIUE incident was the result of a user error and was not malicious in nature. (Finding 12, pages 36-38)

We recommended the University:

- Review existing policies regarding the security and control of confidential information, and assure University-wide procedures exist for ensuring confidential and personal information is adequately

secured in both electronic and hardcopy format.

- Perform a formal risk assessment to evaluate its computer environment and data maintained to assure adequate security controls, including physical and logical access restrictions, have been established to safeguard its computer resources and confidential information.
- Ensure confidential information is adequately secured with methods such as encryption or redaction, including such data maintained on backup media.
- Perform and document reviews of all security incidents and ensure compliance with the notification requirements in the Personal Information Protection Act.

The University agrees with auditors

University officials accepted our recommendation and indicated the campuses have begun to work together to review, document, and create University wide policies on the control of confidential information.

INADEQUATE CONTROLS OVER COMPUTER INVENTORY

357 computers could not be located

Southern Illinois University (University) was unable to locate 357 computers and related items (265 from Carbondale and 92 from Edwardsville) during their annual inventory. These items were deemed by the University to have been lost or stolen during fiscal year 2013, with original acquisition value of \$463,274.

During the current year examination, we noted the University implemented two of the four recommendations from the prior year's audit finding. The University performed an assessment to determine if missing computers contained confidential information, and procedures were established to immediately notify security personnel of any missing or stolen computers. However, the University failed to enhance their practices to prevent the theft or loss of computers.

Computers not protected with encryption software

During testing, the auditors noted the University had not protected its computers with encryption software, thus increasing the risk that confidential information could be exposed. Confidential information routinely collected and maintained by the University includes education records, health records, personal information, and sensitive information.

University officials stated University IT personnel have been actively working on a plan to implement encryption by June

2014 on those computers which continue to have access to confidential information. In addition, University officials stated that they file police reports for computers reported as stolen. (Finding 15, pages 43-44)

We recommended the University:

- review current practices to determine if enhancements can be implemented to prevent the theft or loss of computers;
- ensure confidential information is adequately secured with methods such as encryption or redaction.

University agrees with auditors

University officials accepted our recommendation and indicated it has been actively working to enhance efforts to reduce the number of computers reported as lost or stolen and to protect data on its computers.

NEED TO ENHANCE INTERNAL CONTROLS OVER CASH

Southern Illinois University's (University) internal controls designed to safeguard cash failed to timely identify two instances of theft.

\$33,000 was found missing

The first instance occurred at the Carbondale campus in the Student Health Center. During the year, the department noted a single instance of cash theft, which dated back to at least August 2011 (discovered May 2013). After internal audit review, it was determined that approximately \$33,000 of cash was missing.

At the Edwardsville campus \$7,390 was found missing

The second instance occurred at the Edwardsville campus in the School of Education. During a review of Pcard transactions by Internal Audit, two Pcard transactions (netting to \$440) were flagged. The internal audit department then investigated the matter further and noted an additional \$6,950 of cash missing for a total loss of \$7,390, which dated back to July 2012.

University officials noted controls were not effectively carried out

University officials stated that in both instances, controls had been designed to prevent and detect instances of theft, but the controls were not being effectively carried out within the noted departments. (Finding 17, pages 46-47)

We recommended the University conduct an evaluation of the controls in place over the collection of cash and make the necessary enhancements to ensure their effectiveness.

University agrees with auditors

University officials accepted our recommendation and indicated internal controls have been strengthened within the two departments noted. Additionally, a review of cash

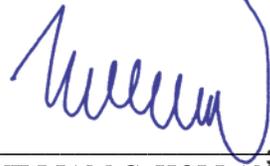
collections across both campuses is planned by Internal Audit later this fiscal year.

OTHER FINDINGS

The remaining findings are reportedly being given attention by the University. We will review the University's progress towards the implementation of our recommendations in our next engagement.

AUDITORS' OPINION

We conducted a compliance examination and OMB A-133 federal single audit of the University for the year ended June 30, 2013 as required by the Illinois State Auditing Act. A financial audit covering the year ending June 30, 2013 was issued separately.



WILLIAM G. HOLLAND
Auditor General

WGH:JAF

SPECIAL ASSISTANT AUDITORS

CliftonLarsonAllen LLP was our special assistant auditors for this engagement.