Department of Legislative Services
Office of Legislative Audits

Department of Information Technology

Combined Presentation on

Fiscal Compliance Audit
Report Dated September 12, 2016

and

Resource Sharing Lease Agreements
Special Review
Report Dated November 18, 2016

Overview

- DoIT is responsible for the State's information technology policies, procedures, and standards, and for overseeing the implementation of major information technology (IT) projects for the State's Executive Branch agencies and commissions.

- DoIT develops the Statewide Information Technology Master Plan; manages the Major Information Technology Development Project (MITDP) Fund; and coordinates, purchases, and manages IT and telecommunications services to State agencies under its authority.

- DoIT is responsible for reviewing, valuating, and approving IT resource sharing agreements entered into by State agencies under its authority.

- DoIT's FY 2015 operating expenditures totaled $99.2 million.

Fiscal Compliance Audit Overview

Our fiscal compliance (FC) report included 7 findings, 2 of which (Findings 1 and 6) were repeated from the prior audit report. Key findings were:

- DoIT lacked documentation that it effectively monitored Major Information Technology Development Projects (MITDPs).
- DoIT had not established a process to independently evaluate the performance of contractual project managers overseeing MITDPs.
- DoIT had not established comprehensive policies for changes to MITDP scope, schedule, or costs (rebaselining) and for the use of independent assessments as a means to assess their health and areas for improvement to help them succeed.
- There were certain security control deficiencies relating to the networks and computer resources under DoIT's responsibility.

Oversight of MITDPs (FC Finding 1)

DoIT lacked sufficient documentation supporting its reviews of annual MITDP status reports and system development documents, and that quarterly portfolio reviews were conducted.

Information Technology Project Requests (ITPRs)
DoIT did not ensure that agencies' annual project status reports, known as ITPRs and required by State law, were current prior to approving them.

ITPRs include a summary of the project scope, the needs addressed, potential risks, possible alternatives, estimated costs, and funding sources. ITPRs also describe how a project meets the goals of the Statewide Information Technology Master Plan.

- Our test of the FY 2015 ITPRs submitted for 5 projects valued at $355.5 million disclosed that DoIT approved the ITPRs even though certain ITPR information for 3 projects valued at $163.6 million had not been updated from the prior year.

Oversight of MITDPs (FC Finding 1 cont.)

System Development Life Cycle (SDLC)

DoIT did not document its approval when agencies completed each SDLC phase of the MITDP, which is intended to reduce project failure risk.

- Although not required by State law, approval of each SDLC phase of the MITDP is critical because these projects are often large and complicated, involve high costs, and support a critical business function for the State.

Quarterly Portfolio Review Meetings

Specific documentation requirements were not established for DoIT's quarterly portfolio review meetings with agencies to discuss MITDP status.

- DoIT frequently did not document significant matters discussed during these meetings, including any required corrective actions.
- DoIT did not document that it verified the agency self-assessment of MITDP status, which were prepared for these meetings.

Oversight of MITDPs (FC Finding 2)

DoIT had not established a process to independently evaluate oversight project managers (OPMs) hired through a vendor to monitor the development and implementation of the 33 MITDPs valued at $850 million as of June 2015.

- DoIT had not established a formal process to independently assess whether OPMs were properly performing their duties and meeting expectations.
- DoIT did not specify the types of documentation that OPMs should gather while overseeing the MITDPs. We found that the OPMs' activity reports varied in content and specificity, thus impeding DoIT's ability to determine the effectiveness of project monitoring.
- DoIT did not measure the workload of each OPM and determine if an appropriate number were assigned to effectively monitor all projects. The vendor contract terms provided for up to 20 OPMs and DoIT could not explain why only 6 were assigned as of June 2015.

Oversight of MITDPs (FC Finding 3)

DoIT had not established comprehensive policies for changes to a project's original (or baseline) scope, schedule, or costs established during the SDLC planning phases and for the use of Independent Verification and Validation (IV&V) assessments.

Rebaselining

- DoIT did not maintain records to readily identify all rebaselining occurrences (such as changes in scope, schedule, and costs) during the life of each project, including the reasons and project impact.
- Rebaselining can occur for valid reasons or can be used to mask cost overruns or schedule delays.
- According to DoIT's records, 12 of the 42 projects it monitored in 2014 (29%) were rebaselined for one or more reasons, such as changes in project scope, schedule, and/or budget.

Oversight of MITDPs (FC Finding 3 cont.)

IV&V Assessments

DoIT lacked a policy defining risk factors and other considerations to trigger an IV&V.

IV&Vs provide an independent means to determine whether a system is being built using practices that lead to a successful implementation (verification), and whether the completed system will provide the needed functionality to satisfy the intended business purpose (validation).

- As of November 2015, DoIT had only initiated one IV&V for one of the 33 MITDPs.
- As of June 30, 2015, DoIT had not documented a determination as to whether to initiate an IV&V for any of the projects being monitored at that time, including 19 projects that were in the more critical implementation/development phases.
- DoIT could not document how IV&V results should be considered during its project oversight.

Other Findings

Findings 4 and 5 – Information Systems

- Critical or sensitive networks (including DoIT's, the Department of Budget and Management's, and the Office of the Governor's) were not properly secured in that certain contractors had been granted unnecessary access and certain security capabilities were not fully used.
- Computers covered by DoIT's managed desktop services were not properly maintained and secured with current malware protection.

Finding 6 – Statewide Contract Procurements

DoIT did not properly instruct State agencies procuring services from DoIT's statewide contract to secure competitive bids received electronically and DoIT did not always properly secure its own bids.

Finding 7 – Universal Service Trust Fund

DoIT did not recommend an appropriate reduction in the Universal Service Fee in recognition of excess funds in the Fund and projected expenditures.

Fiscal Compliance Audit Conclusions

DoIT should

- ensure annual MITDP status reports are current and complete;
- document approvals of project phases and the results of quarterly review meetings;
- evaluate project managers, specify project monitoring documentation and reporting requirements, and ensure adequate resources are devoted to project monitoring efforts;
- establish comprehensive policies for project rebaselining and the use of IV&Vs; and,
- implement recommended actions to provide appropriate network and computer security, secure electronic bid documents, and closely monitor Universal Service Trust Fund activity.

Resource Sharing Special Overview

We conducted a special review of 10 resource sharing lease agreements (RSAs) between 2 telecommunications (telecom) companies and the Department of State Police (DSP), Natural Resources (DNR), or DoIT. Our findings related to DoIT oversight of the RSAs were:

- DoIT did not maintain comprehensive records of the RSAs nor effectively monitor the RSAs executed primarily by DSP and DNR.

- DoIT did not take timely action to address the lease payment arrangements. For about 15 years, RSA payments of $4.4 million were deposited into escrow accounts maintained by a law firm (which were used by DSP and DNR to acquire goods and services). DoIT believes RSA payments should have been deposited into the MITDP Fund.

- DoIT did not ensure that all compensation due from RSAs was received.

Resource Sharing Special (Findings 1 and 2)

Recordkeeping

DoIT did not maintain comprehensive records of all telecommunications resource sharing agreements (RSA) maintained by Executive Branch agencies under its authority, including its own.

- DoIT did not maintain a complete list of existing RSAs, including the value of the agreements and renewal periods.
- At the start of our review, DoIT had a listing of RSAs, but it only included 5 of the 10 RSAs in our review, and no related agreements were on file.
- DoIT also did not have a complete listing of its own RSAs (2 of the 10 RSAs were DoIT's) or a record of equipment attached to its towers.

Consequently, DoIT could not monitor each agreement's terms to ensure that renewal options were properly exercised and that all compensation due was received and accounted for.

Resource Sharing Special (Finding 1)

Lease Payment Arrangements

DoIT did not take timely action when certain RSA payment arrangements were inconsistent with DoIT's understanding of the related requirements of State law.

- Beginning in 2001, lease payments from 2 telecom companies were deposited into interest-bearing escrow accounts maintained by a law firm.
- Based on our review of available records, from 2001 to June 30, 2016, deposits into these escrow accounts totaled $4.4 million.
- Account withdrawals of $3.8 million were used by DNR and DSP to purchase goods and services; controls over this activity were lacking, resulting in certain questionable activity.
- DoIT believed these funds should have been deposited into the MITDP.

Resource Sharing Special (Finding 1)

Lease Payment Arrangements (continued)

- DoIT was aware of the escrow accounts since at least April 2011, but did not initiate any action to limit or stop their use until July 2015. Since then -
  - The law firm was directed to cease making payments from the escrow accounts.
  - A DNR internal audit concluded the accounts effectively created an "off-budget" pool of funds without regard to the State budget or procurement requirements.
  - DoIT provided direction for future RSAs.
  - At the time of our report, the closure of escrow accounts with balances of $536,700 was pending until the disposition of the funds is determined.

Resource Sharing Special (Finding 3)

The financial transactions pertaining to the escrow accounts were not recorded in the State's accounting records and were not monitored by State officials, and the related interest was retained by the law firm.

- Neither DoIT, nor DSP and DNR, had obtained escrow account bank statements to monitor the deposit and disbursement activity and did not ensure the law firm performed monthly bank reconciliations.
- Law firm personnel advised us that the firm did not maintain formal accounting records for the accounts (such as a check register) and did not complete monthly bank reconciliations.
- Interest earned on the escrow accounts ($90,900) was not paid to the State, but was retained by the law firm.

Resource Sharing Special (Finding 4)

- DoIT (as well as DSP and DNR) did not ensure that all compensation due from telecom companies under the RSAs was collected. For eight RSAs, compensation totaling $342,000 was not received, some of which dated back to 2009.

- An initial DoIT (and DSP) RSA had lapsed and provisions were not made for compensation after they expired even though the telecom companies continued using the towers. DoIT advised us that compensation totaling approximately $575,000 should have been received on these agreements through June 2016 (including $200,000 for DoIT's Germantown tower RSA since it expired in October 2012).

Resource Sharing Special Conclusions

DoIT should

- maintain a comprehensive record of all telecom RSAs and tower-installed equipment;
- determine if existing RSAs should be renegotiated, and ensure that all existing arrangements and renewals are supported and approved;
- determine the disposition of the remaining escrow account funds and future RSA payments; and
- establish procedures to ensure that all RSA payments due from telecom companies are received and take necessary actions to collect unpaid compensation.