March 12, 2014 2013-302.1

The Governor of California
President pro Tempore of the Senate
Speaker of the Assembly
State Capitol
Sacramento, California 95814

Dear Governor and Legislative Leaders:

We recently conducted an audit as required by Section 19210 of the California Public Contract Code. Our report, titled *Judicial Branch Procurement: Semiannual Reports to the Legislature Are of Limited Usefulness, Information Systems Have Weak Controls, and Certain Improvements in Procurement Practices Are Needed* (2013-302 & 2013-303), which we issued to the public on December 19, 2013, details our assessment of the Administrative Office of the Courts' (AOC) and eight other judicial entities' implementation of the California Judicial Branch Contract Law (judicial contract law).[1] This law, among other things, requires the Judicial Council of California (Judicial Council)—the policy-making body of the California courts—to provide a report to the Joint Legislative Budget Committee (Budget Committee) and the California State Auditor (state auditor) twice each year detailing information related to the procurement of certain contracts for the judicial branch. The AOC, on behalf of the Judicial Council, uses procurement data from its Oracle Financial System (Oracle) and Phoenix Financial System (Phoenix) to compile the semiannual reports.

Our analysis identified pervasive weaknesses in selected information system controls that affect Oracle and Phoenix.[2] The AOC and the eight other judicial entities we reviewed in our report use Oracle and California's superior courts (superior courts) use Phoenix. In addition to other activities, both systems aid their respective users in issuing purchase orders and recording certain procurement activity.

In accordance with generally accepted government auditing standards, we communicated the detailed results of the weaknesses we identified to the AOC and certain superior courts in separate confidential management letters. Based on our review, we concluded that there is an unacceptably high risk that the data from the applications the AOC and superior courts currently use to perform their day-to-day operations could lead to an incorrect or improper conclusion, regardless of the purpose for which the data are used. This includes, but is not limited to, the AOC's use of the Oracle and Phoenix data in compiling the semiannual reports on behalf of the Judicial Council. Further, the weaknesses we identified could compromise the security and availability of the AOC's and superior courts' information systems, which contain confidential or sensitive information, such as court case management records, human resources data, and financial data.

[1] The judicial contract law is codified in the California Public Contract Code, sections 19201 through 19210.

[2] We determined that the weaknesses were pervasive because many of them affect all or a large part of the AOC's and California's superior courts' information systems.

We are issuing this letter because we believe it is important that the governor and Legislature be made aware of the specific details related to the weaknesses we identified and to provide an update on the progress the AOC has made in implementing our recommendations based on its 60-day response to our December 2013 audit. Although the AOC has agreed to implement some of our recommendations, it has expressed concerns as to whether these recommendations can be fulfilled in the time frame we requested unless additional funding is provided.

Information System Control Weaknesses Affecting the AOC and Superior Courts

In reviewing selected information system controls over the AOC's and the superior courts' information systems, we identified pervasive weaknesses in the general controls—which include the key control categories of security management, access controls, and contingency planning—that affect the AOC's and superior courts' information systems, including Oracle and Phoenix. We also noted deficiencies in the Phoenix application's general controls related to access and business process application controls related to procurement and accounts payable activities.

The results of our review indicate that there is an unacceptably high risk that reliance on data from the applications the AOC and superior courts currently use to perform their day-to-day operations could lead to an incorrect or improper conclusion. This includes, but is not limited to, the AOC's use of the Oracle and Phoenix data in compiling the semiannual reports it submits to the Budget Committee and the state auditor on behalf of the Judicial Council. As computer technology has advanced, government entities have become dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Virtually all state and judicial operations are supported by automated systems and electronic data, and entities would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Consequently, ineffective information system controls can result in significant risk to a broad array of government operations and assets.

Accordingly, we expected that the AOC and superior courts would have well-developed plans, policies, and procedures related to information systems controls. However, we found that some of the AOC's plans were either nonexistent, or in one case, the plan had not been updated since 1997. Further, in its reviews of the superior courts, the AOC repeatedly identified the same concerns, some dating back to 2003, with the superior courts' plans, policies, and procedures relating to their respective systems. In addition, our testing showed weaknesses in the AOC's and superior courts' performance of certain tasks. The weaknesses we identified, including practices we cannot divulge because of their sensitive nature, could compromise the security and availability of these information systems, which contain confidential or sensitive information, such as court case management records, human resources data, and financial data.

Methodology

The U.S. Government Accountability Office (GAO), whose standards we are statutorily required to follow, requires us to assess the sufficiency and appropriateness of computer-processed information that we use to support our findings, conclusions, or recommendations. To accomplish this, we used the industry best practices contained in GAO's *Federal Information System Controls Audit Manual* (FISCAM) as the benchmark against which we evaluated

selected information system controls the AOC and superior courts have implemented. We also relied in part upon a judgmental selection of audit reports the AOC's Internal Audit Services previously published to identify weaknesses related to certain superior courts' general and business process application controls. General controls are the policies and procedures that apply to all or a large segment of the AOC's and the superior courts' information systems and help ensure their proper operation. Business process application controls are directly related to a specific computerized application—Oracle and Phoenix, in this case—and help to ensure that transactions are complete, accurate, secure, and available.

In conducting our review, we identified pervasive weaknesses in the general controls the AOC and superior courts implemented over their information systems—which include Oracle and Phoenix. The strength of general controls is a significant factor in determining the effectiveness of business process application controls. Therefore, because we identified pervasive weaknesses in the AOC's and superior courts' general controls, we did not perform testing of the Oracle and Phoenix business process application controls. Rather, we worked with the AOC and superior courts to follow up on weaknesses the AOC previously identified in Phoenix's business process application controls over procurement and accounts payable activities. Finally, due to the pervasive deficiencies we identified in the key control categories included in our review, we did not proceed with performing exhaustive testing for all control categories. Consequently, there may be additional weaknesses that exist over the Oracle and Phoenix data that we did not identify during our review.

The AOC and Certain Superior Courts Lack Strong General Controls

The primary objectives for general controls are to safeguard data, protect business process applications, and ensure continued computer operations in case of unexpected interruptions. Key general control categories include security management, access controls, configuration management, segregation of duties, and contingency planning. Without effective general controls, business process application controls may be rendered ineffective by circumvention or modification. For example, an effective application control may include an automated edit designed to prevent users from entering unreasonably large dollar amounts into a payment processing system. However, this application control cannot be relied on if weaknesses in general controls permit an individual to make unauthorized program modifications to an application that would allow certain payments to bypass the automated edit.

Security Management Programs Are Weak

The AOC and certain superior courts have weaknesses in their security management programs. Further, the AOC has failed to assess the risks to its information systems, which is the starting point for developing security policies and security plans. An entitywide information security management program—such as for the AOC or each individual superior court—is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

Controls for Monitoring or Restricting Access Are Weak

The AOC's and certain superior courts' general controls for monitoring and restricting access to their information systems are weak. Access controls limit or detect access to computer resources—including data, equipment, and facilities—thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users to authenticate themselves—through the use of secret passwords or other identifiers—and limit the files and other resources that authenticated users can access and the actions that they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment.

However, the AOC's process for removing the network accounts of terminated employees does not provide assurance that staff disables or removes accounts in a timely manner. Further, the AOC was unable to provide audit logs documenting the date and time at which it removed network access for the employees we tested. The AOC is also not adequately prepared to respond to security incidents because it does not have a documented and approved incident management plan.

In addition, certain superior courts had deficiencies in their policies related to deleting or modifying network accounts and failed to identify the appropriate level of network access for their employees. Further, certain superior courts do not have an adequate process for requesting changes to network access, whereas others could not provide sufficient evidence to support the date and time at which they deleted or modified network accounts for the employees included in our review. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, may surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users may intentionally or unintentionally read, add, delete, modify, or extract data or execute changes that are outside their span of authority. Moreover, inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

The AOC and Certain Superior Courts Have Poor Controls Over Contingency Planning

Contingency planning represents a broad scope of activities designed to sustain and recover critical information technology services following an emergency. There are many different types of contingency-related plans, which include, but are not limited to, Business Continuity Plans, Continuity of Operations Plans, and Disaster Recovery Plans. However, the AOC's Disaster Recovery Plan for resuming critical operations is significantly out of date, having been last updated in 1997. Further, the majority of the superior courts included in the AOC's internal audit reports we reviewed had incomplete, insufficient, or untested contingency plans. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. Consequently, if contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Phoenix Application's General and Business Process Application Controls Have Weaknesses

The AOC and superior courts have weaknesses related to the Phoenix application's general controls over logical access. Further, certain superior courts have weaknesses in the business process application controls over procurement and accounts payable activities. For example, we found that the AOC and superior courts do not have an adequate process for changing employees' access to the Phoenix application. In addition, certain superior courts did not have sufficient controls over the data they enter into Phoenix and did not always completely document their procurement transactions. In the absence of strong general and business process application controls, the AOC and certain superior courts cannot ensure that the Phoenix data is complete, accurate, valid, and confidential.

Conclusion

We identified pervasive deficiencies in the general controls the AOC implemented over its information systems, which include Oracle. Likewise, we identified pervasive deficiencies in the general and business process application controls that the AOC and the superior courts implemented over Phoenix. General controls support the functioning of business process application controls, and both are needed to ensure complete and accurate information processing. If the general controls are inadequate, the business process application controls may not function properly and could be overridden. Consequently, until the AOC and the superior courts implement adequate general controls over their information systems, the completeness, accuracy, validity, and confidentiality of their data will continue to be at risk. Therefore, we determined that there is an unacceptably high risk that the data from the applications the AOC and superior courts use in their day-to-day operations could lead to an incorrect or improper conclusion. As a result, the Oracle and Phoenix data are not sufficiently reliable, regardless of the purpose for which the data are used. This includes, but is not limited to, the AOC's use of the Oracle and Phoenix data in compiling the semiannual reports it submits to the Budget Committee and the state auditor on behalf of the Judicial Council. Further, the weaknesses we identified could compromise the security and availability of the AOC's and superior courts' information systems, which contain confidential and sensitive information, such as court case management records, human resources data, and financial data.

Recommendations

The AOC should implement all of the industry best practices related to general and business process application controls as outlined in FISCAM no later than December 31, 2014, thereby strengthening and continuously monitoring the effectiveness of the controls over its information systems. In addition, the AOC should immediately begin implementing improvements to its controls over access to its information systems and place these improvements into effect by February 2014. Finally, the AOC should provide guidance and routinely follow up with the superior courts identified in its internal audits as having control weaknesses—requiring each superior court to provide process updates every six months until their respective audit findings are corrected—to ensure that they make the necessary improvements to their general and business process application controls.

Agency Comments

The AOC expressed concerns in its initial response to our audit report about the conclusions we reached regarding weaknesses in its information systems and its ability to implement our recommendations in the time frame we requested unless additional funding was provided. Nonetheless, the AOC agreed to implement some of the recommendations. In its 60-day response dated February 19, 2014, the AOC discussed the progress it had made implementing our recommendations. Specifically, the AOC asserted that it is developing a Court Information Systems Security Policy Framework, which it intends to present to the Judicial Council for approval at its June 2014 meeting. The AOC also stated that it is reviewing all industry best practices, including those contained in FISCAM, and that implementation will occur in stages by December 2014. Further, in response to our recommendation that it immediately begin implementing improvements to access controls, the AOC asserted that it has developed a new manual process. Although this process may partially address our access control concerns, we believe the AOC will need to take further action to fully address this recommendation. Finally, because our recommendations also affected the superior courts, the AOC stated that it has already begun providing periodic guidance to the superior courts and contacting the superior courts it identified in the internal audit reports it issued during the last two years concerning the status of incomplete items. To gain further assurance regarding the sufficiency of the AOC's corrective actions, the state auditor will continue to monitor the AOC's progress toward implementing our recommendations.

Respectfully submitted,

Elaine M. Howle

ELAINE M. HOWLE, CPA
State Auditor