EXECUTIVE SUMMARY

JUDICIARY
ADMINISTRATIVE OFFICE OF THE COURTS
COURT INFORMATION TECHNOLOGY FUNDS

We found statutorily-generated revenue was dedicated in accordance with 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 dedicated 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.

AUDIT HIGHLIGHTS

- The AOC does not monitor users’ access or activity logs of application systems on a routine basis, and their policies do not require monitoring. 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. Our test of user access to the Automated Case Management System found 8 active users of 21 reviewed that should have been removed.

- 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. However, several AOC mobile devices were accessed without the required password. 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 AOC Remote Access Policy requires that a manager complete and authorize a request form on behalf of an employee needing remote access. Our test of 25 employees disclosed 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.

AUDITEE RESPONSE

The department generally concurs with our findings and recommendations.

For the complete audit report click here.