New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Judiciary
Administrative Office of the Courts
Court Information Technology Funds

July 1, 2012 to August 31, 2015

Stephen M. Eells
State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

PERI A. HOROWITZ
Executive Director
(609) 847-3901

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

GREGORY PICA
Assistant State Auditor

JOHN J. TERMYNA
Assistant State Auditor

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Vincent Prieto
Speaker of the General Assembly

Ms. Peri A. Horowitz
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Judiciary, Administrative Office of the Courts, Court Information Technology Funds for the period of July 1, 2012 to August 31, 2015. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
December 28, 2015

Table of Contents

Scope

We have completed an audit of the Judiciary, Administrative Office of the Courts (AOC), Court Information Technology Funds for the period July 1, 2012 to August 31, 2015. A number of statutes have been enacted which increased various court fees for the general purpose of improving and modernizing the Judiciary's information technology capabilities. Our audit included financial activities from five accounts that were created as a result of these statutes; see Appendix I for a schedule of the various accounts. Total revenue and expenditures included in the audit scope were $126 million and $139 million, respectively.

We also reviewed select general controls, including security management, physical security, contingency planning, change management, and logical access, over the case management systems that capture the dedicated revenue transactions for the five accounts.

Objectives

The objectives of our audit were to determine whether the statutorily-generated revenue was dedicated in accordance with the respective statutes; the expenditures from dedicated accounts were in compliance with the respective statutes, applicable Treasury Circular Letters, and internal policies; and the financial transactions were properly recorded in the state's accounting system. An additional objective was to determine the adequacy of select general controls over several case management systems used to capture the dedicated revenue transactions for the five accounts.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

In preparation for our testing, we studied legislation, circular letters promulgated by the Department of the Treasury, policies of the Judiciary, and the Judiciary's Information Technology Strategic Plans. Provisions we considered significant were documented and compliance with those requirements was verified by interview, observation, and through our testing of financial transactions. We also read the budget messages, reviewed financial trends, and interviewed Judiciary personnel to obtain an understanding of the programs and the internal controls.

A nonstatistical sampling approach was used. Our samples of financial transactions were designed to provide conclusions on our audit objectives, as well as internal controls and compliance. Sample populations were sorted and transactions were judgmentally selected for testing.

Conclusions

We found the statutorily-generated revenue was dedicated in accordance with the respective statutes; the expenditures from dedicated accounts were in compliance with the respective statutes, applicable Treasury Circular Letters, and internal policies; and the financial transactions were properly recorded in the state's accounting system. In making these determinations, we found internal controls over the expenditure process could be improved. We also found select general controls over the case management systems used to capture the dedicated revenue transactions for the five accounts were adequate, but that incompatible levels of user access existed, users' access to systems was not periodically reviewed or removed timely, and there was noncompliance with certain security policies.

Application Systems Monitoring

The AOC should monitor users' access and application systems' activity logs on a routine basis to detect inappropriate or unauthorized activity.

The AOC does not monitor users' access or activity logs of application systems on a routine basis, nor is monitoring required per their policies. The lack of such requirements puts the AOC at greater risk of theft or loss of financial and other data. Periodic review of users' access would assist in identifying users whose access should be removed or who have inappropriate levels of access. Monitoring of application systems activity logs may assist in identifying the frequency and appropriateness of access to financial transactions or data.

User Access

The AOC does not specifically review user access to its Automated Case Management System (ACMS), which is one of the primary systems used to capture case-related financial data. It does, however, review user access of county prosecutor office staff by distributing a questionnaire to the respective offices to confirm if users' system access is still required. We judgmentally sampled four county offices' application access review responses. The responses from the counties included examples of users whose access to ACMS needed to be removed. Additionally, we tested separated employees where access to ACMS should have been removed. These two sources provided us with nine separated users and 12 county users whose ACMS access should have been removed. We found that eight users' access, four from each source, had not been removed. The information that was provided to us for review did not reveal any improprieties.

ACMS users are provided with an access level code or codes for the system that is based on their job requirements. We were provided with a list of 60 ACMS users with sensitive access level codes. We reviewed this information for combined access levels deemed incompatible by AOC that when present may enable a user to create unauthorized transactions. We found two users were assigned incompatible access level codes. Although the incompatible access levels were corrected by the AOC upon our notification, financial data was left vulnerable in the interim. The information that was provided to us for review did not reveal any improprieties.

The AOC contracted with a vendor to conduct a risk assessment which included user access review. Their report was issued in March 2015. Although the report stated there was an absence of regular reviews of user access to certain application systems, the AOC had not followed up, as our review found similar circumstances subsequent to the vendor's report. A routine review of user access may identify incompatible access level codes or access that should be removed.

The AOC stated that they intend to conduct user access reviews of the ACMS, as they do for users of other systems, in the near future.

Application Systems Review

The AOC maintains database activity logs for investigative purposes but does not review these logs for other purposes. The absence of a procedure to review application activity logs creates an increased risk of unauthorized access by users being undetected. Best practice dictates that a procedure of periodic review of user access to applications be conducted to prevent or identify inappropriate access, anomalies, threats, or vulnerabilities.

Recommendation

The AOC should formalize a policy with procedures requiring routine review of application systems users' access to ensure that only authorized access is present. The AOC should also create and implement a policy and procedure to review application systems activity logs to mitigate potential threats.

»»-«

Remote Access

The AOC should enforce its remote user access and password management policies to prevent unauthorized system access.

Remote Access Policy

The AOC does not require or maintain the documentation that authorizes remote access to application systems, leaving systems vulnerable to breach, loss, or theft of data. The AOC permits remote access by employees to its systems under certain circumstances. The Remote Access policy requires that a manager complete and authorize a request form on behalf of an employee needing remote access. The form is subsequently authorized by a Clerk of the Court or Assistant Director and the AOC Information Technology Office. The Information Technology Office then issues the employee a Virtual Private Network (VPN) to access the authorized AOC systems remotely. Access to the systems also requires a token and several layers of passwords.

We judgmentally sampled 25 of the 1506 employees with an active VPN and found the access request form was not available for 21 employees. Of the four forms available for review, two forms did not have the required authorization to obtain remote access.

Password Management Policy

Several AOC mobile devices were accessed without the required password. The AOC Password Management Policy states that in order to obtain access to any Judiciary computer system, application, or infrastructure, an authorized user must create a password and the password must contain a sufficient level of complexity.

Numerous AOC employees are assigned a Judiciary mobile device that, when issued, should only be able to be accessed through an authentication process. The authentication process verifies the user is accessing the device with a unique username and password. The AOC uses a mobile device management solutions company that tracks AOC's mobile devices, logs and tests users' passwords or lack thereof, and provides reports to the AOC. The reports are used for incident or investigative purposes but are not used as a routine monitoring tool, which could detect unwanted access. We reviewed a mobile usage monitoring report that disclosed 37 of 1515 users were able to access their device even though a password or strong password was not present. The absence of a strong password leaves the mobile device and AOC application systems vulnerable to breach.

Recommendation

The AOC should enforce its remote access policy and require that all active VPNs be properly authorized and maintain evidence of authorizations for future reference. The AOC should ensure their mobile devices are not accessed without a password or a strong password. In addition, it should use the reports provided by the mobile device management solutions company as a monitoring tool to detect unwanted access.

»»←«

Internal Controls

Expenditures made from dedicated funding sources should comply with all AOC required procedures to ensure they are proper, accurate, and allowable.

The AOC did not consistently follow its documentation process when expenditures were made from information technology dedicated funds. Implementation of a strong system of internal controls is the responsibility of management and is necessary to decrease the risk that errors will occur and not be detected. The AOC has established adequate internal controls but is not consistently abiding by its own rules. We judgmentally sampled 179 payment voucher-type expenditure transactions from the five dedicated funds in our scope totaling $12.9 million out of a population of $57 million. The following internal control exceptions were found.

- The AOC's procedures require that a justification be provided on the internal requisition form; justification is an essential component in determining whether an expense meets the criteria of a dedicated fund. The form that documents the justification for a purchase was not provided for our review for nine percent of our sampled items. An additional six percent had the form, but the justification portion was blank.

- Payments should not be made until there is evidence that goods or service were received. Although evidence of receipt was lacking in only three percent of the sampled expenditures, these exceptions included the purchase of GoPro cameras, iPad minis, and a Mac minicomputer. We found no evidence that these items had ever been placed in use.

Recommendation

The AOC should comply with its procedures when processing expenditures from dedicated funds to ensure that only justified purchases are made and that documentation is maintained supporting the receipt of goods.

APPENDIX 1

Judiciary – Administrative Office of the Courts
Court Information Technology Funds
Schedule of Revenues and Expenditures
by Fiscal Year

N.J.S.A. Statutes		2013	2014	2015	Total
21st Century Improvement Fund - Digital E-Courts					
2B:1-9 and	Revenue	$ -	$ -	$ 6,175,885	$ 6,175,885
2B:1-10	Expenditures	-	-	2,137,879	2,137,879
Court Technology Improvement Fund					
	Revenue	12,268,076	12,832,704	13,065,630	38,166,410
2B:1-6	Expenditures	21,469,860	11,219,361	5,606,379	38,295,600
Court Computerized Information Systems Fund - Electronic Access to Court Records					
	Revenue	1,843,619	1,251,900	1,222,120	4,317,639
2B:1-4	Expenditures	3,407,557	5,946,414	2,447,055	11,801,026
Comprehensive Enforcement Program Fund - Comprehensive Automated Probation System					
2B:1-9 and	Revenue	509,872	503,579	496,924	1,510,375
2B:19-4	Expenditures	469,108	707,398	201,217	1,377,723
Automated Traffic System Fund					
	Revenue	25,638,241	25,623,994	24,897,398	76,159,633
2B:12-30	Expenditures	24,868,388	31,446,408	28,596,878	84,911,674
Grand Total in Audit Scope					
	Total Revenue	$ 40,259,808	$ 40,212,177	$ 45,857,957	$ 126,329,942
	Total Expenditures	$ 50,214,913	$ 49,319,581	$ 38,989,408	$ 138,523,902

New Jersey Courts
Independence • Integrity • Fairness • Quality Service

Administrative Office of the Courts

GLENN A. GRANT, J.A.D.
Acting Administrative Director of the Courts

www.njcourts.com • Phone: 609-984-0275 • Fax: 609-984-6968

December 21, 2015

Mr. John J. Termyna, Assistant State Auditor
Office of the State Auditor
Office of Legislative Services
125 South Warren Street
P.O. Box 067
Trenton, NJ 08625-0067

Re: Judiciary Response -- Draft OLS audit report on the Judiciary, Administrative Office of the Courts, Court Information Technology Funds for the period July 1, 2012 to August 31, 2015

Dear Mr. Termyna:

I am in receipt of the draft OLS audit report on the Judiciary, Administrative Office of the Courts, Court Information Technology Funds for the period July 1, 2012 to August 31, 2015. Thank you for the work that your team of auditors did in conducting this audit. The following are the Judiciary's responses to the three findings in the draft report.

Finding #1 – Application System Monitoring (page 3) – "The AOC should monitor users' access and application systems' activity logs on a routine basis to detect inappropriate or unauthorized activity."

OLS Recommendation: "The AOC should formalize a policy with procedures requiring routine review of application users' access to ensure that only authorized access is present. The AOC should also create a policy and procedure to review application systems activity logs to mitigate threats."

Judiciary Response:
User Access
The Judiciary's Information Security Unit already conducts access reviews at regular intervals of all external agencies. The Judiciary Information Security Unit is in the process of formalizing an internal access recertification program, which at periodic regular intervals will review and validate user access to all Judiciary applications, including the Automated Case Management System (ACMS). With regard to separated employees, it is Judiciary policy to remove access upon separation.

Applications Systems Review
The Judiciary's Information Security Unit has acquired a Security and Incident Event Manager (SIEM), which stores, analyzes and reports on log data on Judiciary network devices and servers. The Information

Security Unit will expand the log collection to include the application systems activity logs and will research best practices in order to develop and implement policy and procedures for the regular periodic review of the application systems activity logs.

Finding #2 – Remote Access (page 4) – "The AOC should enforce its remote user access and password management policies to prevent unauthorized system access."

OLS Recommendation: "The AOC should enforce its remote [user] access policy and require that all active VPNs be properly authorized and maintain evidence of authorizations for future reference. The AOC should ensure their mobile devices are not accessed without a password or a strong password. In addition, it should use the reports provided by the mobile device management solutions company as a monitoring tool to detect unwanted access."

Judiciary Response:

Remote User Access Policy

The Judiciary's Information Technology Office will enforce the Judiciary's remote user access policy and require that that all VPNs be properly authorized as well as maintain evidence of those authorizations for future reference.

Password Management Policy

With regard to the finding that the Judiciary's Password Management Policy does not prevent unauthorized system access by remote users, the report that was provided to the auditors that served as the basis for that finding was flawed. The Judiciary was able to identify the existence of this flaw and diagnose its cause upon review of the auditor's finding. That diagnosis revealed that the software configuration policy within the Mobile Device Management (MDM) solution used by the Judiciary to manage its mobile devices is in fact set to require that all mobile devices have passcodes compliant with the Judiciary's Password Management Policy. This feature cannot be disabled by the end-users on their Judiciary-owned devices, thus preventing any device from being used without a valid passcode. However, it was found that the reporting function of the MDM solution generates reports that do not correctly or properly reflect the mobile device configurations, inaccurately reporting configurations without the passcodes that are in fact in place. The Judiciary has notified the vendor that provided the MDM solution of this defect in that product's reporting function. The Judiciary will monitor this report going forward to ensure that it properly reflects the mobile device configurations and will seek a remedy if the issue continues.

Finding #3 – Internal Controls (page 5): "Expenditures made from dedicated funding sources should comply with all AOC required procedures to ensure they are proper, accurate, and allowable."

OLS Recommendation: "The AOC should comply with its procedures when processing expenditures from dedicated funds to ensure that only justified purchases are made and that documentation is maintained supporting the receipt of goods."

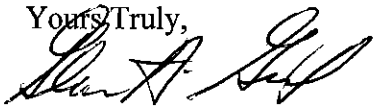
Judiciary Response:

The Judiciary agrees that only justified purchases should be made from dedicated funding sources and that documentation supporting the receipt of goods should be retained. The Judiciary adheres to those principles in its purchases.

Ensure that only justified purchases are made
The AOC Purchasing Unit makes every effort to comply with all procedures when processing expenditures from dedicated funds so as to ensure that only justified purchases are made and will take every action necessary in the future to ensure that all required information is included on purchasing requests.

Maintain documentation supporting the receipt of goods
The internal controls used by the Accounting Unit in the AOC's Financial Services Division include a three-way match when processing payments against purchase orders. The match includes the invoice, the purchase order, and either the packing slip, e-mail confirmation of receipt from the end-user or a signed Request for Recipient Certification form. The Accounting Unit was provided with a list of two payments from the auditors test; PO #'s 7720238 and 7804971. Both payment records included a separate e-mail from ITO confirming receipt. The Judiciary Accounting Unit requires verification of receipt in the absence of a physical packing slip. That was done in both sample instances by retaining an email confirmation of receipt. The Judiciary has given clear evidence that all standard and appropriate business practices are followed when paying for goods and services.

Yours Truly,



Glenn A. Grant, J.A.D.

Cc: Steven D. Bonville, Chief of Staff
Shelley R. Webster, Director, OMAS
Jack McCarthy III, Director, ITO
Robert O'Neill, Assistant Director, Financial Services Division
Francesca Bianco, Chief, Information Security Unit