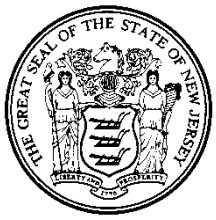

New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Information Technology Governance

August 1, 2016 to May 31, 2017

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

DAVID J. KASCHAK
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 Information Technology Governance for the period of August 1, 2016 to May 31, 2017. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
October 26, 2017

Table of Contents

Scope

The scope of the audit included IT governance operations across the executive branch, including both the Office of Information Technology (OIT) and the individual agencies and departments. Specifically excluded from this audit were boards, commissions, and authorities of the executive branch, as well as the judicial and legislative branches.

Objectives

The objectives of this audit were: (1) to assess the effectiveness and efficiency of the executive branch's IT governance in ensuring that IT decision making supports business objectives, and (2) to assess the effectiveness of the IT governance framework in providing guidance and direction to the executive branch.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

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. Additional guidance for the conduct of the audit was taken from the Control Objectives for Information Technology (CObIT) v.5 published by ISACA, ISO/IEC 38500 – Information technology – Governance of IT for the organization published by the International Organization for Standardization, and other relevant publications related to IT governance best practices.

In preparation for our testing, we studied legislation; agency and statewide policies and procedures; and industry standards and best practices for IT governance. Provisions we considered significant were documented and compliance was verified by interviews of key personnel, review of governance-related documentation, and performance of other tests we considered necessary.

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

Conclusion

Overall, we found that both the OIT as well as the individual agencies recognize the importance of IT governance, and have made progress toward implementing governance practices which support business objectives. However, we noted areas where improvement is necessary in order

to have an effective governance structure which fully supports the varied missions of the executive branch, while providing transparency and accountability.

Background

Information technology (IT) governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. Governance of any type is rooted in the concept that all stakeholders' needs will be addressed to the extent possible, that responsibility for various measurements and results are assigned to parties having the authority and skill to handle the task, and that support for the governance process is obtained from all participants. The concept of IT governance is tied closely with overall organizational governance because information technology cannot effectively and efficiently be utilized to achieve an organization's goals if those goals are not properly defined. For example, the strategic planning process must take place at an organizational business level before the results can be used to develop an IT strategic plan in support of the IT governance process, since the IT strategic plan should be directly related to the business initiatives identified by the organizational business strategic plan.

In 2007 the legislature passed the Office of Information Technology Reorganization Act, which established the Office of Information Technology (OIT) as in but not of the Department of the Treasury. Notwithstanding this designation, the OIT "shall be independent of any supervision or control by the State Treasurer, or the department, or by any division, board, office, or other officer thereof". This act also stated that the OIT shall be directed by the Chief Technology Officer (CTO), who will report directly to the Governor and, under the direction of the CTO, "shall be responsible for providing and maintaining the information technology infrastructure of the Executive Branch of State Government, including all ancillary departments and agencies of the Executive Branch of State Government." In addition, the CTO has the authority to "coordinate and conduct all information technology operations in the Executive Branch of State Government, including agency technology operations". The act also directs all executive branch agencies and departments to cooperate fully with the OIT and the CTO to implement the provisions of the act to "ensure effective use of information technology within the Executive Branch of State Government."

After this legislation passed, we have conducted multiple audits of the OIT and executive branch IT operations. Repeatedly, we have referenced the Information Technology Reorganization Act in our findings and recommendations because of the responsibility for statewide IT operations that it assigns to the OIT. Previous OIT management disagreed with our interpretation of the act, and stated that the ultimate responsibility for items such as security, project management, and contingency planning lies with the individual agencies. The OIT established policies that reflected this position. In contrast, since the appointment of the new CTO and the restructuring of the OIT last year, there has been a noticeable effort to use the authority granted in the act to establish areas of OIT statewide control. Subsequent to our audit period, the Governor signed Executive Order No. 225 which, based on the recommendations of the CTO, authorizes the CTO to identify, consolidate, and centralize IT infrastructure assets and operations. The CTO is also specifically directed to decentralize the application development of

all "agency-specific applications that do not serve shared business requirements across the Executive Branch."

Defining and implementing IT governance measures would allow the OIT to better fulfill its charge of coordinating and conducting all IT operations in the executive branch. Because of the close ties between IT governance and overall business governance, the OIT faces challenges when addressing executive branch IT governance. Individual agencies are responsible for fulfilling their statutory missions to the citizens of the state, but the OIT is not directly responsible for those same missions. Therefore, it is difficult for the OIT to adopt an IT governance framework for the executive branch because they cannot connect that framework to all of the varied business missions of the agencies. The OIT is aware of this, and in our discussions with its management, they have stated that the OIT must create a hybrid governance framework that allows individual agencies to use IT to meet their business missions, while allowing the OIT to define governance requirements and to assign responsibility for those requirements. In summary, the OIT must create a framework that allows the agencies and departments the autonomy to fulfill their statutory missions while also providing structure, guidance, and support from an enterprise perspective.

We focused our audit on compliance with the Information Technology Reorganization Act's requirement that the OIT coordinate and conduct all IT operations in the executive branch. This compliance was assessed within the current organizational model used by the executive branch. We did not evaluate whether this particular model was the most efficient or effective for the executive branch, but rather we worked within the existing structure to make recommendations.

Information Technology Governance Framework

The executive branch has not adopted a statewide information technology governance framework.

From our discussions with management at both the Office of Information Technology (OIT) and executive branch agency levels, we found the following conditions related to IT governance statewide.

- At the beginning of the audit period, the OIT did not have an executive branch IT governance framework. During the audit period, one had been developed that defines the governance decision-making hierarchy that the OIT is proposing; however, this document is still in draft form. This framework features senior-level business and technology experts working together at each agency. The framework will be connected to the Governor's Cabinet; however, the Cabinet will not make decisions unless absolutely necessary. Decisions will be made at the lowest level appropriate for the specific issue. This framework defines general decision-making responsibilities at the agency level, but the agencies will have to assign these responsibilities to specific staff members based on the internal structure of their agency.

- Discussions with executive branch agency IT personnel, as well as requests for documented IT governance frameworks at the agency level, found that 12 of the 14 agencies we surveyed have not, in the absence of an enterprise IT governance framework, adopted a framework of their own. Of the two that have adopted a framework, only one has instituted any type of compliance monitoring at the agency level.

- Discussions with executive branch IT personnel found that 11 of the 14 agencies do not have a formal unit tasked with implementing IT governance that includes the appropriate personnel. The task of IT governance should not fall solely on IT management, but should include key business leaders as well.

Industry standards recommend that organizations have an IT governance structure guiding them to ensure IT resources are used the most efficient and effective way to support the accomplishment of the organization's mission and objectives. Based on our discussions with OIT management, prior to the restructuring in June 2016 the previous OIT management had established a division responsible for IT governance. Although this division did conduct some statewide strategic planning and worked with agency IT management to identify common issues, they did not establish an IT governance framework, nor provide guidance on implementing IT governance at the agency level. With this lack of emphasis and guidance on governance, few agencies pursued developing and adopting a governance framework on their own.

Although agencies may be very adept at managing the IT resources they are responsible for in order to achieve strategic goals, the goal of IT governance is support for the long-term business

objectives of the organization. The lack of a formally adopted IT governance framework can contribute to the inefficient and/or ineffective use of IT resources to meet those objectives. In order to implement such a framework, both the OIT and state agencies need a properly staffed unit, including both IT and business leaders, with responsibility for the task. In addition, monitoring at either the OIT or agency level is necessary to assess compliance with the adopted framework.

Recommendation

We recommend the OIT finalize and adopt the IT governance framework that is currently in draft form. In addition, we recommend the OIT create implementation guidance for agencies which includes establishing a representative group charged with agency IT governance as well as a monitoring process for compliance with the governance framework.

Information Technology Strategic Planning

Neither the executive branch as a whole, nor many of its individual agencies, have a current information technology strategic plan.

From our discussions with management at the OIT and at state agency levels, we found a lack of current IT strategic plans. In the spring of 2013, OIT management conducted a statewide strategic planning project which involved the agencies completing and submitting to the OIT an IT strategic plan covering the period July 1, 2014 to June 30, 2016. The OIT used the information contained in those plans to craft an OIT strategic plan for the same period.

When our audit began, we found no evidence that an OIT strategic plan covering any period beyond this had been developed or was in development. Current OIT management stated that the restructuring of the OIT that accompanied the appointment of the new Chief Technology Officer (CTO) needed to be fully realized before the strategic planning process could begin. As of the end of the audit period, the OIT strategic planning process has begun, but no completion date has been set. Additionally, of the 14 agencies that we surveyed, 12 did not have an IT strategic plan that covered the current period. These agencies' last strategic plans were the July 1, 2014 to June 30, 2016 plans submitted as part of the aforementioned project.

Strategic planning is a critical and necessary part of managing an organization, and should be performed periodically depending on the maturity of the organization. It is essential for setting goals and providing direction to an organization's IT management team, and a lack of a current strategic plan could lead organizations to use resources in an inefficient or ineffective manner.

Based on our discussions with OIT, there was no action by the previous management team to repeat the strategic planning project that was used for the fiscal year 2014 to 2016 time period. When the new CTO took over in 2016, there was a reassessment of the vision and mission of

the OIT which needed to be completed before strategic planning could begin. With regard to the individual agencies, there was no definitive reason why the 12 agencies did not develop IT strategic plans for their organizations. Some agencies noted that IT strategic planning flows naturally from business strategic planning, and that their agency had not prepared a business strategic plan for them to utilize. Other agencies noted that they had insufficient resources or time to complete many of the items from the previous strategic plan, and therefore decided to continue with the existing plan.

Recommendation

We recommend the OIT complete its strategic planning process in a timely manner and provide guidance to the agencies on developing their own IT strategic plans. The agency plans do not necessarily have to be incorporated directly into the OIT strategic plan as was done previously; however, agency plans should be submitted to OIT for information and documentation purposes.

Data Governance

The executive branch does not have a data governance framework.

A data governance framework is a logical structure for the classification, organization, and communication of activities involved in making decisions about enterprise data. Effective data governance serves an important function within the enterprise by setting the parameters for data management and usage, creating processes for resolving data issues, and enabling business users to make decisions based on high-quality data and well-managed information assets. Poor data governance can result in a loss of financial and information assets, as well as compromise the executive branch's responsibility as a steward of the data it is entrusted with.

The executive branch is lacking in some aspects of data governance. At the beginning of the audit period, discussions with the Office of Information Technology (OIT) disclosed that there was no data governance framework. There had been one in draft form previously, but it was never finalized because of the many concerns expressed by the agencies. From our field visits and information requests to the agencies, we found that 10 of the 14 agencies surveyed had not adopted their own data governance framework in the absence of one at the executive branch level. In addition, only two agencies had developed a standardized template to use as a basis for all data sharing agreements. However, 10 of the 14 agencies we surveyed had at least one data sharing agreement in place, meaning that they were allowing an entity, either internal or external to the state, to access and use their data. Our review of data sharing agreements in place at all 10 of the agencies utilizing them noted that they contained the necessary elements of an agreement. This includes items such as assigning responsibilities to each party, defining the dataset parameters and time frame of the agreement, and addressing data confidentiality and destruction.

In February of 2017, the legislature passed the New Jersey Open Data Initiative which statutorily created the position of Chief Data Officer (CDO) for the executive branch and granted authority to the CDO, in consultation with the Attorney General, to establish any policies and procedures necessary to fulfill the provisions of the act and monitor agencies' compliance. It also charged the CDO with enabling and coordinating the open sharing of data between agencies. This authority will greatly assist the OIT in implementing a data governance framework. The OIT has started the process of bringing agencies together to create a data governance framework, but the project is still in development.

Recommendation

We recommend the OIT use the authority granted in the New Jersey Open Data Initiative to complete and implement a data governance framework for the executive branch. In addition, the OIT should provide guidance to agencies with regard to data sharing, as well as document all existing data sharing agreements in order to facilitate data sharing between state agencies as well as between the agencies and outside parties.

Enterprise Security Program

The executive branch should improve the organization and message of its Enterprise Security Program.

In 2015, the Chief Information Security Officer (CISO) and Office of Information Technology (OIT) security group were relocated to the campus of the Office of Homeland Security and Preparedness (OHSP). The CISO became an OHSP employee, but members of the security group remained OIT employees. The move was enacted to consolidate information security resources and use them in the most efficient way. However, it further separated the security personnel at OIT from the agencies to whom they provided services, as well as raised uncertainty about the direction of enterprise security policy, since only the OIT currently has the authority to establish such policy.

The focus of our field work with state agencies was to determine what changes have occurred after the OIT security group moved to OHSP in 2015. Of the 14 agencies we spoke with, 10 expressed that they had an overall negative experience with the security group after they moved from OIT to OHSP. The majority of the agencies' issues were connected to lack of communication from the security group and agency confusion as to the responsibility for security guidance. All of the agencies stated that they adhere to the existing OIT security policies; however, three agencies have developed their own security framework to compensate for the perceived lack of guidance. Of the agencies we interviewed, six stated that they perform some level of monitoring with the enterprise security policy, while the others relied on the monitoring efforts of the OIT and the OHSP. We found no evidence that the OIT security group

did not continue to perform their functions for the agencies, only that communication with the agencies was lacking.

We discussed the situation with OHSP and OIT security management, and they agreed that clear communication channels had not been established with the agencies, but that the OHSP had begun to reach out to all agencies to discuss any issues they might have. They are also working on an updated enterprise security framework as well as revising, consolidating, and rebranding enterprise security policies in order to provide additional clarity to agencies. In addition, the OHSP is expanding its enterprise security offerings in order to provide standardization across the executive branch and centralization of security operations. There has also been discussion about how the OIT and the OHSP can work together to issue enterprise IT policy.

The OHSP did not anticipate the communication needs of the agencies and the OIT security group, and therefore did not provide either with effective channels for communication in both directions. This lack of communication could cause the agencies to duplicate security measures already being addressed at an enterprise level. In addition, it becomes difficult for the agencies and the OIT security group to assess overall effectiveness of the security measures in place without detailed knowledge of the efforts of all parties.

Recommendation

We recommend the OIT and the OHSP work together with the agencies to identify security measures in place at all levels, and establish open and reliable communication paths. The OIT and the OHSP should also work together to clarify and standardize enterprise policies, procedures, and standards in the area of information security. If any question is raised about the legal authority to establish enterprise IT policy, the OIT and the OHSP should take steps appropriate to obtain the authority necessary to successfully implement the security framework.

Risk Assessments

The executive branch has not coordinated and supported the conducting of agency information technology risk assessments.

One of the documents we requested from each state agency was their most recent agency-wide IT risk assessment. Agencies provided various documents covering topics such as asset classification, network vulnerability, disaster recovery, project management, and individual application risk. Although all of these documents are components of an agency-wide IT risk assessment, only three agencies presented a complete risk assessment.

Risk assessments address the potential adverse impacts to organizational operations and assets arising from the use of information systems and the information processed, stored, and

transmitted by those systems. Organizations conduct IT risk assessments to determine risks to the organization's core business functions and processes, infrastructure and support services, and information systems. The Office of Information Technology (OIT) management team published a risk management policy in 2014 that is focused on information security risk management. It requires agencies to complete periodic risk assessments, prioritize the risks, and implement mitigation controls and procedures. The OIT must consider the risks that agencies face in order to help coordinate the response to those risks, and agency assessments are a key element in that understanding. The new OIT management has begun some comprehensive IT risk assessment initiatives related to security, therefore setting a precedent for the OIT to take the lead in this area. Although agencies have conducted components of an IT risk assessment, a lack of comprehensive and consistent risk analyses prevents the state from identifying the shared IT risks of the agencies, and the opportunity for shared solutions that may be available.

Recommendation

We recommend the OIT coordinate and guide agencies through a comprehensive IT risk assessment process, and use the results of that risk assessment to develop its governance priorities.

⋙➤✦⋘

Compliance Monitoring

The executive branch does not have a process in place for the monitoring of compliance with enterprise frameworks and policies.

One of the vital pieces of a successful governance structure is the monitoring of compliance with the governance framework as well as organizational policies. Currently, the OIT does not perform a monitoring function, nor do they coordinate the monitoring activities of agencies. In our discussions with agencies, 8 of 14 stated that they themselves did not have an adequate monitoring and compliance function for standard operating procedures. In addition, of the two agencies that have developed their own governance framework, only one instituted any type of compliance monitoring. One agency discussed their inability to support a monitoring function for their data sharing agreements, and multiple agencies expressed that they would like to see better support and guidance in the area of compliance.

Multiple statewide IT policies assign responsibility for oversight of the implementation and operation of a policy's tenets to the OIT. Because there is currently no enterprise policy related to information technology or data governance, the monitoring and compliance functions for these policies are not yet defined. Although it is not necessary for OIT to perform the monitoring function for all enterprise policies directly, they should, at a minimum, set compliance requirements for the agencies. Without an effective compliance function, an organization cannot be certain that policies and procedures are being followed. Since policies

are created to standardize operations and adhere to industry standards, failure to comply with policies can expose the organization to risk.

Recommendation

We recommend the OIT develop a monitoring and compliance function to conduct or oversee compliance monitoring activities as necessary at the OIT and agency levels. Also, new policies that are established should include a description of the necessary compliance monitoring activities, as well as assign responsibility for those activities.

Observations

Funding Model

The funding model for the Office of Information Technology should be reexamined.

The Office of Information Technology (OIT), for budgetary purposes, is placed within the Department of the Treasury. Prior to fiscal year 2008, OIT was funded by billing a combination of amounts appropriated for IT in other state agencies, federal funds, and dedicated resources. State user agencies paid the OIT from these sources for the information processing services provided. In fiscal year 2008 the process was changed, and $41.4 million in state appropriations for OIT services was moved from the agencies directly to the OIT "to provide flexibility and funding certainty in operating the State's core information technology infrastructure."

The amounts moved to the OIT appropriation were determined by the Office of Management and Budget (OMB) based on the billed amounts agencies paid with their state appropriated funds in fiscal year 2007. For example, if an agency paid for their services with one half state appropriations and one half federal or dedicated funds in fiscal year 2007, the amount that was paid for with state appropriations was moved to the OIT's direct appropriation the following year. For all subsequent years, half of the services provided by the OIT would be charged against the OIT's direct appropriation, and the remaining half would be billed directly to the agency by the OIT finance department. It should be noted that the state billing rate is lower than the non-state rate.

Some agencies designated as 100% state-funded had their complete IT budget re-appropriated to the OIT. However, that did not eliminate the need for those agencies to maintain agency IT staff. For the 14 agencies we surveyed, we identified 157 application development staff and 70 network staff employed directly by those agencies. In addition, agencies must maintain IT management, security, operating system, and database personnel. These must be paid for with the agency's funds.

Agencies currently pay the OIT based on the split determined in fiscal year 2007, regardless of the agency's actual current funding sources. The OIT annually requests that the OMB review, and possibly adjust, these splits. If an individual agency believes that their split should be adjusted, they can contact the OMB directly and request that it be reviewed. The OIT noted there have been instances where the split has been adjusted as a result of such a request.

Rates for services are set at the beginning of the fiscal year based on usage estimates to allow the OIT to recover 100 percent of its costs through the combination of charges against advanced appropriations and direct billings to agencies. If usage is lower than expected, rates must be recalculated to ensure the OIT recovers all costs.

With regard to the billing process itself, seven of the agencies we surveyed stated that they have found inaccuracies and inconsistencies in the billing statements they receive from the OIT. In addition, agencies who are billed directly for services are concerned that they will be billed for new services without consultation or prior notice of the new charges, and will have to find resources to pay for them. The OIT has stated that they are working to improve the billing system, as well as create a catalog of services with consistent, fixed pricing.

The fiscal year 2008 budget stated that the change was made to create flexibility and funding certainty to assist the OIT's implementation of the recommendations provided by the Commission on Government Efficiency and Reform. This commission was created to overhaul and modernize the state's information technology systems, including the creation of a comprehensive business plan for statewide services, the coordination of planning across all departments, and the identification of potential management efficiencies.

The current conditions are a result of multiple factors. First, the decision to move the OIT to a dedicated funding model shifted appropriations from the agencies to the OIT, but did not remove the agencies' need for their own IT personnel. Secondly, the OIT has had difficulty determining accurate billing rates for services because of the effects of changing demand, although this has been a main focus of the new CTO. Lastly, OIT must bill 100 percent of their operation either against their advance appropriation or directly to agencies for payment, which means they must have an agency to associate with the charged amount.

There are five potential effects this situation could have.

- A cycle could arise in which agencies stop using an OIT service because it is more expensive than what the agency would pay for the same service from an outside vendor. This loss of business would drive the price higher for the remaining customers, since OIT must bill for 100 percent of its costs. This would make the OIT service even more expensive, and more agencies may choose to stop using the OIT for services.

- The current state/non-state funding splits that are used in the billing process may no longer accurately reflect the actual funding sources for the agencies. This could lead to incorrect use

of the state and non-state rates when billing agencies for services, and potential underpayment or overpayment for services.

- New services that are added to agency billings could eventually cause billing to exceed the OIT's appropriation, or increase billings in excess of the agencies' own expected IT budgets.

- The fact that the OIT must charge 100 percent of its services to the agencies hinders the ability for the OIT to be on the leading edge of new technology and to maintain knowledge levels for staff. If an agency requests information regarding a new technology, the OIT would have to charge that agency for the time spent researching the topic. This strongly discourages the exploration of new initiatives at, or through, OIT.

- Since agencies needed to keep their own IT personnel in place, there is some question as to the cost savings of the funding model change. The OIT has begun studying this issue by requiring agencies to submit all IT expenditures, both OIT charged and agency level, to the OIT on a quarterly basis.

There is a need for the departments involved in the budgeting and billing process to evaluate the current funding model for OIT and determine if it is the most effective and efficient way to finance statewide OIT operations. If the decision is made not to change the current model, then aspects of the model should be changed to address the five concerns listed above.

Training

IT training opportunities are not being effectively and efficiently maximized.

While reviewing the strategic plans of the agencies we surveyed, we found that all of them identified a lack of training for IT staff as either a current weakness or a future threat. Agencies felt that training was not adequate to provide professional development for their staff.

In the ever-changing world of information technology, keeping personnel current on the latest technologies, and methodologies for managing those technologies, is crucial to having the most efficient and effective use of resources. In addition, OIT and agency management have both expressed a desire to create a common knowledge base which would be shared across agencies in order to improve communication. For example, the OHSP recently provided security training to agency personnel in order to establish a baseline which all agencies can share.

Based on our discussions with agency IT management, resource issues were the biggest cause of the lack of training. The lack of funding caused training to be de-emphasized at the agency level because identifying training needs is fruitless if the training cannot be provided. Failure to provide training opportunities leaves the organization with personnel who are not operating at the most effective level possible. In addition, the current decentralized training structure can lead to the lack of a common knowledge base between agencies, as well as not being the most efficient and effective use of limited training resources.

The OIT has an opportunity to work with agencies to identify common training needs and help the agencies make the most efficient use of funds by coordinating statewide training whenever possible.

State of New Jersey

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

Office of Information Technology
P.O. Box 212
Trenton, New Jersey 08625-0212

DAVE WEINSTEIN
Chief Technology Officer

October 19, 2017

David J. Kaschak
Assistant State Auditor
Office of the State Auditor
Office of Legislative Services
P.O. Box 067
Trenton, NJ 08625-0067

Dear Mr. Kaschak:

Enclosed is the New Jersey Office of Information Technology's (NJOIT's) response to the draft Information Technology Governance report you provided to us on October 2, 2017.

As requested we have provided you with NJOIT's written comments so they can be presented in conjunction with your official release to the Governor and the Legislature scheduled for Tuesday, October 24, 2017.

Sincerely

David J. Weinstein
Chief Technology Officer
Office of Information Technology

The New Jersey Office of Information Technology's
Response to

The New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor's

Information Technology Governance Audit
August 1, 2016 to May 31, 2107

FINDINGS

OSA Finding: "The executive branch has not adopted a statewide information technology governance framework. "

OSA Recommendation: *"We recommend the OIT finalize and adopt the IT governance framework that is currently in draft form. In addition, we recommend the OIT create implementation guidance for agencies which includes establishing a representative group charged with agency IT governance as well as a monitoring process for compliance with the governance framework."*

NJOIT Response:

The NJOIT agrees with the recommendation and will finalize a single unified Governance Framework for the executive branch escalating up through the Cabinet and ultimately the Governor's office. The Enterprise Governance Framework (the Framework) will address Technology and Information (Data) Governance initially as required by this audit, and will be flexible enough to scale as needed to include other governance areas identified by the Executive, Legislative or Judicial branches.

The NJOIT shall publish policies and guidelines for executive branch Agencies to facilitate their compliance with and participation in the Framework.

The NJOIT shall expand its current Internal Monitoring and Compliance (IMAC) Unit to enable the monitoring of Agency compliance with the Framework for technology governance.

OSA Finding: "Neither the executive branch as a whole, nor many of its individual agencies, have a current information technology strategic plan."

OSA Recommendation: *"We recommend the OIT complete its strategic planning process in a timely manner, and provide guidance to the agencies on developing their own IT strategic plans. The agency plans do not necessarily have to be incorporated directly into the OIT strategic plan as was done previously; however, agency plans should be submitted to OIT for information and documentation purposes."*

NJOIT Response:

The NJOIT agrees with the recommendation requiring current and coordinated strategic plans across the executive branch for information technology. The NJOIT will develop and implement an Enterprise Strategic Planning process for information technology tied to and in support of the Governor's and Agencies' Business Strategy; The Strategic planning process shall align with beginning of each new administrative term (or every four years) and the resulting plans shall be monitored annually.

The NJOIT shall publish policies and guidelines for executive branch Agencies to facilitate their participation in Enterprise Strategic Planning process for Information Technology and their compliance with the published plans.

The NJOIT shall confirm Agency Strategic Plans for information technology and monitor via architectural review processes and by the review of technology purchases request based on defined criteria.

OSA Finding: "The executive branch does not have a data governance framework."

OSA Recommendation: *"We recommend the OIT use the authority granted in the New Jersey Open Data Initiative to complete and implement a data governance framework for the executive branch. In addition, the OIT should provide guidance to agencies with regard to data sharing, as well as document all existing data sharing agreements in order to facilitate data sharing between state agencies as well as between agencies and outside parties."*

NJOIT Response:

The NJOIT agrees with the recommendation and will finalize a single unified Governance Framework for the executive branch escalating up through the Cabinet and ultimately the Governor's office. The Enterprise Governance Framework (the Framework) will address Technology and Information (Data) Governance initially as required by this audit, and will be flexible enough to scale as needed to include other governance areas identified by the Executive, Legislative or Judicial branches.

The NJOIT and the State Chief Data Officer will work in cooperation with the Attorney General to develop a single data sharing agreement for use within the executive branch and one for use with external stakeholders; and as required by P.L.2017, CHAPTER 2, (6) ensure that...

"Notwithstanding any rule, regulation or statute to the contrary, agencies shall be actively encouraged by the Chief Data Officer and the State Treasurer to share open data and datasets with each other without formal agreements, provided that no existing laws regarding the security of personal, private, and confidential information are violated. The sharing of personal, private, or confidential data shall be permitted only when in conformity with restrictions, established by the Chief Data Officer in cooperation with the Attorney General, to ensure that the data is used in a manner that is secure and in conformity with State law."

The NJOIT shall publish policies and guidelines for executive branch Agencies to facilitate their compliance with and participation in the Framework.

The NJOIT will work in cooperation with the State Chief Data Officer to enable the monitoring of Agency compliance with the Framework for information governance.

OSA Finding: "The executive branch should improve the organization and message of its Enterprise Security Program."

OSA Recommendation: *"We recommend the OIT and the OHSP work together with the agencies to identify security measures in place at all levels, and establish open and reliable communication paths. The OIT and the OHSP should also work together to clarify and standardize enterprise policies, procedures, and standards in the area of information security. If any question is raised about the legal authority to establish enterprise IT policy, the OIT and the OHSP should take steps appropriate to obtain the authority necessary to successfully implement the security framework."*

NJOIT Response:

The NJOIT, as an Agency of the executive branch, will comply with the enterprise security standards as defined by the OHSP for the executive branch; In addition, to support NJOIT's mission and to secure the state's infrastructure, the NJOIT will work in cooperation with the OHSP to define and implement additional security measures as necessary.

The State Chief Data Officer, as required by New Jersey Open Data Initiative, shall develop policies, procedures and standards to be used by all agencies to ensure data is reliable and fit for purpose, and will coordinate with the NJOIT and the OHSP to develop enterprise security standards for the state's data and information.

The NJOIT will coordinate with the OHSP to ensure consistent messaging within our agency but will defer to the OHSP on messaging across the executive branch for enterprise security initiatives.

OSA Finding: "The executive branch is not coordinating and supporting the conducting of agency information technology risk assessments."

OSA Recommendation: *"We recommend the OIT coordinate and guide agencies though a comprehensive IT risk assessment process, and use the results of that risk assessment to develop its governance priorities."*

NJOIT Response:

The NJOIT agrees with the recommendation for routine and comprehensive IT risk assessments. However, the authority to define the requirements of assessment, to coordinate them across the executive branch, and to ensure compliance with the findings of the assessments, lies with the OHSP.

The NJOIT will conduct risk assessments on the enterprise and internal IT assets for which NJOIT is responsible, and use those results to inform NJOIT priorities.

The NJOIT will defer to OHSP to direct agencies on their own assessment protocol and schedule, and how any results of assessments will impact agency or enterprise strategic security priorities.

OSA Finding: "The executive branch does not have a process in place for the monitoring of compliance with enterprise frameworks and policies."

OSA Recommendation: *"We recommend the OIT develop a monitoring and compliance function to conduct or oversee compliance monitoring activities as necessary at the OIT and agency levels. Also, new policies that are established should include a description of the compliance monitoring necessary, as well as assign responsibility for those activities."*

NJOIT Response:

The NJOIT agrees with the recommendation for routine monitoring and compliance auditing for enterprise IT policies and frameworks. In 2016, the NJOIT established a new Deputy Chief Technology Officer (DCTO) for Policy and Governance to bifurcate those responsibilities from IT operations and to elevate the importance of the governance function for technology and data.

Since the beginning of the audit, the NJOIT has modified its policy development process and is currently updating all polices to include a monitoring and compliance component.

Additionally, NJOIT's Internal Monitoring and Compliance (IMAC) Unit has been moved under the DCTO for Policy and Governance. Its original mission, to facilitate external auditing of NJOIT, will be expanded to include monitoring and compliance activities for all NJOIT (internal and executive branch) IT policies.

OBSERVATIONS

OSA Observation: "The funding model for the Office of Information Technology should be reexamined."

NJOIT Response:

The NJOIT concurs with the observation that the current funding model does not adequately fund research and development of new technology. The NJOIT will work in cooperation with the Department of Treasury to develop a model to more effectively and efficiently finance statewide IT operations and support the innovation, research and development of new technology.

OSA Observation: "IT training opportunities are not being effectively and efficiently maximized."

NJOIT Response:

The NJOIT concurs with the observation that a focused, coordinated training program for IT skills would better leverage scarce training resources statewide as well as providing a consistent foundation of IT skillsets for the executive branch. The NJOIT will review options for developing a more centralized training and development program for high-demand IT skills; which may be leveraged across the executive branch.