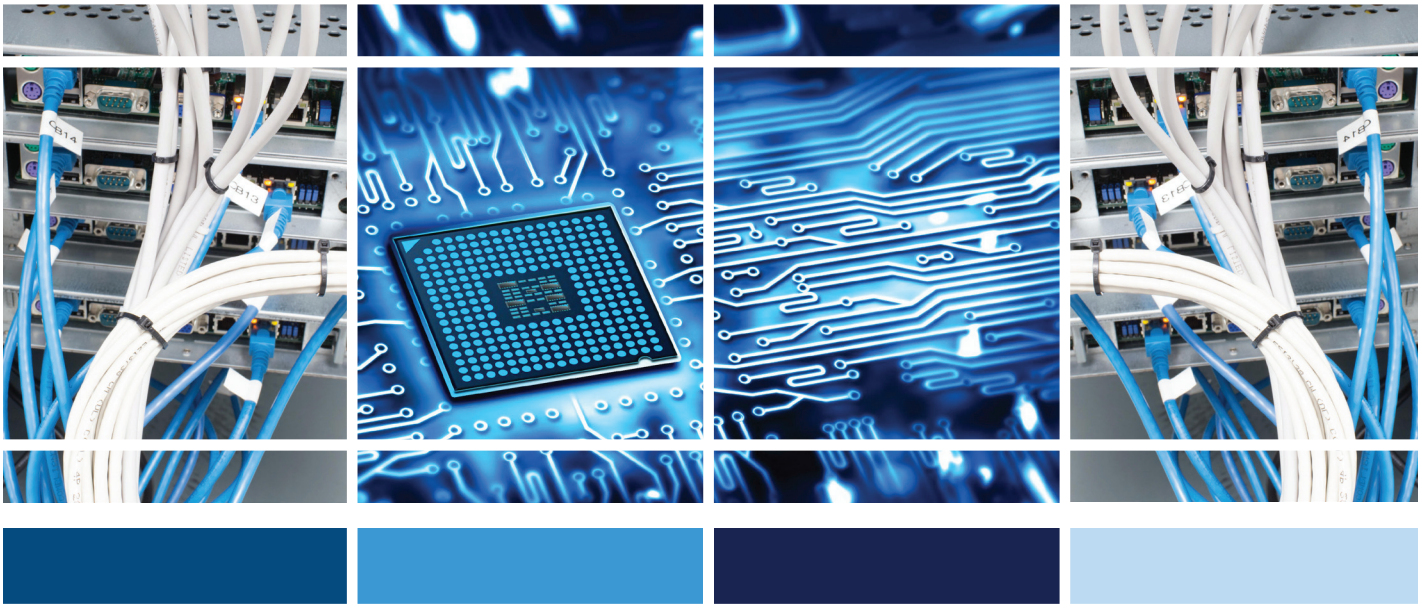
Report to the Governor and the General Assembly of Virginia

Virginia's Information Technology Governance Structure



JLARC
JOINT LEGISLATIVE AUDIT
AND REVIEW COMMISSION

Commonwealth of Virginia
September 2014

JLARC Staff for this Report
Kimberly Sarte, Assistant Director for Ongoing Oversight and Fiscal Analysis
Mark Gribbin, Principal Legislative Analyst for Ongoing Oversight and Fiscal Analysis

Report No. 459

http://jlarc.virginia.gov

COMMONWEALTH of VIRGINIA

Joint Legislative Audit and Review Commission
201 North 9th Street, General Assembly Building, Suite 1100
Richmond, Virginia 23219

Hal E. Greer
Director

(804) 786-1258

December 15, 2014

The Honorable John C. Watkins, Chair
Joint Legislative Audit and Review Commission
General Assembly Building
Richmond, Virginia 23219

Dear Senator Watkins:

The 2013 Appropriation Act directed the Joint Legislative Audit and Review Commission to review and evaluate the Virginia Information Technologies Agency on a continuing basis.

This report was briefed to the Commission and authorized for printing on September 8, 2014. On behalf of the Commission staff, I would like to thank the Secretary of Technology, the Chief Information Officer, and the staff of the Virginia Information Technologies Agency for assistance during this review. I would also like to acknowledge staff of the many Virginia agencies and IT professionals in other states who provided information and assistance.

Sincerely,

Hal E. Greer
Director

Contents

Summary i

Recommendations v

Chapters

1. Overview of State IT Governance 1

2. Separating Secretary and CIO Responsibilities 9

3. Improving Central IT Leadership 21

4. Clarifying VITA's Statutory Responsibilities 27

5. Increasing Agency Involvement in Central IT Decisions 37

Appendixes 45

Report summary
Virginia's IT Governance Structure

WHAT WE FOUND

Overlapping secretarial and CIO responsibilities make it unclear who is accountable for central IT decisions

The Secretary of Technology and the Chief Information Officer (CIO) have several overlapping responsibilities for governing the state's information technology (IT), making it unclear who is accountable for central IT decisions. Both the secretary and CIO approve VITA's contracts for statewide IT services, which can undermine the CIO's authority by allowing vendors to circumvent the CIO and go directly to the secretary. The secretary and CIO also have overlapping responsibility for approving state IT standards and agency investments. Overlapping approval does not appear to add benefits, and no other Virginia cabinet secretary is charged with approving the specific decisions of an agency director. The added approval authority appears unnecessary because, like all cabinet secretaries in Virginia, the Secretary of Technology is already vested with general supervisory powers.

The secretary and CIO also have overlapping responsibility for coordinating the development of enterprise applications, which are used to manage the state's central administrative functions. Past coordination efforts have required secretarial intervention in inter-agency disputes, and the secretary is best positioned to perform this responsibility.

WHY WE DID THIS STUDY

Under the Appropriation Act, the Joint Legislative Audit and Review Commission (JLARC) is required "to review and evaluate the Virginia Information Technologies Agency (VITA) on a continuing basis and to make special studies and reports as may be requested." In November 2013, because of concerns identified during the course of JLARC's ongoing oversight, the Commission Chair and Vice-Chair approved a review of the state's information technology governance structure.

ABOUT IT GOVERNANCE

Information technology (IT) is essential to the daily operations of state government. Effective IT governance is needed to ensure continuity of agency operations, protect sensitive personal information about Commonwealth citizens, and avoid wasted spending.

Virginia has established a partially centralized structure for governing IT, which requires cooperation between the Virginia Information Technologies Agency (VITA) and other state agencies. The Chief Information Officer oversees VITA and reports to the Secretary of Technology.

Although the state's partially centralized IT structure has provided benefits, it has also created challenges. Challenges need to be addressed promptly because the state will soon make major decisions about its future IT needs when its contract for central IT services with Northrop Grumman expires in 2019.

CIO does not regularly meet with the state's executive leadership

Virginia's CIO does not appear to have regular discussions with the governor or cabinet, even though their support is critical for statewide IT initiatives. The Secretary of Technology's role in ensuring effective communications of state IT issues with the state's executive leadership is also not explicit. CIOs in other states and private companies emphasized the importance of regular discussions with their executive leadership about IT issues. Discussion of major IT issues will be especially important as the state

determines how to meet its future needs when its contract for IT services with Northrop Grumman expires in 2019.

CIO needs assistance to fulfill dual roles

The CIO performs two roles: (1) central leader overseeing state IT and (2) IT services provider to state agencies. Fulfilling both of these roles is challenging, and the current CIO indicated that his duties limit his ability to regularly meet with agency directors to discuss statewide initiatives. Additionally, these roles can sometimes conflict with one another because the CIO could use oversight powers to compel agency actions that benefit VITA instead of the state as a whole. Other Virginia agency directors are often assisted by one or more deputies. These deputies allow for delegation of responsibility and create internal divisions within the agency that reduce the risk posed by conflicting duties.

VITA's main responsibilities are not clearly defined

Current statute does not clearly define VITA's main duties. Most notably, VITA's responsibility to centralize the state's IT infrastructure, which is one of the main reasons it was created, is established in the uncodified Acts of Assembly instead of the Code of Virginia. Other key responsibilities for setting IT standards and overseeing agency projects and procurements are either not entirely codified or spread throughout several sections of Code. Many of the responsibilities are duplicative and inconsistent with one another. This makes it difficult to determine the scope of VITA's responsibilities and the authority it has for enforcing agency compliance with central IT requirements.

Responsibility for securing state data is not clearly assigned

VITA and agencies must cooperate to effectively secure the state's data. VITA and agency cooperation has substantially reduced security incidents in the past year, but cooperation is still lacking in several areas. Most notably, only 32 percent of agencies have performed all of the security audits that are needed to ensure sensitive data is properly protected. Compliance appears to be low because some agencies may not view IT security as a high priority. This may be due in part to Virginia statute, which does not clearly assign agencies with responsibility for protecting their data or complying with the state's IT security and risk management program.

Agencies generally comply with IT procurement requirements, but some enforcement mechanisms are lacking

Agencies appear to generally comply with IT procurement requirements, but violations can create security risks and support challenges. Virginia statutes include many provisions that are intended to encourage agency compliance with state procurement laws. However, it is not clear whether two of these provisions apply to IT procurements: the

provision that the state comptroller is to stop payments for improperly conducted procurements, and the provision that holds purchasing officers accountable for repeatedly and intentionally violating procurement requirements.

Agency involvement in central IT decisions is limited

Even though agencies have a substantial stake in central IT decisions, they do not have an active role in the decision making process. Agency involvement is limited to advisory bodies. The most significant agency advisory body, the IT Advisory Council (ITAC), has been largely ineffective. Agencies had limited involvement in many of the decisions that led to the contract for services from Northrop Grumman, which appears to be one reason why these services sometimes do not meet agency needs.

Other states and private companies involve business leaders, such as agencies, in their central IT decisions, and each uses an approach that is unique to its organization. Virginia could benefit by developing its own governance approach that includes agencies in key central IT decisions, including planning for the end of the state's contract with Northrop Grumman.

WHAT WE RECOMMEND

Legislative action

- Remove statutory requirements that the Secretary of Technology approve specific CIO operational decisions.
- Assign the secretary responsibility for communicating IT issues to the state's executive leadership.
- Develop and enact legislation that reorganizes, clarifies, and codifies VITA's statutory responsibilities.
- Assign agency directors responsibility for securing their IT data, and assign VITA responsibility for supporting agency efforts.
- Clarify that IT procurements shall be stopped if they do not follow requirements and that purchasing officers are accountable for violations.

Executive action

- The secretary and CIO should implement procedures that ensure the CIO meets and discusses IT issues with the state's executive leadership.
- VITA should establish a classified deputy CIO position to assist the CIO.
- The ITAC should develop a proposal for including agencies in planning for the expiration of the Northrop Grumman contract and a proposal for more broadly involving agencies in key central IT decisions.

See page v for the complete list of recommendations.

Recommendations

Virginia's IT Governance Structure

RECOMMENDATION 1

The General Assembly may wish to consider amending the Code of Virginia and the Appropriation Act to remove requirements that the Secretary of Technology approve specific operational decisions made by the CIO, including (1) approving VITA contracts and amendments for statewide IT services, (2) approving and making other decisions related to agency IT projects and procurements, and (3) approving and developing state IT standards (Chapter 2, page 15).

RECOMMENDATION 2

The General Assembly may wish to consider amending § 2.2-225 and § 2.2-2007 of the Code of Virginia to reassign the CIO's responsibilities for coordinating the development of central administrative enterprise applications to the Secretary of Technology (Chapter 2, page 17).

RECOMMENDATION 3

The General Assembly may wish to consider amending the Appropriation Act to require that the CIO approve contractual agreements between agencies and CGI Technologies and Solutions, Inc. (Chapter 2, page 18).

RECOMMENDATION 4

The General Assembly may wish to consider amending § 2.2-225 of the Code of Virginia to vest the Secretary of Technology with responsibility for communicating state IT issues to the governor and members of the cabinet (Chapter 3, page 24).

RECOMMENDATION 5

The governor's office, Secretary of Technology, and the CIO should develop and implement procedures for regular discussion of critical state IT issues with the governor and the cabinet. Procedures should ensure that the CIO has the opportunity to directly confer with the governor or governor's staff and other cabinet members about these issues (Chapter 3, page 24).

RECOMMENDATION 6

VITA should establish and the Secretary of Technology should approve a classified position of Deputy CIO to assist the CIO in the fulfillment of the CIO's duties, including managing VITA services and assisting in planning for the end of the Northrop Grumman contract (Chapter 3, page 26).

RECOMMENDATION 7

The General Assembly may wish to consider amending the Appropriation Act to direct the formation of a technical working group, led by the Division of Legislative Services and including staff of JLARC, the Joint Commission on Technology and Science, the Office of the Secretary of Technology, VITA, and the Office of the Attorney General, to develop legislation that reorganizes, clarifies, and codifies VITA's existing responsibilities, including those established in enactment clauses and the Appropriation Act. Legislation should be presented to the Joint Legislative Audit and Review Commission by November 2015 so that it may be considered for the 2016 General Assembly session (Chapter 4, page 30).

RECOMMENDATION 8

The General Assembly may wish to consider amending the Code of Virginia to adopt the legislative changes developed by the technical working group for reorganizing, clarifying, and codifying VITA's existing responsibilities (Chapter 4, page 30).

RECOMMENDATION 9

The General Assembly may wish to consider amending § 2.2-603 of the Code of Virginia to assign agency directors responsibility for securing the electronic data held by their agencies and clarify their responsibility to comply with the requirements of the state's IT security and risk management program (Chapter 4, page 35).

RECOMMENDATION 10

The General Assembly may wish to consider amending § 2.2-2009 of the Code of Virginia to assign the CIO responsibility for providing agencies with information and other assistance needed to meet the requirements of the state's IT security and risk management program (Chapter 4, page 35).

RECOMMENDATION 11

VITA should amend IT standards to reflect its responsibility to provide agencies with information and other assistance needed to meet the requirements of the state's IT security and risk management program (Chapter 4, page 35).

RECOMMENDATION 12

The General Assembly may wish to consider amending § 2.2-2012 of the Code of Virginia to stipulate that the state comptroller shall not authorize payment for IT purchases made in violation of state laws or IT procurement requirements and that intentional violations of centralized IT purchasing requirements can result in the responsible purchasing officer being suspended or removed from office (Chapter 4, page 36).

RECOMMENDATION 13

The state Information Technology Advisory Council should develop and VITA should implement a specific proposal for involving agencies in planning for the expiration of the state's contract with Northrop Grumman by April 2015 (Chapter 5, page 43).

RECOMMENDATION 14

The General Assembly may wish to consider amending the Appropriation Act to require that the Information Technology Advisory Council (ITAC) develop a proposal for improving agency involvement in key central IT decisions. In developing the proposal, ITAC should consider the appropriate level of agency involvement in decisions affecting all areas of governance. The proposal may include changes to the statutory governance structure, if ITAC determines such changes are needed. The written proposal should be provided to the JLARC chairman by November 2015 (Chapter 5, page 43).

1 Overview of State IT Governance

SUMMARY Effective governance of information technology (IT) is essential to successful state operations. By properly managing IT, the state can better serve its citizens and maintain the continuity of its operations. IT failures can disrupt service delivery, waste money, and put the personal information of Virginians at risk. Virginia's IT governance responsibilities are defined under statute and include responsibilities for planning and standards, managing assets, making investments, and ensuring security. Responsibilities are vested with central authorities, most notably the Virginia Information Technologies Agency, and with individual state agencies. IT reforms carried out over the last several years have centralized several aspects of the state's IT governance structure. These reforms have generated several benefits, but some longstanding issues remain unaddressed and new challenges have been created. These concerns have taken on an increased urgency because the state will need to make major decisions regarding its IT environment in the next several years.

The General Assembly's mandate for this study directed JLARC "to review and evaluate the Virginia Information Technologies Agency (VITA) on a continuing basis and to make special studies and reports as may be requested." The mandate authorized JLARC to review (i) VITA's infrastructure outsourcing contracts; (ii) the adequacy of VITA's planning and oversight responsibilities, including VITA's oversight of the security of governmental information; and (iii) the adequacy of VITA's oversight of the procurement activities of state agencies (Appendix A). To address concerns identified during the course of ongoing oversight, JLARC staff proposed a review of the state's information technology (IT) governance structure in November 2013. The study was approved by the JLARC Chair and Vice-Chair.

This review examines how responsibilities should be vested with the Secretary of Technology, the Chief Information Officer (CIO), VITA, and state agencies. The distribution of these responsibilities has a direct impact on VITA's ability to perform its duties, including its ability to provide cost-effective services that meet agency needs. The distribution of responsibility also impacts the ability of agencies to carry out their operations.

Effective IT governance is essential to successful state operations

IT is essential to the daily operations of state government, and many agencies rely on IT to provide services to citizens. For example, approximately half of all of the Department of Motor Vehicle's customer transactions occur over the internet rather than in person at a DMV business center. Moreover, even those transactions

that occur at business centers cannot be completed without the support of IT systems. Agencies also rely on IT to support their internal administration, such as financial management and human resources.

Large organizations, including the state government, have complex governance structures that assign responsibilities for managing different aspects of their IT. By effectively managing IT, organizations can improve their operations and achieve organizational goals. For example, Virginia's Secretary of Health and Human Resources has set a strategic goal to improve health care quality, cost, and provider satisfaction. The secretary identified IT as a critical tool for achieving this goal, most notably by delivering new capabilities, such as electronic health records. Developing such new IT capabilities requires effective execution of responsibilities, including appropriate planning, investment management, and assessment of security needs.

Effective IT governance is also needed to ensure the continuity of state operations. A failure to properly execute responsibilities can lead to technological breakdowns that disrupt operations and services to citizens. In 2010, an incident at Virginia's main data center resulted in an IT outage that affected 26 agencies. For seven days, the affected agencies were unable to provide basic services, such as issuing driver's licenses and processing child support payments. An independent audit found that the contractor that operated the data center for the state did not follow key industry best practices for monitoring, testing, and managing its infrastructure. The audit noted that this deficiency represented "an insufficient degree of self-governance" by the contractor, which led to the delay in restoring operations.

Previous IT studies by JLARC

Review of Information Technology in Virginia State Government (1997)

Review of Information Technology Systems Development (2002)

Review of Information Technology Services in Virginia (2010)

All reports are available on the JLARC website.

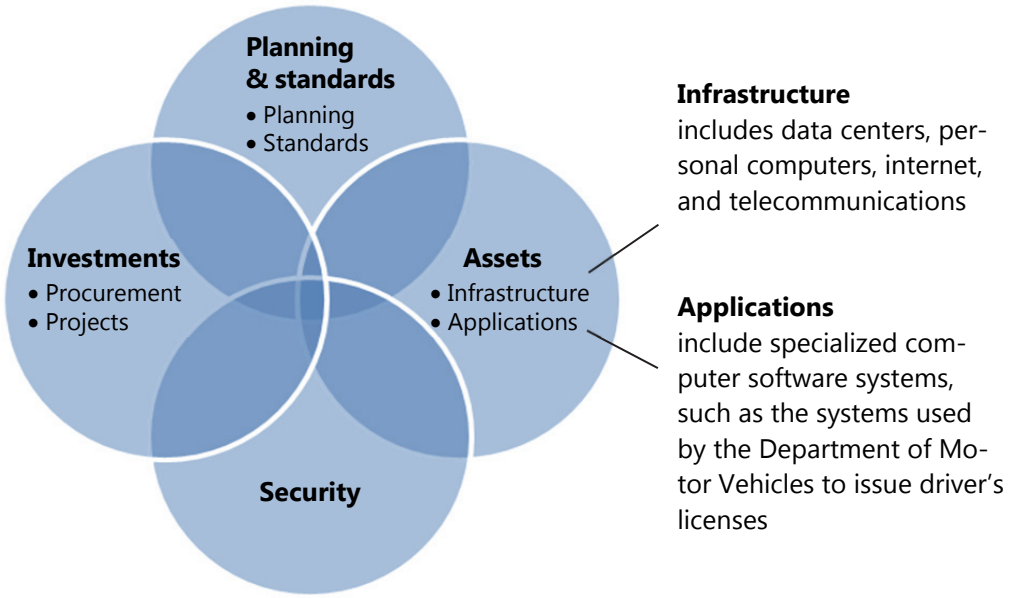
Ineffective IT governance can also lead to wasteful spending. In 2002, a JLARC study found that the state wasted at least $75 million on failed IT projects from 1991 to 2002 and incurred an additional $28 million in cost overruns. JLARC staff reported that some projects suffered from poor planning, such as a lack of formal project plans to guide them to completion. Others were poorly managed, including projects that were led by unqualified staff or lacked supervision by agency leadership. The report recommended a well-defined project management process to improve governance of IT projects.

Ineffective governance can increase the risk of data loss and theft. In 2012, tax data held by the South Carolina Department of Revenue was compromised when a security breach resulted in the theft of millions of citizen social security and bank account numbers. The breach occurred because the department did not have standard security measures in place to protect its data. South Carolina's inspector general attributed this failing to poor governance, finding that no state entity was responsible for developing and enforcing IT security standards.

IT responsibilities are divided between agencies and central authorities

Virginia's IT governance responsibilities are defined under statute and include responsibilities for planning and standards, managing assets, making investments, and ensuring security (Figure 1-1). Fulfilling responsibilities in one governance area has a direct impact on other areas. For example, planning decisions determine what investments are pursued. Investments lead to the development of new IT assets, which must in turn be secured.

FIGURE 1-1
Virginia's IT governance responsibilities



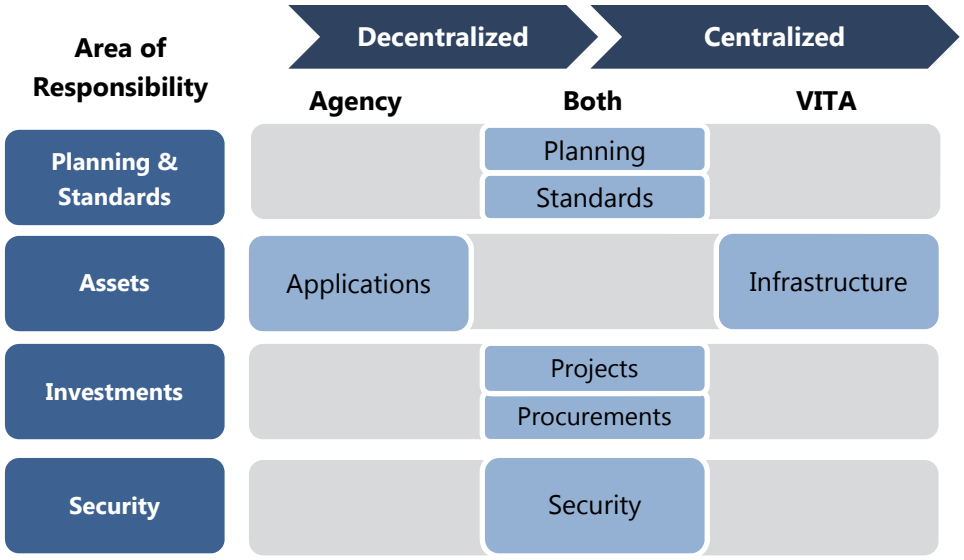
Source: JLARC staff analysis of IT governance models and the Code of Virginia.

IT governance responsibilities can be vested with a central state authority or decentralized to state agencies. Virginia has centralized some IT responsibilities, while others remain either partly or completely decentralized (Figure 1-2). Most notably, Virginia has centralized its infrastructure assets under VITA. Through a contract with Northrop Grumman, VITA provides executive branch agencies with data center services, personal computer and internet services, and other infrastructure services. Agencies maintain control over their specialized applications. For example, the Department of Motor Vehicles maintains control over the applications it uses to issue driver's licenses. Agencies are responsible for planning and carrying out their own investments and managing and securing their assets. These activities must be performed in accordance with VITA's standards, which means both parties have responsibilities for IT operations.

Northrop Grumman contract

Northrop Grumman provides IT infrastructure services to Virginia's executive branch agencies. The state's contract with Northrop Grumman was signed in 2005 and the term will expire in 2019.

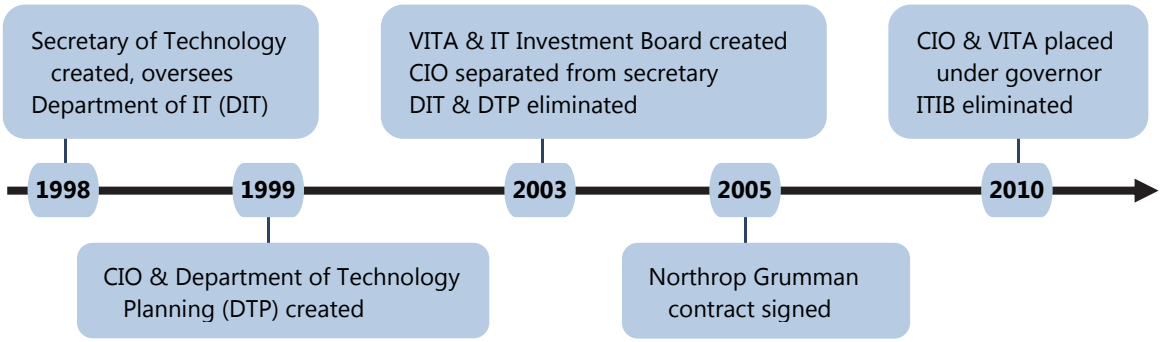
FIGURE 1-2
Virginia's IT governance structure



Source: JLARC staff analysis of the Code of Virginia.
Note: Figure depicts IT governance responsibilities for main executive branch agencies. Institutions of higher education, independent agencies, and agencies in other branches of government retain complete responsibility for their IT infrastructure. However, some are subject to IT standards and investment and security oversight.

Virginia has gradually increased centralization of IT over the past two decades (Figure 1-3). From 1998 to 2010, the General Assembly passed a series of reforms that shifted IT responsibility toward central authorities. In 1998 and 1999, the offices of the Secretary of Technology and the CIO were created to provide central IT leadership. In 2003, VITA was established as an independent agency charged with centralizing infrastructure assets, standardizing practices, and improving other areas of IT. In 2010, VITA ceased to be an independent agency and was placed under the authority of the governor. Virginia's movement towards centralization is reflective of the trends in other states and private corporations.

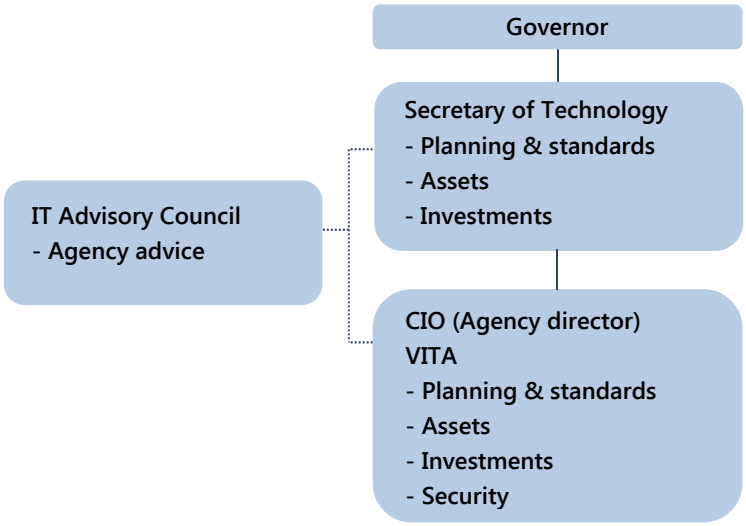
FIGURE 1-3
Evolution of Virginia's IT governance structure



Source: JLARC staff analysis of past JLARC reports and the Code of Virginia.

The state's central IT responsibilities are now concentrated with three parties: the Secretary of Technology, the CIO, and VITA. The secretary and CIO are the state's central IT leaders and VITA is the central IT agency. The CIO serves as the VITA agency director and reports to the secretary (Figure 1-4). Because the CIO is the head of VITA, duties assigned to VITA are essentially the responsibilities of the CIO and vice versa. The secretary and the CIO are separate positions with overlapping responsibilities.

FIGURE 1-4
Central IT reporting structure and responsibilities



Source: JLARC staff analysis of the Code of Virginia.

The Information Technology Advisory Council (ITAC) is the statutory body for fostering cooperation between the central IT authorities and agencies. ITAC is composed of agency appointees from each secretariat, plus two citizen members, and is tasked with advising the secretary and the CIO on all technology issues. ITAC has no formal role in central IT decisions.

Increased IT centralization has benefited the state but created governance challenges

Increased centralization of IT has provided Virginia with several benefits. Foremost, centralization has allowed the state to modernize and standardize its IT infrastructure. This has greatly improved the state's ability to manage and secure its assets. Additionally, centralization improved statewide planning and budgeting by providing greater transparency into the number, cost, and condition of the state's IT assets. Centralization resulted in consolidation of duplicative assets, such as data centers and email systems, that were independently operated by agencies.

Central oversight of agency projects appears to have reduced wasted spending on failed IT projects. Projects that have experienced trouble, such as delays, have been suspended until solutions were found or shut down if issues could not be resolved. Before VITA was created, some projects continued for years with unresolved problems, wasting millions of dollars.

Although centralization has provided benefits, it has not fully addressed several past governance concerns. A JLARC review conducted in 1997 recommended that the state establish a CIO to provide strong central leadership "in coordinating the information technology activities of state agencies and institutions." The office of the CIO was initially created to play this role, and VITA was created to further improve central authority. Still, a 2010 JLARC study found that agencies often did not comply with state standards or cooperate with central planning efforts. Challenges in coordinating agency IT activities appear to persist into the present.

Increased centralization led to divisions of responsibility between VITA and agencies, which has created new governance challenges. According to JLARC's 2010 report, agencies indicated that central infrastructure services provided by Northrop Grumman were costly and often did not meet their business needs. VITA indicated that agencies were sometimes reluctant to cooperate on infrastructure issues, such as consolidation of data centers. These concerns also appear to persist into the present, suggesting that VITA and agencies continue to have difficulty cooperating in areas of shared responsibility.

Potential weaknesses in Virginia's IT governance structure need to be identified and addressed promptly, because the state will soon make major decisions about its future IT environment. The state's contract for IT services with Northrop Grumman is set to expire in 2019. Between now and the end of the contract, the state must determine how it will meet its future IT infrastructure needs. Responsibilities

need to be clearly defined and appropriately assigned to ensure the best options are chosen.

Although management of the state's IT resources can be improved by changing the governance structure, the effectiveness of reforms will remain dependent on the actions of key stakeholders, including central IT authorities, state agencies, the governor, and the General Assembly. Historically, IT has been perceived as a support function and given mixed levels of priority. IT will need to be viewed by all parties as a high priority if efforts to improve governance are to succeed.

2 Separating Secretary and CIO Responsibilities

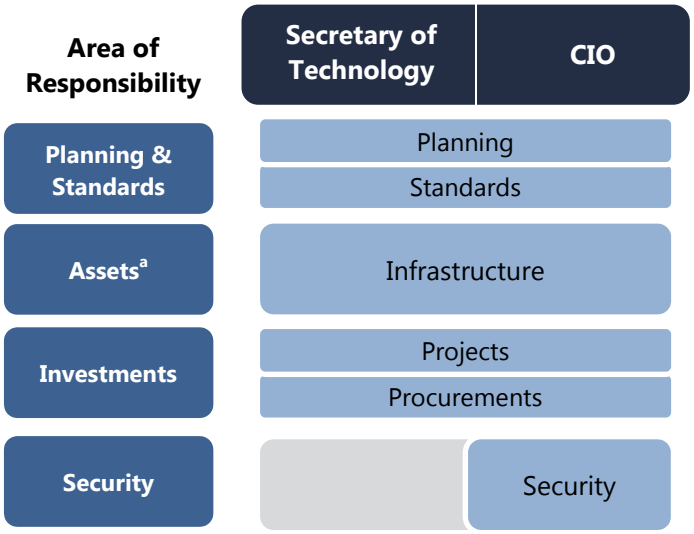
SUMMARY The state's central IT leaders, the Secretary of Technology and the CIO, have been assigned overlapping responsibilities under statute. The most notable overlap is that many of the decisions that are assigned to the CIO, such as approving contracts for statewide IT services, also require the explicit approval of the secretary. Requirements for secretarial approval can undermine the CIO's authority and do not appear to provide benefits. The secretary's approval authorities are not typical of those granted to cabinet secretaries in Virginia, and the secretary can adequately supervise the CIO and VITA without these authorities. The second area where the responsibilities of the secretary and the CIO overlap is coordinating the development of enterprise applications. This responsibility should be assigned to the secretary because it is consistent with the types of broad planning duties that are often assigned to secretaries. Eliminating the overlapping responsibilities of the secretary and CIO will improve IT governance by clarifying who is accountable for carrying out critical central functions.

Clear division of responsibility is important for good governance. In Virginia state government, the responsibilities of cabinet secretaries and agency directors are typically complementary. Secretaries are assigned high-level planning and supervision responsibilities, whereas agency directors are assigned operations and decision-making responsibilities. When the responsibilities of secretaries and agency directors overlap, it becomes uncertain who is accountable for decisions because neither party is clearly responsible for carrying out a given function.

The Secretary of Technology and the CIO are the state's central IT leaders. The secretary oversees the CIO, who manages VITA and is responsible for carrying out most central IT functions. However, many of the responsibilities that have been vested with the CIO under statute have also been vested with the secretary (Figure 2-1).

The secretary's and CIO's responsibilities overlap in almost all areas of central IT governance. Both parties are involved in making contract decisions that directly impact the state's IT infrastructure. Both parties play a role in planning to meet the state's IT needs, setting standards for agencies to follow, such as project management standards, and overseeing agency IT investments. Security is the one area where the responsibilities of the Secretary and CIO do not overlap.

FIGURE 2-1
Overlapping responsibilities of the secretary and CIO



Source: JLARC staff analysis of the Code of Virginia.
a Assets include both IT infrastructure and applications. Only infrastructure is shown here because the Secretary of Technology and the CIO are responsible for infrastructure but not applications. State agencies are responsible for applications.

CIO should be given full authority to carry out most central IT responsibilities

The secretary is statutorily responsible for approving specific operational decisions made by the CIO. This approval authority effectively gives the two parties overlapping responsibility for most areas of central IT. Most notably, the CIO's decisions related to statewide contracts, such as the state's contract for IT infrastructure services with Northrop Grumman, require approval by the secretary. The secretary also approves state IT standards and agency IT projects and procurements of over $1 million, but only after they have first been approved by the CIO.

Secretarial approval of statewide IT contracts can undermine the CIO's authority

The Code of Virginia gives the CIO the responsibility to negotiate contracts for statewide IT services but gives the secretary final approval over contract agreements. The secretary's approval authority can undermine the CIO's ability to negotiate with vendors. If vendors are not satisfied with the terms offered by the CIO, they can go around the CIO and negotiate directly with the secretary instead. Vendors may also decide to bypass the CIO altogether and deal exclusively with the secretary from the start.

JLARC staff identified two case studies that illustrate how the CIO's ability to negotiate and oversee contracts can be undermined due to a lack of clear authority. In the first case study, it appears that the state was negatively impacted by the exclusion of

the CIO. In the second case study, the CIO was initially excluded but ultimately brought in and negative repercussions were avoided.

CASE STUDY 1
CIO stopped from using penalties to improve Northrop Grumman performance

In February 2009, the CIO was considering financial penalties against the state's IT infrastructure contractor, Northrop Grumman, for inadequate performance. At the time, the CIO reported to the IT Investment Board, which had the supervisory role that is now vested with the Secretary of Technology. The CIO met with the board chair and one other member to discuss withholding payments to encourage better performance. After the meeting, the two board members began to meet privately with senior Northrop Grumman officials without the CIO's involvement. Following these meetings, the CIO was instructed not to withhold payment from Northrop Grumman. When the CIO pressed the issue a few months later, the CIO was removed from office.

In this instance, the CIO was excluded from critical discussions between senior state IT leaders and Northrop Grumman. This undermined the CIO's authority to negotiate with the contractor and prevented the CIO from using financial penalties to improve the contractor's performance.

CASE STUDY 2
CIO initially excluded from restitution negotiations with Northrop Grumman

In August 2010, an IT outage shut down operations at 26 state government agencies for seven days. An independent audit of the incident found that problems with Northrop Grumman's management practices contributed to the prolonged outage. Accordingly, the state decided to seek restitution for financial damages from Northrop Grumman.

Although the CIO was responsible for managing the contract with Northrop Grumman, the CIO indicated that restitution negotiations were initially conducted by the Secretary of Technology without CIO involvement. The CIO indicated that he was asked by the secretary to review settlement proposals that the secretary had negotiated without CIO participation. The CIO indicated he had significant concerns about a key concession contained in the agreement with Northrop Grumman and concluded that he should not sign it.

The CIO stated that following consultation with the Office of the Attorney General, direct negotiations were eventually handed over to the CIO. Northrop Grumman ultimately agreed to pay Virginia $5 million in restitution.

State IT investments: reviewed by VITA and approved by CIO and secretary

Agency IT investments include projects and procurements, including related solicitations, contracts, and contract amendments. Investments are reviewed by VITA staff to determine whether they should be allowed to move forward. Large agency investments must be approved by the CIO. Investments of over $1 million must also be approved by the Secretary of Technology.

The CIO is the party responsible for the day-to-day administration of contracts for statewide IT services, and therefore has the best understanding of statewide needs. The CIO also manages VITA staff with technical knowledge about the IT services that are provided under the contracts. For these reasons, the CIO should be given full authority for negotiating and approving contracts for statewide IT services. This would be consistent with past JLARC reports, which emphasized the importance of establishing clear lines of accountability for central IT decisions.

Secretarial approval authority over other CIO actions does not appear to provide benefits

The Secretary of Technology has several other responsibilities that overlap with those of the CIO. These include the responsibility to:

- approve state agency IT projects and procurements valued at over $1 million, including related contracts and amendments;
- make additional decisions for major IT projects, including designating oversight committees and deciding whether a project should be terminated;
- approve IT standards, including technical standards;
- develop data standards; and
- develop criteria for what constitutes a major project under the state's IT project management standards.

Secretary's approval and other direct authorities over state agency IT investments do not appear to add benefits

The secretary's approval and additional decision-making authorities for major agency IT projects and procurements appear to add limited value. The CIO and VITA's project management division review all major projects and procurements before they are presented to the secretary for approval. The CIO and VITA staff also monitor the progress of these investments as they move towards completion, and they have the technical expertise needed to identify and help resolve potential problems. The secretary relies on the CIO and VITA staff to provide information and answer questions about the investments, meaning that the secretary's review does not add a layer of independent oversight. The added approval layer can introduce delay if the secretary is unable to review a proposed investment in a timely manner. VITA staff indicated that in the previous administration some secretarial approvals were delayed by up to two weeks.

The secretary's approval and additional decision-making authorities also raise a possible conflict of duties with the secretary's role in promoting the state's private IT sector. In the latter capacity, the secretary is charged with helping attract and grow technology businesses in Virginia. Some of these businesses may bid for contracts

offered by state agencies. The secretary could potentially use the authority to approve agency investments to direct agencies toward these businesses even if they do not offer the best value. Although the structure creates the potential for conflict, it is important to note that JLARC staff did not find any instances of malfeasance.

Secretarial authority to approve and develop IT standards does not appear to add benefits

According to the Secretary of Technology, the secretary's office provides the strategic perspective needed to shape the state's high-level IT policies and initiatives. However, the secretary's approval authority over state IT standards is at the operational level, and the secretary's involvement in these approvals does not appear to provide benefits.

VITA's IT standards are the "rules" that agencies must follow for acquiring and managing their IT assets, and many standards are highly technical. VITA staff have the technical understanding that is needed to develop standards that meet overarching goals, such as which protections are needed to ensure that personal computers are adequately secured. VITA staff develop standards, the CIO approves them, and the secretary provides final approval. Because of the impact on state operations, VITA solicits the input of agencies on proposed standards before they are published. The agency viewpoint is crucial because it can provide feedback on how standards will affect agency IT and business operations. In contrast, the added layer of secretarial approval does not appear to add a broader perspective to reviews because, like the CIO, the secretary represents the central IT viewpoint.

IT standards

VITA is charged with developing "policies, standards, and guidelines" defining how IT assets are managed, investments are made, and security is ensured. This report uses the term "standards" to refer to all of the above. IT standards include rules that agencies must follow, requirements for the types of technology they use, and standards for how data is stored, transmitted, and protected.

The secretary's responsibilities for developing data standards and project management criteria appear misplaced because VITA has the technical expertise and staff resources needed to carry out these duties. The secretary is required to develop data standards for information commonly used by state agencies and a plan for implementing them. In practice, VITA staff professionals, who are trained in the design of IT systems, developed the state's plan for standardizing data and are leading the effort to implement new standards. The secretary is also required to develop criteria defining major IT projects. In practice, this requirement was fulfilled by VITA's project management professionals, who developed the criteria as part of a general revision of the state's IT project management standards.

Secretary's authority to approve specific CIO actions is not typical and appears redundant with general secretarial powers

The Secretary of Technology's responsibilities for approving specific CIO decisions are not typical of the powers vested with other secretaries. Under the Code of Virginia, secretaries are generally responsible for supervising the agencies within their secretariat and planning their strategic direction (§ 2.2-200). Several secretaries are also given duties for coordinating programs or policy initiatives that involve the agencies within their secretariats, such as the Secretary of Administration's responsibility to establish

TABLE 2-1
Responsibilities of Virginia cabinet secretaries

	Type of responsibility				
Secretary	**Supervise & coordinate agencies**	**Set strategic direction**	**Implement program & planning initiatives**	**Monitor specific agency actions**	**Approve specific agency actions**
Technology	✓	✓	✓	✓	✓
Public Safety & Homeland Security	✓	✓	✓	✓	
Veterans and Defense Affairs	✓	✓	✓	✓	
Administration	✓	✓	✓		
Health and Human Resources	✓	✓	✓		
Natural Resources	✓	✓	✓		
Commerce and Trade	✓	✓			
Education	✓	✓			
Agriculture and Forestry	✓	✓			
Finance	✓	✓			

Source: JLARC staff analysis of the Code of Virginia.
Note: The Secretary of the Commonwealth is not listed because that office does not have the same general powers and authorities of the other secretaries and does not directly oversee state agencies.

a statewide telecommuting policy. Three secretaries are charged with monitoring specific actions taken by their agencies but are not charged with approving agency actions. For example, the Secretary of Veterans and Defense Affairs is responsible for monitoring agency efforts to provide services to veterans but not for approving how agencies decide to provide those services. Only the Secretary of Technology appears to have explicit responsibilities for approving specific decisions made by an agency director (Table 2-1).

The Secretary of Technology's unusual approval authorities were transferred from the IT Investment Board. This board had been charged with closely supervising VITA and the CIO, and it had many managerial responsibilities. When the board was eliminated in 2010, VITA and the CIO were moved under the secretary. Several of the board's managerial responsibilities were also transferred to the secretary, even though they were not typical of a cabinet secretary's duties.

The specific approval authorities vested with the Secretary of Technology are not necessary for effective supervision. The general powers granted to secretaries already include the authority to hold agency directors accountable for their actions and the performance of their duties. These general powers allow secretaries to review major decisions and acquire all manner of information from agency directors. For example,

the Secretary of Administration does not have a statutory responsibility to approve employee health insurance contracts signed by the Department of Human Resources Management or statewide contracts signed by the Department of General Services, but can use supervisory powers to review and provide input on proposed agreements. The Secretary of Technology could similarly use the general powers of the office to gather and review information on items of interest such as proposed contracts for statewide IT services.

Agency directors, including the CIO, are generally charged with directing the operations of state government (§§ 2.2-601 through 2.2-604). The CIO is also tasked by the Code with fulfilling central IT oversight responsibilities as well as managing VITA and the services it provides to state agencies. To fulfill these responsibilities most effectively, the CIO needs the authority to make final decisions on operational matters. This includes final approval of VITA's contracts for statewide IT services, agency IT projects and procurements, and IT standards. As the head of VITA, the CIO has the staff and resources that are needed to make decisions in each of these areas.

RECOMMENDATION 1

The General Assembly may wish to consider amending the Code of Virginia and the Appropriation Act to remove requirements that the Secretary of Technology approve specific operational decisions made by the CIO, including (1) approving VITA contracts and amendments for statewide IT services, (2) approving and making other decisions related to agency IT projects and procurements, and (3) approving and developing state IT standards.

Secretary should coordinate development of enterprise applications

Under the state's partially centralized IT structure, state agencies maintain control over applications, including enterprise applications. Enterprise applications are IT software systems that are used across state agencies to manage central administrative functions. These include applications for financial, procurement, and human resources management. For example, Virginia's Commonwealth Accounting and Reporting System (CARS) is the application that state agencies use to record and report financial transactions. Although agencies maintain control over enterprise applications, both the Secretary of Technology and the CIO have been vested with responsibility for coordinating agency efforts to modernize these applications as part of their general responsibility for overseeing enterprise IT efforts.

Modernizing enterprise applications requires coordinating with state agencies

Development of Cardinal

The development of Cardinal, the state's new enterprise accounting application, has involved three types of partners.

The Department of Accounts (DOA) is a lead agency. Other state agencies are customers. The Department of Transportation (VDOT) is a third type of partner: a development agency.

The development agency (VDOT) built a financial management system that has been modified by the lead agency (DOA) to create Cardinal. Customers (state agencies) will begin using Cardinal in late 2014.

The state relies on an incomplete and partly outdated patchwork of enterprise applications to support its central administrative functions (Table 2-2). These applications have been built and maintained by individual lead agencies, and some applications are over 30 years old. For these reasons, the applications are not able to easily share information across systems and agencies. This creates challenges in managing and reporting on the state's operations at the enterprise level.

Funding has not been provided for a major modernization of enterprise applications, so they are instead being upgraded incrementally. This approach requires the state to decide which specific applications should be modernized first and how projects will be funded. It also requires careful coordination between the lead agencies that "own" the applications and the customer agencies that use them. For example, the Department of Accounts is leading the effort to replace CARS, the state's central accounting system, with a new system called Cardinal. This task requires careful coordination with all state agencies.

The state's previous efforts to develop enterprise applications on an incremental basis have been hindered by a lack of cooperation among agencies. For example, the Departments of General Services and Transportation have had challenges reaching

TABLE 2-2
Virginia's enterprise applications

Enterprise application	Function	Lead agency
Financial		
Commonwealth Accounting and Reporting System (CARS)[a]	Accounting	Accounts
Commonwealth Integrated Payroll/ Personnel System (CIPPS)	Payroll	Accounts
Performance Budgeting System	Budgeting	Planning & Budget
Procurement		
Virginia eProcurement Portal (eVA)	Procurement	General Services
Human resources		
Personnel Management and Information System (PMIS)	Employee records	Human Resources
Time, Attendance & Leave (TAL)	Timekeeping	Human Resources

Source: JLARC staff analysis of agency websites and system documentation.

[a] Virginia is in process of replacing CARS with a new enterprise application called Cardinal.

agreement on whether changes are needed to the state's enterprise application for procurement.

Secretary is best positioned to coordinate the development of enterprise applications

The Secretary of Technology and the CIO have overlapping responsibility for coordinating the development of enterprise applications. Of the two IT leaders, the secretary appears best positioned to fulfill this responsibility because secretarial intervention may be necessary to resolve inter-agency conflict. For example, the Secretaries of Administration and Transportation are working to resolve the dispute between the Departments of General Services and Transportation about changes to the state's enterprise procurement application. The Secretary of Technology is a peer to these secretaries and is therefore best positioned to represent central IT leadership in discussions.

Vesting the secretary with responsibility for coordinating the development of enterprise applications would not diminish the ability of the CIO to carry out his duties. Enterprise applications are developed by a lead agency, not by the CIO or VITA. Agencies are responsible for developing applications, which are used to carry out agency business processes, such as financial reporting, and must be tailored to meet specific operational needs. The CIO's role has been to have VITA provide infrastructure, such as the servers that support applications, and monitor related projects and procurements to ensure they comply with state standards. The CIO can continue to perform this role even if the secretary is responsible for coordinating with agencies.

Giving the Secretary of Technology authority to coordinate the development of enterprise applications would be consistent with the authority that is granted to other secretaries. In Virginia, cabinet secretaries are generally responsible for planning and coordinating agency activities within their areas of responsibility (§ 2.2-200).

Although the secretary should coordinate efforts to modernize enterprise applications, several related responsibilities should remain with the CIO. Projects to develop enterprise applications should remain subject to the state's project management process, which is overseen by the CIO. Further, enterprise IT efforts other than enterprise applications should rest with the CIO, as head of the state's central IT agency. These include projects to foster data sharing and other initiatives where it is reasonable for VITA to serve as the lead agency or oversee other agencies' efforts.

RECOMMENDATION 2

The General Assembly may wish to consider amending § 2.2-225 and § 2.2-2007 of the Code of Virginia to reassign the CIO's responsibilities for coordinating the development of central administrative enterprise applications to the Secretary of Technology.

State's contract for development of enterprise applications should be managed like other statewide IT contracts

Recent APA report recommended terminating CGI contract

A 2013 report by the Auditor of Public Accounts found that the CGI contract no longer serves its original purpose and the state should consider terminating it or allowing it to expire. The report noted that the contract can be used for consulting services that could instead be competitively procured under a state contract.

The state has a master services agreement with a private company, CGI Technologies and Solutions Inc., for enterprise applications development services. This contract was signed in 2006 under a public-private partnership agreement. The contract has not yet been used to develop new enterprise applications, but it remains available for use by state agencies. The contract is currently managed by the governor's office.

State agencies that are leading the development of enterprise applications could continue to be allowed to use the CGI contract, but it should be placed under the supervision of the CIO. The CGI contract can currently be used to acquire IT services without following the standard procurement process that is overseen by VITA. This allows agencies to procure goods or services that may not comply with the state's IT standards. For example, because VITA does not approve procurements made under the contract, agencies could potentially use contract services to develop a new application that does not conform to the state's IT security standards, placing agency operations at risk. The contract could also be used by agencies to hire temporary contractors to increase their IT staff, undermining the state's efforts to monitor the use of contract labor. Moving the CGI contract under the CIO's authority would help ensure compliance with state requirements.

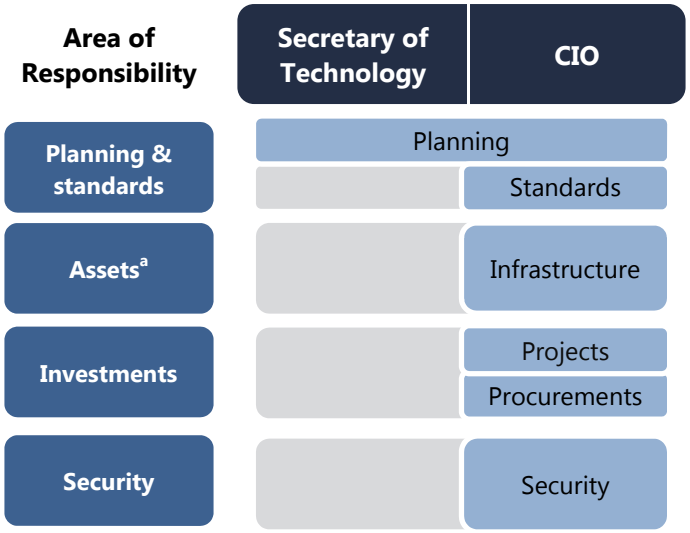
RECOMMENDATION 3

The General Assembly may wish to consider amending the Appropriation Act to require that the CIO approve contractual agreements between agencies and CGI Technologies and Solutions, Inc.

Proposed realignment clearly separates secretary and CIO responsibilities

The changes proposed in this chapter would realign the central IT responsibilities vested with the Secretary of Technology and the CIO (Figure 2-2). The secretary's specific approval authorities related to statewide IT contracts for infrastructure and other services, agency projects and procurements, and IT standards would be removed so that the CIO is vested with full responsibility for these areas. The CIO would continue to maintain responsibility for security. The CIO and secretary would both continue to have planning responsibilities, but responsibility for coordinating the development of enterprise applications would be moved to the secretary in order to minimize overlap within this area. The secretary would retain general supervisory authority and the strategic policy and planning responsibilities that are vested with the office.

FIGURE 2-2
Proposed realignment of central IT responsibilities



Source: JLARC staff analysis of proposed changes.

[a] Assets include both IT infrastructure and applications. Only infrastructure is shown here because the Secretary of Technology and the CIO are responsible for infrastructure but not applications. State agencies are responsible for applications.

3 Improving Central IT Leadership

SUMMARY The effectiveness of central IT leadership could be improved by providing additional support to the CIO. Under the current leadership structure, the CIO reports to the governor through the Secretary of Technology. This reporting structure insulates the CIO from political influence but risks disrupting the line of communication between the CIO and the executive leadership. The CIO appears to have had few regular interactions with the governor or cabinet members, even though their support is critical for the success of statewide IT initiatives. To resolve this issue, the secretary's role as an advocate for state IT issues should be formalized, and procedures should be established to ensure the CIO is able to regularly discuss major IT issues with the governor and cabinet. Within VITA, the CIO's dual responsibilities as central IT leader and agency director create a potential for conflict between oversight and service provider duties. The wide range of responsibilities also place demands on the CIO's time. The appointment of a Deputy CIO would free the CIO to focus on the leadership role and improve internal separation between oversight and services.

The division of responsibility between the Secretary of Technology and the CIO gives Virginia two IT leaders at different levels of the executive branch. The secretary serves as the leader for IT issues in the governor's cabinet, directing implementation of broad technology initiatives and supervising IT agencies. In this capacity, the secretary is positioned to raise state IT issues with Virginia's executive leadership. The CIO serves a dual role as (1) central leader charged with oversight of state IT and (2) the VITA agency director charged with providing IT services to state agencies. In these capacities, the CIO has a better understanding of state IT issues that need to be communicated to the executive leadership.

IT governance is most effective when both the secretary and CIO directly discuss issues with executive leadership

IT is critical to state operations, and major issues need to be discussed with the state's executive leadership. Effective communication is especially critical for gaining support of the governor and cabinet secretaries for statewide initiatives that require agency cooperation. Communication with the executive leadership will be especially important in the near future. The state's contract with Northrop Grumman for IT infrastructure services will expire in 2019, and the state will need to

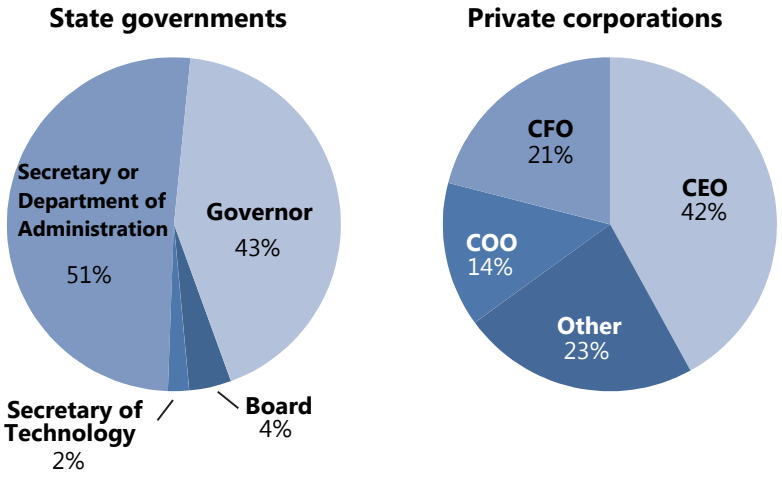
determine how its future needs will be met. The CIO will need to discuss the options for change with the governor and other state leaders.

Most organizations do not have two IT leaders, but having a CIO at the agency level is common

Virginia's current central IT reporting structure has the CIO report to the Secretary of Technology, who then reports to the governor. This arrangement is unusual because it creates two central IT leaders, with one leader reporting to another. Other states have either a CIO or a Secretary of Technology but not both.

Although it is unusual to have two central IT leaders, it is not unusual to have a CIO report to a subordinate of the chief executive. JLARC staff estimate that about half (51 percent) of state CIOs currently report to an administrative subordinate of the governor, such as a secretary of administration or equivalent position (Figure 3-1). A 2012 survey conducted by Gartner, a leading IT research consultant, found similar results in the private sector. More than half of companies (58 percent) indicated that the CIO reports to another corporate officer, typically a chief financial or operating officer, instead of the chief executive officer.

FIGURE 3-1
Slight majority of CIOs report to a subordinate of the chief executive



Source: JLARC staff analysis of other state websites and NASCIO and Gartner surveys.

Current reporting structure insulates CIO from political influence but can obstruct communications

Virginia's current CIO reporting structure, which places the CIO at the agency level rather than the cabinet level, mitigates risks that have been identified in past JLARC reports. Foremost, locating the CIO outside the cabinet makes the position less subject to political influence because it adds a layer of separation between the policy priorities of the cabinet and the operational goals of the CIO. A 2002 JLARC report concluded

that the offices of the Secretary of Technology and the CIO should be separated, among other reasons, to avoid the risk of political influence. The report noted that "The CIO position needs to be protected from external influence so that decisions are based on technological and business needs rather than external considerations."

Having the CIO as an agency director also likely reduces turnover at the position. As an agency director, the CIO serves at the will of the governor, but turnover among Virginia's agency directors is generally lower than for secretaries. The National Association of State CIOs indicated that the tenures of other state CIOs are generally short because of high turnover among cabinet-level CIOs when the governor changes. Ensuring the stability of the CIO position was a point of emphasis in the 2002 JLARC report.

Having the CIO report to the Secretary of Technology instead of the Secretary of Administration may be beneficial because it gives IT matters a higher profile in the governor's cabinet. The Secretary of Technology is focused on IT issues and may therefore be better positioned to understand, support, and communicate technology issues than the Secretary of Administration.

Although the state's IT structure mitigates the risk of political influence and turnover, it creates a risk that the CIO will not be able to effectively confer with the governor and cabinet secretaries. Communication problems can occur if the Secretary of Technology does not include the CIO in high-level discussions or relay issues identified by the CIO to the executive leadership.

JLARC staff did not find any instances where the secretary refused to communicate issues raised by the CIO, but the secretary's responsibility to support and communicate state IT issues is not clearly established under the Code of Virginia. This stands in contrast to the secretary's responsibilities for promoting private sector IT issues, which are clearly established under statute. This should be balanced by placing a similar emphasis on secretary's role in communicating state IT issues.

Examples of state IT issues

State IT issues that may need to be dis-cussed with executive leadership include:

- Changes to the state's model for providing central IT services
- Statewide IT initiatives requiring agency cooperation, such as efforts to establish data standards
- Major IT investments needed by the state or specific agencies, such as replacement of outdated applications
- Problems with agencies not complying with security, asset management, and other requirements.

Discussion of IT issues between the CIO and executive leadership should be improved

The support of the governor and cabinet secretaries is critical to ensuring the success of statewide IT initiatives, but Virginia's CIO does not appear to have regular interaction with these executive leaders. As of July 2014, the CIO indicated he has met with the current governor and chief of staff only once and has not participated in any meetings with the cabinet secretaries. The CIO indicated that he also had limited interaction with the prior governor and administration. The Secretary of Technology regularly meets with the executive leadership but does not have the CIO's detailed understanding of state IT issues.

CIOs in other states indicated that they have regular discussions with their executive leadership even if they do not report directly to the governor's office. The CIO of Pennsylvania, who is an agency director like Virginia's CIO, indicated that he has quarterly meetings with that state's cabinet to brief them on IT issues. The CIOs of

three other states interviewed by JLARC staff also indicated they regularly confer with their governor's office and cabinet members.

Private sector IT professionals also emphasized the importance of clear communication between the CIO and the chief executive. According to research performed by Gartner, it is vitally important that the CIO regularly interact with the chief executive, especially in discussing business decisions that will ultimately be supported by IT solutions. The frequency and quality of interactions between the CIO and senior executives appears to be more important than a direct reporting line.

The apparent lack of interaction between Virginia's CIO and executive leadership may limit effective communication of critical state IT issues and should be addressed. First, the Secretary of Technology's intended role as an advocate for state IT issues in the cabinet should be emphasized by clearly establishing this as a statutory responsibility. This type of leadership responsibility is consistent with the high-level responsibilities that are generally assigned to Virginia's cabinet secretaries. Second, the governor's office, the secretary, and CIO should develop procedures for discussing state IT issues with the governor and the cabinet. These procedures should ensure CIO involvement in critical decisions. For example, the procedure could stipulate CIO participation in designated cabinet meetings or require CIO participation in meetings with the governor's office or cabinet where state IT issues are to be discussed.

RECOMMENDATION 4

The General Assembly may wish to consider amending § 2.2-225 of the Code of Virginia to vest the Secretary of Technology with responsibility for communicating state IT issues to the governor and members of the cabinet.

RECOMMENDATION 5

The governor's office, Secretary of Technology, and the CIO should develop and implement procedures for regular discussion of critical state IT issues with the governor and the cabinet. Procedures should ensure that the CIO has the opportunity to directly confer with the governor or governor's staff and other cabinet members about these issues.

CIO needs assistance to fulfill dual role as central IT leader and agency director

The CIO has dual responsibilities to serve as a central IT leader and the VITA agency director. In the capacity of central IT leader, the CIO is responsible for overseeing all state IT. In this role, the CIO sets the standards governing the management of IT assets, investments, and security, and monitors agencies to ensure standards are being followed. In the capacity of agency director, the CIO is responsible for VITA and the services it provides to state agencies. Through this role, the CIO manages the delivery of IT infrastructure services under the contract with Northrop Grumman.

The CIO's responsibilities for managing VITA services are time consuming and may limit the CIO's ability to perform oversight responsibilities. The current CIO indicated that he is not able to meet regularly with other agency directors about statewide initiatives, such as efforts to improve the security of IT assets. In contrast, the current CIO of Pennsylvania indicated that direct discussions with agency directors is one of his primary work activities. Preparing for the end of the Northrop Grumman contract in 2019 will create additional demands on the Virginia CIO, further constraining the ability of the CIO to fulfill oversight and service roles.

The CIO's dual role creates a potential conflict of duties, because the CIO could use oversight authorities to benefit VITA's service operations. It is important to note that JLARC staff have not found any indication that the CIO or VITA staff have acted in a self-interested manner. However, JLARC's 2010 report found that the perception of a conflict undermined VITA's ability to oversee agencies. For example, several agencies identified instances where they were required to use VITA services instead of lower-cost alternatives provided by a third party. Agencies indicated VITA appeared to be acting in its own interest to maintain customers, instead of acting in the interest of the state and allowing agencies to use less costly services. The perception of VITA's objectivity appears to have improved since the 2010 report was completed, but some agencies continued to raise this concern.

It is not unusual for agency directors to be assigned dual roles, but they are often assisted by deputies who oversee major operations. DGS is similar to VITA in that it has both oversight and service provider responsibilities. For example, DGS sets standards that agencies must follow for facilities management, non-IT procurements, and the acquisition, leasing, and disposal of vehicles and other property. DGS also provides agencies with services in each of these areas. The DGS director is assisted by a deputy director, who oversees several major areas of operations, including central procurements, vehicle fleet management, and the surplus property disposal program.

VITA should follow the example of other agencies and establish a classified deputy CIO position. The Deputy CIO should be second-in-command to the CIO and should be charged with assisting the CIO in the fulfillment of his duties. These should include helping the CIO manage VITA services and assisting the CIO in planning for the end of the Northrop Grumman contract. This additional leadership support would reduce the risk posed by VITA's conflicting duties, although it would not eliminate it entirely. This would also allow the CIO to commit more time and attention to central leadership responsibilities, such as conferring with the executive leadership and agency directors.

RECOMMENDATION 6

VITA should establish and the Secretary of Technology should approve a classified position of Deputy CIO to assist the CIO in the fulfillment of the CIO's duties, including managing VITA services and assisting in planning for the end of the Northrop Grumman contract.

4 Clarifying VITA's Statutory Responsibilities

SUMMARY VITA's main responsibilities need to be more clearly defined in order for VITA to effectively fulfill its role as the state's central IT agency. Most of VITA's responsibilities for managing and overseeing the state's IT environment, including its responsibility to centralize the state's infrastructure, are not clearly or concisely presented in the Code of Virginia. This makes it difficult to discern the limits of VITA's responsibilities and the enforcement mechanisms at its disposal. In the critical security area, VITA and agencies have effectively cooperated on a few targeted efforts to improve the security of state data, but cooperation in other areas is lacking. Cooperation could be improved by clearly assigning agencies with responsibility for securing state data and clarifying requirements for agencies to comply with the state's IT security and risk management program. In the procurement area, agency compliance with central IT procurement requirements has also improved in recent years. However, violations can create security risks and support challenges, and procurement requirements could be clarified to improve compliance.

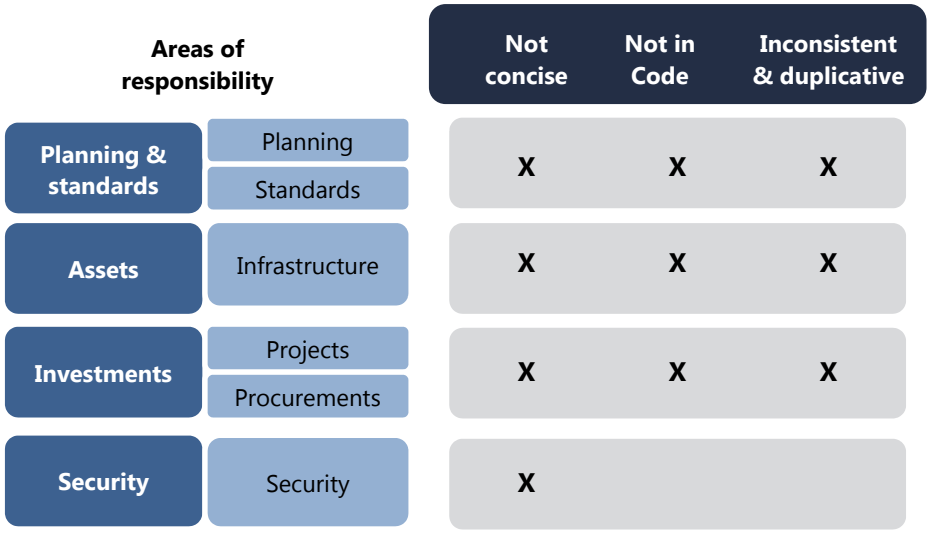
As the state's central IT agency, VITA oversees and provides services to other executive branch agencies. VITA's responsibilities need to be clearly defined so it can effectively carry out its role and ensure that agencies comply with state IT standards, including the requirement to use VITA's infrastructure services. Clearly defined responsibilities are especially important for VITA because it often must rely on its statutory powers to compel agency compliance. Lack of compliance with IT standards undermines the centralized structure the state has worked to achieve.

VITA's main responsibilities are not clearly defined

When VITA was created, many of its main responsibilities were established in the Acts of Assembly and the Appropriation Act instead of the Code of Virginia. This makes it difficult to determine the scope of VITA's duties. VITA also inherited several responsibilities from predecessors, such as the Department of Information Technology. The older responsibilities were not reconciled with VITA's newer ones, resulting in inconsistent and duplicative statutes (Figure 4-1).

Most notably, VITA's authority to control the state's IT infrastructure assets is not codified, even though this was the main reason VITA was created. The requirement that VITA centralize and manage the state's IT infrastructure is established only in the enactment clauses of the Acts of Assembly that created VITA. These uncodified clauses are also the only law defining which agencies are required to use VITA's infrastructure

FIGURE 4-1
VITA's main responsibilities are not clearly defined



Source: JLARC staff analysis of the Code of Virginia, Appropriation Act (2014), HB1926 (2003), and SB1247 (2003).

services. Because the enactment clauses do not appear in the Code of Virginia, the extent of VITA's authority over IT infrastructure is not readily apparent under statute.

VITA's responsibility for overseeing agency IT investments is not clearly and concisely defined. VITA's central procurement authority is described in the Code, the Acts of Assembly, and the Appropriation Act. Each provides a different definition of VITA's procurement authority. For example, the Code appears to give VITA procurement authority over all executive branch entities, whereas the Appropriation Act and enactment clauses in the Acts of Assembly appear to exempt institutions of higher education. It is therefore not readily apparent which state entities VITA is responsible for overseeing.

References to VITA's investment oversight responsibilities for agency IT projects are dispersed throughout the Code of Virginia—31 responsibilities defined in 10 different sections—and several are duplicative. For example, the CIO's role in approving IT projects is defined in three ways in three different sections of statute. This inconsistency and duplication makes it difficult to determine the scope of VITA's responsibilities for project oversight.

VITA's responsibilities for developing IT standards are also duplicative. VITA has 27 standard-setting responsibilities defined in six different sections of the Code. It is twice given broad responsibility for setting statewide IT standards. Despite this broad authority, it is also given responsibilities for setting standards in specific areas, including project oversight (7 instances), procurement (4 instances), and general operation and maintenance of IT assets (3 instances). As with VITA's

Virginia laws

Laws passed by the General Assembly are set forth in: (1) the Code of Virginia, (3) the Appropriation Act, and (3) the uncodified Acts of Assembly. The Appropriation Act supersedes the Code of Virginia to the extent that there is any conflict. The uncodified Acts of Assembly remain law unless they are superseded by newer legislation.

project oversight, this duplication results in inconsistencies that make it difficult to determine the scope of VITA's responsibilities.

Several of VITA's responsibilities in each area are difficult to understand because they are not clearly and concisely defined. For example, VITA is responsible for approving "all agreements and contracts for communications services prior to execution." This initially appears to give VITA responsibility only for approving the procurement of telephone and cellular services. However, a separate section of the Code defines "communications services" as a broad array of IT infrastructure services including telephone and cellular services as well as data center and internet services. VITA therefore has the authority to approve a much wider range of contracts than the term "communications services" suggests, but determining the scope of its authority requires a detailed understanding of the Code. Several other sections of VITA's governing statutes are equally complicated and difficult to interpret.

The lack of clearly established statutory authority may limit VITA's ability to carry out its oversight and service provider responsibilities. Three state agencies, Virginia State Police, Department of Emergency Management, and the Virginia Employment Commission, do not fully participate in the state's central IT services model. This creates security risks because VITA cannot as effectively monitor the IT infrastructure used by these agencies. It creates management challenges and added costs because these agencies continue to use computers and other equipment that are not supported under the state's contract with Northrop Grumman. VITA staff indicated that they have been unable to compel agency participation, due in part to the vague nature of VITA's statutory responsibilities. Clarifying that agencies must comply with VITA oversight requirements and use its central IT services could encourage further cooperation in this and other areas.

To maximize the effectiveness of Virginia's IT operations, the VITA statutes should be amended so that VITA's responsibilities are clearly identified. Statute should identify each area of central responsibility, VITA's powers and authorities under each area, and the state entities that are subject to VITA's authority. This legislation should be developed by a technical working group, led by the Division of Legislative Services in partnership with key stakeholders. The working group should limit its efforts to clarifying existing VITA statutes. In the event that a policy decision is needed, such as how to resolve two conflicting responsibilities, the working group should bring the issue to the attention of the legislature. The final legislation proposed by the working group should be presented to the Joint Legislative Audit and Review Commission. Legislation should be presented by November 2015 so that it may be considered for the 2016 General Assembly session.

RECOMMENDATION 7

The General Assembly may wish to consider amending the Appropriation Act to direct the formation of a technical working group, led by the Division of Legislative Services and including staff of JLARC, the Joint Commission on Technology and Science, the Office of the Secretary of Technology, VITA, and the Office of the Attorney General, to develop legislation that reorganizes, clarifies, and codifies VITA's existing responsibilities, including those established in enactment clauses and the Appropriation Act. Legislation should be presented to the Joint Legislative Audit and Review Commission by November 2015 so that it may be considered for the 2016 General Assembly session.

RECOMMENDATION 8

The General Assembly may wish to consider amending the Code of Virginia to adopt the legislative changes developed by the technical working group for reorganizing, clarifying, and codifying VITA's existing responsibilities.

Responsibility for securing the state's data is not clearly assigned in statute

Securing the state's data is one of the most critical IT governance responsibilities. The state's IT systems hold highly sensitive personal information about its citizens that it is obligated to protect, including social security numbers, financial account information, and health records. Other state data is not sensitive to citizens but is critical to the daily operations of agencies, such as roadway inventories used by the Virginia Department of Transportation to inform its maintenance operations. This data also needs to be protected from theft, loss, misuse, and unauthorized access.

Two-factor authentication

In order to access a secure IT system, employees must typically enter a password to authenticate their identities. Under a two-factor authentication approach, the employee must enter a second piece of information in addition to the password. A common approach is to provide employees with a device or computer program that generates a random number that the employee must type in to verify their credentials.

Failure to properly secure data violates the trust between government and its citizens and can have serious financial implications. In 2012, tax data held by the South Carolina Department of Revenue was compromised in a security breach. The breach resulted in the theft of 3.8 million social security numbers and 3.3 million bank account numbers. South Carolina has paid an estimated $20 million to provide citizens with identity fraud protection. A similar breach in Utah involved the theft of 280,000 social security numbers and $9 million in state spending to help protect citizens from identity fraud. In addition to the direct costs to the states, fraudulent activities resulting from these thefts have the potential to cost individual citizens, banks, and retailers millions of dollars more.

VITA and agencies must cooperate to secure data

VITA and agencies must cooperate to effectively secure the state's data. VITA, through its contractor Northrop Grumman, is responsible for securing IT infrastructure, which includes data centers, personal computers, and internet services. For example, Northrop Grumman manages the internet "spam filters" that block email messages contaminated with computer viruses. Agencies are responsible for

securing their applications, for example, by placing passwords and other controls to restrict access to their applications. VITA and agencies must work together, because a weakness in one area of security can allow other defenses to be bypassed.

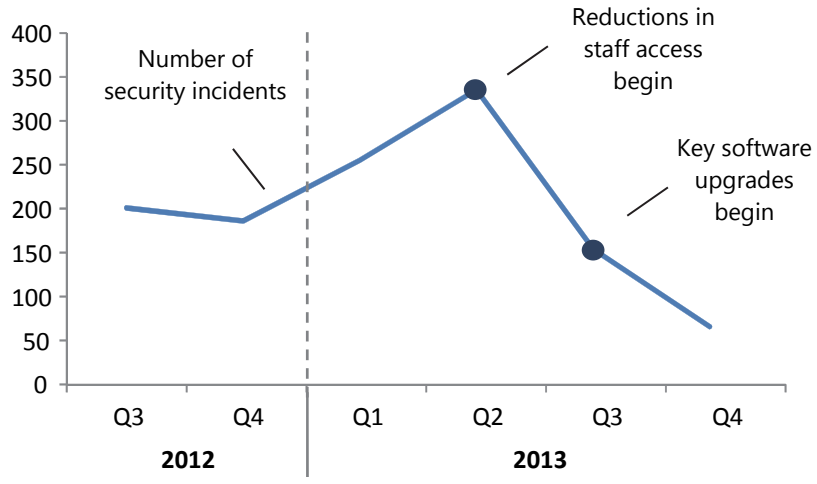
The 2012 South Carolina breach is an example of how both infrastructure and applications must be protected to effectively secure data. The breach occurred when an employee opened a virus-infected email that stole the employee's credentials. Intruders then used the credentials to gain access to sensitive applications and, ultimately, millions of personal data files.

The South Carolina incident could have been avoided if proper security measures were in place. Infrastructure security controls, such as spam filters, could have stopped the infected email before it reached the employee. Applications security controls, such as passwords and another identifiers, or a "two-factor" process for verifying employee credentials, could have limited the ability of intruders to use stolen credentials to access sensitive data.

Cooperation between VITA and agencies has reduced security incidents but could be further improved

VITA has successfully collaborated with agencies on several statewide security initiatives. Most notably, VITA and agencies reduced the number of employees with broad access to state systems. They also fixed security vulnerabilities in software that is commonly used by agencies. VITA reported an 80 percent reduction in security incidents from the second to the last quarter of 2013, mostly due to these efforts (Figure 4-2).

FIGURE 4-2
Cooperation between VITA and agencies has reduced security incidents



Source: JLARC staff analysis of VITA security initiatives and incident trends.
Note: VITA defines a security incident as any event in which the IT environment has been compromised, such as an incident where a computer virus has infected an office computer.

VITA indicated that implementation of the above efforts was challenging because agency cooperation was initially lacking. It took two years to get agencies to begin restricting employee access and a full year before agencies started to address the widespread security vulnerabilities in their software. According to VITA staff, repeated communications from the CIO and others within VITA to agency IT directors, and even agency heads, was needed to prompt action.

VITA indicated that it has also faced challenges in gaining agency cooperation in an ongoing effort to replace an old computer operating system, Windows XP, which is highly vulnerable to attack. Replacing this type of software can disrupt agency operations, so VITA needs agency cooperation before it can move forward. However, several agencies were slow to replace Windows XP on thousands of their computers. Securing these at-risk computers will cost the state an additional $800,000 to $900,000 in fiscal year 2015.

CASE STUDY
Upgrading from Windows XP

Windows XP is an operating system for personal computers that was widely deployed across the state. In 2011, Microsoft announced that it would end support for Windows XP by April 8, 2014. This meant that it would no longer develop security patches and other fixes that ensure the operating system is secure.

In 2012, VITA began working with agencies to upgrade more than 50,000 computers from Windows XP to a newer version of Windows. Close cooperation was necessary because agencies needed to modify their applications to work on the new operating system. However, as of the April deadline, 3,965 computers were still using Windows XP.

Because regular support has ended, agencies still using Windows XP must pay Microsoft a one-time fee for special support. They must also pay additional fees to VITA for special internet protections for most of these computers. The total cost of added support fees for Windows XP is estimated to be $800,000 to $900,000 for fiscal year 2015.

IT security and risk management program

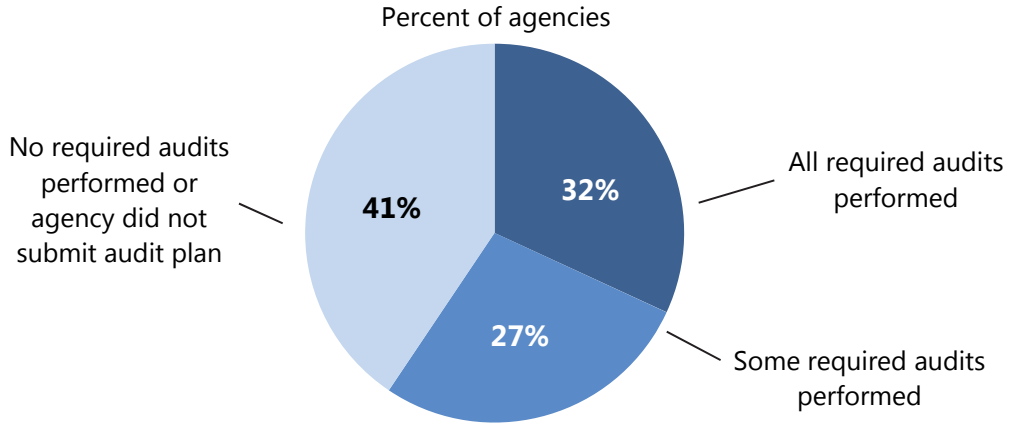
VITA sets requirements and monitors agency compliance with the state's IT security and risk management program. The most substantial component of the program requires agencies to perform security audits of their sensitive applications every three years to identify vulnerabilities. Other program requirements include appointing a certified agency IT security officer and assessing and documenting risks posed by security incidents.

VITA has also faced challenges in gaining agency compliance with the state's IT security and risk management program. Under the program, VITA requires agencies to plan and perform security audits of their sensitive applications. These audits identify vulnerabilities in their applications that could be exploited by intruders. Agencies are responsible for fixing any vulnerabilities that are identified and reporting remediation to VITA.

In 2013, VITA's annual security report found that only 32 percent of state agencies fully met the requirement to perform security audits of their sensitive applications (Figure 4-3). An additional 27 percent performed audits of some, but not all,

sensitive applications. The remaining 41 percent of agencies did not complete any required audits or did not submit a plan identifying which applications needed to be audited. Agencies that did not meet their audit obligations included both large and small agencies across almost all of the state's secretariats (Appendix C). Based on low compliance, VITA's report concludes that "agencies are not implementing the controls needed to protect their data and ensure only authorized personnel can access their applications," which "contributes significantly" to malicious attacks by outside parties.

FIGURE 4-3
Only 32 percent of agencies performed security audits of sensitive applications



Source: JLARC staff analysis of VITA's Annual Report on Information Security in the Commonwealth for 2013.
Note: Shows percentage of agencies that performed required security audits of sensitive IT applications every three years. Agencies that did not submit a plan identifying audit requirements are grouped with agencies that did not conduct any of the required security audits.

Compliance with security audit requirements and other efforts appears to be low because some agencies do not appear to view IT security as a high priority. VITA and agency IT directors indicated that agencies have not allocated the resources needed to carry out their security responsibilities. IT directors indicated that this was partly because their agency directors may not clearly understand their obligations to protect data. VITA indicated that agencies are also generally more likely to commit resources to developing new operations-oriented capabilities rather than toward less visible efforts to improve security.

In order to complete security audits, agencies need information from VITA about the security of the infrastructure that supports their applications. Agencies indicated that getting this information from VITA can be challenging, but VITA ultimately provides most of what they need. However, to facilitate agency security audits, VITA could improve its responsiveness to agency requests.

CIO's security responsibilities

The CIO is responsible for developing and enforcing IT security standards and responding to security incidents, such as data breaches at state agencies. As the head of VITA, the CIO is also responsible for ensuring that the state's IT infrastructure is secure.

Security could be improved by expressly assigning data protection responsibilities to agencies and VITA

Even though data protection is a critical responsibility, Virginia statute does not assign this overall responsibility to any party. Agencies are assigned statutory responsibility for protecting a highly sensitive subset of state data: personal information (§ 2.2-3800). However, several types of personal information are exempted from these protection requirements, such as data held by criminal justice agencies. Moreover, the protection requirements do not extend to the dozens of other types of non-personal data maintained by agencies that are critical to their operations, such as agency budgeting and financial accounting data.

Although Virginia statute does not assign general responsibility for securing data, other state and federal requirements give agency directors this responsibility. The state's IT security standard unequivocally states "each agency head is responsible for the security of the agency's electronic information." Similarly, the federal government has enacted requirements that make agencies that use sensitive federal data responsible for its protection. For example, state agencies that handle federal tax and social security administration information are responsible for protecting it.

Consistent with other state and federal requirements, agency directors should be assigned statutory responsibility for protecting all agency data. Clarifying the responsibilities of agencies should help increase the priority that they place on security and the resources they allocate to address security concerns. This added emphasis may also encourage compliance with VITA security initiatives and the state's IT security and risk management program.

To further encourage compliance, the section of the Code of Virginia describing the duties of agency directors (§ 2.2-603) should be amended to reference agency directors' responsibility to comply with the security and risk management program (§ 2.2-2009). The section of the Code describing VITA's responsibilities already states that agency directors have this responsibility, but low compliance rates suggest that this responsibility is not being effectively communicated. The recommended change would make this responsibility more visible.

Because VITA manages the state's IT infrastructure, its cooperation is needed for agencies to successfully fulfill their security obligations. VITA should be assigned statutory responsibility for providing agencies with all information needed to meet the requirements of the security and risk management program. This would include information that agencies need to complete security audits of their applications. VITA's security standards should be revised to reflect this responsibility.

RECOMMENDATION 9

The General Assembly may wish to consider amending § 2.2-603 of the Code of Virginia to assign agency directors responsibility for securing the electronic data held by their agencies and clarify their responsibility to comply with the requirements of the state's IT security and risk management program.

RECOMMENDATION 10

The General Assembly may wish to consider amending § 2.2-2009 of the Code of Virginia to assign the CIO responsibility for providing agencies with information and other assistance needed to meet the requirements of the state's IT security and risk management program.

RECOMMENDATION 11

VITA should amend IT standards to reflect its responsibility to provide agencies with information and other assistance needed to meet the requirements of the state's IT security and risk management program.

IT procurement requirements could be clarified to improve agency compliance

IT procurement is another key area where requirements could be clarified. When VITA was created in 2003, it was given central authority over IT procurements. VITA sets IT procurement rules, makes purchases on behalf of agencies, and oversees agencies' IT procurements. Agencies appear to generally comply with procurement requirements; 97 percent of agency IT procurements followed the proper process in 2013. However, those few procurements that do not follow the process can create security risks and support challenges.

One example of a procurement that did not follow the proper process is the purchase by the Virginia Employment Commission (VEC) of $750,000 in network cabling and equipment for its headquarters in 2012. Although VEC informally notified VITA it was preparing to install this equipment, the procurement was not identified for VITA review under the required process. Consequently, the procurement moved forward without VITA review and approval. VEC staff indicated that the procurement was not marked for VITA review because they believed it fell outside the scope of VITA's authority. The type of network purchased by VEC does not conform to state standards. As a result, VITA indicated it cannot be monitored as effectively as other state networks, and that problems, such as virus infections, are more challenging to address.

VITA and the Department of General Services (DGS), which is responsible for the state's non-IT procurements, have been vested with similar authorities for overseeing agency procurements. VITA could use its existing authority to establish additional controls similar to those used by DGS. For example, VITA could establish a single

Central procurement intended to reduce costs

Central IT procurement is intended to reduce costs by ensuring the use of state IT con-tracts, improving services through efficient and timely processes, and promoting standardization of the state's IT assets through procurement reviews.

integrated process for certifying when an agency has been delegated one-time procurement authority. The lack of a clear process may have contributed to VEC proceeding with its network purchase without gaining VITA approval. However, before adding new requirements, VITA should ensure that they will not unnecessarily delay procurements, most of which already follow the required process.

Similar DGS and VITA procurement authorities

DGS and VITA have the authority to set procurement requirements that most executive branch agencies must follow. Both are vested with the authority to procure goods and services themselves or to delegate procurement authority to agencies. Both may revoke delegated authority if an agency does not comply with their requirements.

The Code of Virginia includes several provisions that are designed to encourage compliance with the requirements set by VITA, DGS, and state procurement laws. However, two statutory provisions that are intended to encourage agency compliance are established in the DGS section of Code, and so it is not clear whether they also apply to IT procurements. The first provision allows the state comptroller to stop payment on procurements that have not been properly conducted or otherwise violate the state's procurement laws. The second provision states that purchasing officers who continually and intentionally commit violations are to be held accountable by being suspended or removed from office for malfeasance. Although these two provisions clearly apply to non-IT procurements, it is not clear whether they also apply to IT procurements. Clarifying that these provisions apply to IT procurements would further encourage agency compliance by ensuring all procurements are subject to the same enforcement mechanisms.

RECOMMENDATION 12

The General Assembly may wish to consider amending § 2.2-2012 of the Code of Virginia to stipulate that the state comptroller shall not authorize payment for IT purchases made in violation of state laws or IT procurement requirements and that intentional violations of centralized IT purchasing requirements can result in the responsible purchasing officer being suspended or removed from office.

5 Increasing Agency Involvement in Central IT Decisions

SUMMARY Virginia's IT governance structure is partially centralized, meaning that VITA and agencies each maintain responsibility for different aspects of IT. VITA controls the state's IT infrastructure and provides services to agencies. Although agencies are required to use VITA's services, they have limited input into decisions governing those services. The state has created agency bodies to advise on services and other central IT issues, but they have been largely ineffective because they do not play a role in the decision process. Agencies also had limited involvement in several of the decisions that led to the contract for services from Northrop Grumman, which appears to be one reason why these services sometimes do not meet agency needs. In contrast, CIOs in other states indicated they involve agencies directly in central IT decisions. CIOs of private companies indicated that they also work closely with their business leaders to develop services that meet company needs. Because there is no "best model" for Virginia to follow, the Secretary of Technology, CIO, and agencies should be charged with developing a new governance approach for involving agencies in the central IT decision process. In the short term, these parties should develop and implement a separate proposal specifically for involving agencies in planning for the end of the state's contract with Northrop Grumman.

Virginia's IT governance responsibilities are shared between VITA and state agencies. This partially centralized structure makes cooperation between VITA and agencies vital to the successful management of IT and, by extension, state operations. As discussed in previous chapters, VITA needs agency cooperation in order to carry out its IT oversight and service responsibilities. For example, VITA needs agency cooperation to upgrade infrastructure assets and identify security risks. Similarly, agencies depend on VITA to provide the data center, personal computing, and internet services they need for daily operations.

Agency involvement in the decision to contract for services from Northrop Grumman varied, with a limited number of agencies having substantial involvement in some decisions but no involvement in several others. The lack of agency involvement in several critical decisions appears to be one reason why these services sometimes do not meet agency needs.

Agencies have a limited role in central IT decisions, which impairs effective governance

IT is a tool that organizations use to help achieve business objectives. IT decisions should therefore be largely driven by business decisions. However, Virginia's central

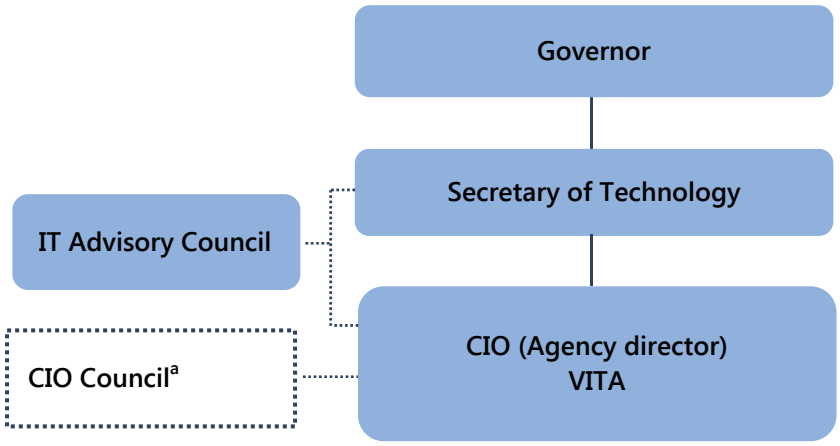
IT services are managed with limited input from the agencies whose business operations they support. In some cases, lack of agency involvement in central IT decisions appears to have impaired effective decision making.

Agency involvement in central IT governance is limited

Even though agencies have a substantial stake in central IT decisions, they have a minimal role in the current governance structure. Agency involvement is facilitated through two advisory bodies: the Information Technology Advisory Council (ITAC) and the CIO Council (Figure 5-1). ITAC is intended to represent agency business leaders, while the CIO Council is intended to represent agency IT directors. These bodies provide agencies with an avenue for advising on central IT decisions but do not give them a formal role in the decision-making process. For example, neither ITAC nor the CIO Council is vested with the authority to request or approve changes to VITA's infrastructure services.

ITAC was created under statute in 2010 as the main body for providing agency advice on IT issues, but it has not effectively performed this role. ITAC has not carried out several basic responsibilities expected of an advisory board. Specifically, ITAC has not issued recommendations to the CIO or secretary; it has not directed the development of studies or reports, or adopted rules and procedures for the conduct of its business. ITAC has not appointed a new chairman for 2014, or held regular meetings. It met only twice in 2013 and not at all in 2014.

FIGURE 5-1
Agency involvement in central IT governance



Source: JLARC staff analysis of the Code of Virginia and VITA materials.
[a] The CIO Council is not established under statute and so is not a formal component of the state's IT governance structure.

It appears that ITAC has not carried out the basic tasks assigned to it because of its limited governance role. ITAC's advisory duties are only vaguely defined, and the secretary and CIO have total control over central IT decisions so are free to ignore ITAC's advice. ITAC members therefore do not have an incentive to invest the time and effort needed to develop thoughtful advice.

Although generally ineffective, ITAC does appear to have successfully accomplished one task. ITAC was directed by the legislature to develop the state technology business plan, which describes how IT can support state objectives. To accomplish this task, ITAC created a working group to guide the plan's development and review the final document prepared by VITA staff. ITAC appears to have been successful because it was given a clear goal to accomplish and a deadline for accomplishing it.

CIO Council membership

The CIO Council is composed of 15 IT directors representing the nine largest VITA customer agencies as well as representatives from six medium and small agencies. Members are invited to join by the CIO.

The CIO Council, the state's other agency advisory group, was created by the CIO in 2009 to "provide state agencies additional input into decision-making regarding information technology." The council is not established under Code and does not have a charter or any specific duties, so it is not a formal component of the state's IT governance structure.

The CIO Council meets regularly and its members are actively engaged in advising VITA on services, planning decisions, and issues of special concern to agencies. The CIO indicated that the council's advice is useful and helps inform VITA's decisions. However, as with ITAC, the council's influence is limited because it has no formal role in central decisions. As one council member indicated, the council "is not leading decisions or pointing VITA in the direction that agencies need it to go."

The lack of agency involvement in central IT decisions may be detrimental to both VITA and agencies. Excluding agencies from the decision process limits their ability to ensure that central IT services meet their needs. VITA may also be negatively impacted because agencies are less willing to cooperate on statewide initiatives that have been developed without their participation.

Problems with infrastructure services illustrate need for greater agency involvement in central IT decisions

Agencies have had a limited role in major central IT decisions that directly affect their operations, including several of the decisions that led to the state's contract for infrastructure services with Northrop Grumman. Agencies were not involved in the decision to centralize all infrastructure services through a broad partnership with a single private company. Thirteen agencies were brought into the decision process after the initial direction was set. These agencies were involved in reviewing and approving most aspects of the proposed partnership, but not in determining how IT services could best meet their business needs. More recently, agencies had no role in the 2010 decision to renegotiate and extend the contract with Northrop Grumman, which reset service prices and performance expectations.

Northrop Grumman selected through PPEA process

Shortly after VITA's 2003 creation, several companies submitted proposals for providing central IT services under the Public-Private Education and Infrastructure Act (PPEA). The state elected to pursue a PPEA partnership instead of a typical competitive bid procurement.

Limited agency involvement appears to have been one of the factors that led the state to contract for services that often did not meet agency needs. Over a third of agencies surveyed for JLARC's 2010 report rated Northrop Grumman's services as poor in every category except security. Agencies indicated that several Northrop Grumman service offerings did not meet basic needs, such as adequate computer memory or email storage. The report found this was because VITA entered into the contract with Northrop Grumman without an adequate understanding of agency business needs. The report also concluded that a lack of understanding of the unique needs of state agencies led VITA to incorrectly assume the contract with Northrop Grumman would reduce statewide IT costs.

Agencies interviewed by JLARC staff in 2014 indicated that the quality of services has improved, but still sometimes do not meet needs. Most notably, agencies indicated that Northrop Grumman is slow to respond to agency requests. For example, several agencies indicated it can take an unreasonably long time for Northrop Grumman to provide new infrastructure, such as computer servers and wireless networks. Additionally, agencies indicated that the company can be slow to respond to day-to-day problems, such as fixing broken computers.

Responsiveness issues appear to stem from how the contract with Northrop Grumman is designed. Under the contract, Northrop Grumman's performance is measured on a statewide basis, which means that it can meet its overall performance requirements even if services to some individual agencies are sub-par. There are also gaps in the performance measures. Most notably, there is no measure that holds Northrop Grumman accountable for installing new equipment in a timely manner. In other instances, the performance measures do not appear to hold Northrop Grumman to a high standard. For example, Northrop Grumman is only required to provide on-site assistance to agencies within one business day (eight hours) after receiving a request. Northrop Grumman can be late in responding to 30 percent of same-day requests without incurring a penalty.

Other states and private companies involve business leaders in central IT decisions

Public and private sector CIOs indicate that they involve business leaders in central IT decisions. This allows business leaders to communicate their needs to the central IT providers, who can then develop technology services that best meet those needs.

JLARC staff interviewed CIOs from five other states that have partially or fully centralized IT responsibilities, and found that each includes agencies directly in its central IT decision process (Table 5-1). Georgia is the state most similar to Virginia in terms of how its IT has been centralized. Georgia's central IT agency sets standards and oversees agency investments. Like Virginia, Georgia consolidated its IT infrastructure several years ago under an outsourcing agreement. To support the

TABLE 5-1
Other states incorporate agencies directly into central IT governance

State	Centralized oversight	Centralized infrastructure	Centralized IT staff	Agencies have role in central IT decisions
Minnesota	✓	✓	✓	✓
North Carolina	✓	✓	✓	✓
Pennsylvania	✓	✓	✓	✓
Georgia	✓	✓		✓
Ohio	✓			✓
Virginia	✓	✓		

Source: JLARC staff interviews with the state CIOs of Georgia, Minnesota, North Carolina, Ohio, & Pennsylvania.

centralized model, Georgia has recently established several non-statutory agency groups to promote cooperation and "buy-in" on decisions. These groups are responsible for:

- identifying statewide and multi-agency business needs,
- participating in decisions on new infrastructure services and standards, and
- reviewing major IT projects.

Minnesota, North Carolina, and Pennsylvania have included agencies directly in their central IT decision processes by requiring agency CIOs to report to the state CIO. This direct reporting relationship allows agency CIOs to effectively communicate their needs and helps the state CIO ensure cooperation. Minnesota and North Carolina have also implemented additional mechanisms to ensure that central services meet agency needs:

- Minnesota's central IT agency has developed service performance agreements with each agency it serves.
- North Carolina has established agency-led groups that make IT business decisions and manage specific central services, such as personal computing.

Ohio, which is less centralized than Virginia, also appears to involve agencies in central decisions. The Ohio CIO, with the support of the governor, has recently formed "line of business" groups composed of agencies with similar missions (comparable to Virginia's secretariats). These groups are charged with identifying how agencies can work together to achieve goals, such as through consolidation of the state's data centers. The Ohio CIO indicated that this approach puts agencies in charge of deciding how to move forward with centralization and helps to develop the agency "buy in" needed to succeed.

Corporate IT structures also emphasize close cooperation between business leaders and the central technology office. A 2013 report by the National Association of State CIOs found that private sector CIOs "emphasized the importance of having an [IT] organizational structure closely aligned with their business units." The CIOs indicated that their companies' business and IT representatives met regularly to ensure technology services were meeting business needs.

The variety of approaches used by other states for involving agencies in their central IT decision processes indicates that there is no clear "best model" for Virginia to follow. CIOs in other states indicated that each state's model should be customized, because each state has a different executive branch structure, political environment, and historical experience that can impact what approaches are feasible. Moreover, these CIOs stressed that the model must have the support of the state's key stakeholders to succeed, most notably the governor, legislature, central IT authorities, and major state agencies.

To improve agency involvement in Virginia, the CIO, Secretary of Technology, and agencies should develop a proposal for incorporating agencies into the state's central IT decision process. ITAC, whose membership includes representatives from each of these parties, should be the specific body tasked with leading this effort. Although ITAC has generally been ineffective as an advisory body, it has shown that it can succeed in accomplishing discrete tasks when given a clear goal and a time frame for achieving it. Agencies that serve on ITAC will have the incentive to participate in the effort because they stand to benefit from changes to the central IT decision process. To ensure that ITAC effectively carries out its tasks, the governor should review the current ITAC appointees and determine if changes to its membership are needed. In carrying out its work, ITAC should consider involving the CIO Council, other IT advisory bodies, and state agencies that are not represented among ITAC's membership.

Proposed changes for improving agency involvement in key central IT decisions should be presented to the JLARC chairman by November 2015. The proposal may include changes to the statutory governance structure, if ITAC determines such changes are needed. ITAC should propose changes that it believes are best suited to meet Virginia's needs and can be feasibly implemented. ITAC should consider what level of agency involvement is most appropriate and how to balance the need to involve multiple stakeholders with the need to make timely decisions.

In the short term, ITAC should develop and implement a specific proposal for involving agencies in planning for the end of the state's contract with Northrop Grumman. Several critical planning decisions related to the end of the contract will be made by the end of 2015. VITA should implement ITAC's proposed process by April 2015 in order to ensure adequate agency involvement in these decisions.

RECOMMENDATION 13

The state Information Technology Advisory Council should develop and VITA should implement a specific proposal for involving agencies in planning for the expiration of the state's contract with Northrop Grumman by April 2015.

RECOMMENDATION 14

The General Assembly may wish to consider amending the Appropriation Act to require that the Information Technology Advisory Council (ITAC) develop a proposal for improving agency involvement in key central IT decisions. In developing the proposal, ITAC should consider the appropriate level of agency involvement in decisions affecting all areas of governance. The proposal may include changes to the statutory governance structure, if ITAC determines such changes are needed. The written proposal should be provided to the JLARC chairman by November 2015.

Appendix A: Study Mandate

2012-2014 Appropriation Act

Passed as Chapter 806 of the Acts of Assembly, May 3, 2013

§ 1-11. Item 31

E.1. The General Assembly hereby designates the Joint Legislative Audit and Review Commission (JLARC) to review and evaluate the Virginia Information Technologies Agency (VITA) on a continuing basis and to make such special studies and reports as may be requested by the General Assembly, the House Appropriations Committee, or the Senate Finance Committee.

2. The areas of review and evaluation to be conducted by the Commission shall include, but are not limited to, the following: (i) VITA's infrastructure outsourcing contracts and any amendments thereto; (ii) adequacy of VITA's planning and oversight responsibilities, including VITA's oversight of information technology projects and the security of governmental information; (iii) cost-effectiveness and adequacy of VITA's procurement services and its oversight of the procurement activities of State agencies.

3. For the purpose of carrying out its duties and notwithstanding any contrary provision of law, JLARC shall have the legal authority to access the information, records, facilities, and employees of VITA.

4. Records provided to VITA by a private entity pertaining to VITA's comprehensive infrastructure agreement or any successor contract, or any contractual amendments thereto for the operation of the Commonwealth's information technology infrastructure shall be exempt from the Virginia Freedom of Information Act (§ 2.2-3700 et seq.), to the extent that such records contain (i) trade secrets of the private entity as defined in the Uniform Trade Secrets Act (§ 59.1-336 et seq.) or (ii) financial records of the private entity, including balance sheets and financial statements, that are not generally available to the public through regulatory disclosure or otherwise. In order for the records specified in clauses (i) and (ii) to be excluded from the Virginia Freedom of Information Act, the private entity shall make a written request to VITA:

a. Invoking such exclusion upon submission of the data or other materials for which protection from disclosure is sought;

b. Identifying with specificity the data or other materials for which protection is sought; and

c. Stating the reasons why protection is necessary.

VITA shall determine whether the requested exclusion from disclosure is necessary to protect the trade secrets or financial records of the private entity. VITA shall make a written determination of the nature and scope of the protection to be afforded by it under this subdivision. Once a written determination is made by VITA, the records afforded protection under this subdivision shall continue to be protected from disclosure when in the possession of VITA or JLARC.

Except as specifically provided in this item, nothing in this item shall be construed to authorize the withholding of (a) procurement records as required by § 56-575.17; (b) information concerning the

terms and conditions of any interim or comprehensive agreement, service contract, lease, partnership, or any agreement of any kind entered into by VITA and the private entity; (c) information concerning the terms and conditions of any financing arrangement that involves the use of any public funds; or (d) information concerning the performance of the private entity under the comprehensive infrastructure agreement, or any successor contract, or any contractual amendments thereto for the operation of the Commonwealth's information technology infrastructure.

5. The Chairman of JLARC may appoint a permanent subcommittee to provide guidance and direction for VITA review and evaluation activities, subject to the full Commission's supervision and such guidelines as the Commission itself may provide.

6. All agencies of the Commonwealth shall cooperate as requested by JLARC in the performance of its duties under this authority.

Appendix B: Research Activities and Methods

JLARC staff conducted the following primary research activities for this review:

- interviews with staff and executives representing Virginia and other states, and
- review of documents, data, and literature relating to the governance of information technology (IT).

INTERVIEWS

JLARC staff conducted interviews with representatives from Virginia state government, including both the current and prior Secretary of Technology, the Chief Information Officer (CIO) and representatives from the Virginia Information Technologies Agency (VITA), and representatives from other state agencies. VITA staff interviewed included managers who oversee or are directly involved in planning, standards setting, contract negotiations, oversight of contractual services, security oversight, project management, and central procurement. State agency representatives who were interviewed included agency heads, senior administrators, and IT directors. The Virginia agencies interviewed are listed below.

- The Secretary of Technology (including both the current and prior office-holders),
- The Chief Information Officer (CIO) and staff of the Virginia Information Technologies Agency (VITA),
- Department for Aging and Rehabilitative Services,
- Department of Environmental Quality,
- Department of General Services,
- Department of Human Resources Management,
- Department of Motor Vehicles,
- Department of Social Services,
- Virginia Department of Health,
- Virginia Department of Transportation,
- Virginia Employment Commission,
- The Office of the Attorney General, and
- The Auditor of Public Accounts.

In addition to the above interviews, JLARC staff attended meetings of the state's IT governance bodies, including the CIO Council, the Information Security Council, and the Commonwealth Data Stewards Group. JLARC staff did not attend meetings of the Information Technology Advisory Council because the group did not conduct any meetings during the course of the study.

JLARC staff also conducted interviews with the CIOs of other state governments and the executive director of the National Association of State CIOs (NASCIO). The following parties were interviewed:

- CIO of Georgia,
- CIO of Minnesota,
- CIO of North Carolina,
- CIO of Ohio,
- CIO of Pennsylvania, and
- Executive Director of NASCIO.

DOCUMENTS, DATA, AND LITERATURE

JLARC staff reviewed extensive state documents and data related to the governance of IT in Virginia. The types of documents and data reviewed are listed below.

- IT statutes, including the Code of Virginia, current and past appropriation acts, and past IT reform bills in the Acts of Assembly;
- IT standards for asset management, project management, procurement, and security
- IT contracts, amendments, and agreements, including the state's respective contracts with Northrop Grumman and CGI Technologies and Solutions, Inc.;
- VITA and agency correspondence, including letters and emails;
- VITA data, including service performance, procurement, and financial data;
- VITA reports and presentations, including its annual security report and presentations to the CIO Council; and
- Agency organization charts.

In addition to the above primary documents and data, JLARC staff reviewed research literature related to Virginia in particular and IT governance in general. The types of literature reviewed are listed below.

- JLARC reports,
- Auditor of Public Accounts reports,
- NASCIO reports,
- Reports by Gartner Inc., a private sector technology consulting agency, and
- IT and other special reports from other states, such as the report by the Inspector General of South Carolina regarding that state's security breach.

The Gartner reports cited in this study were *CEO Advisory: When Should the CIO Report to the CEO?* 2011; *CEO Advisory: Think Harder About Your CIO's Reporting Line*, 2012; and *Best Actions in a Decade of CIO Resolutions as CIOs Move From Technical Manager to Digital Leader*, 2013. The NASCIO report cited in this study was *State CIO Leadership in Government Innovation and Transformation*, 2013.

Appendix C: Agency Compliance with Security Audit Requirements

VITA oversees the state's IT security and risk management program (§ 2.2-2009 of the Code of Virginia). The program requires that agencies review their IT applications to determine which applications are sensitive and need to be secured. Applications are sensitive if they hold sensitive data, such as personal citizen information, or if they are critical to agency operations. The program requires that agencies perform security audits of sensitive applications every three years to identify vulnerabilities that could be used by intruders to gain unauthorized access. Each agency is required to submit to VITA an audit plan that describes its sensitive applications and when it plans to audit them. The agency must then conduct audits and report the audit outcomes to VITA, along with its plans for and progress made in addressing any vulnerabilities that were identified. The following table shows the extent to which agencies have satisfied the basic requirements to submit a security audit plan and perform audits of their sensitive systems.

TABLE C-1
Agency compliance with security audit requirements

Agency	Secretariat	% of required audits performed	Agency size (Group)[a]
All required audits performed			
Virginia Employment Commission	Commerce and Trade	100%	I
State Corporation Commission	Independent	100%	I
Department of Environmental Quality	Natural Resources	100%	I
Department of Juvenile Justice	Public Safety & Homeland Security	100%	I
Department of State Police	Public Safety & Homeland Security	100%	I
Department of Transportation	Transportation	100%	I
Department of Veterans Services	Veterans & Defense Affairs	100%	I
Department of General Services	Administration	100%[b]	I
Department of Human Resource Management	Administration	100%	II
Dept. of Agriculture & Consumer Services	Agriculture & Forestry	100%	II
Department of Forestry	Agriculture & Forestry	100%	II
Dept. of Professional & Occupational Reg.	Commerce & Trade	100%	II
The Library of Virginia	Education	100%	II
Department of Medical Assistance Services	Health & Human Resources	100%	II
Virginia College Savings Plan	Independent	100%	II
Virginia Retirement System	Independent	100%	II
Virginia Workers Compensation Commission	Independent	100%	II
Marine Resources Commission	Natural Resources	100%	II
Department of Forensic Science	Public Safety & Homeland Security	100%	II

Agency	Secretariat	% of required audits performed	Agency size (Group)[a]
Board of Accountancy	Commerce & Trade	100%	III
Department of Minority Business Enterprise[c]	Commerce & Trade	100%	III
Department of Aviation	Transportation	100%	III
Some required audits performed			
Norfolk State University	Education	13%	I
Virginia State University	Education	81%	I
Department of Taxation	Finance	69%	I
Department of Health	Health & Human Resources	67%	I
Department of Social Services	Health & Human Resources	25%	I
Department for Aging & Rehabilitative Services	Health & Human Resources	64%	I
Indigent Defense Commission	Judicial	33%	I
Department of Conservation & Recreation	Natural Resources	33%	I
Department of Corrections	Public Safety & Homeland Security	92%	I
Department of Alcoholic Beverage Control	Public Safety & Homeland Security	72%	I
Department of Motor Vehicles	Transportation	93%	I
Dept. of Housing and Community Development	Commerce & Trade	40%	II
Department of Mines Minerals & Energy	Commerce & Trade	20%	II
Department of Education	Education	44%	II
Jamestown-Yorktown Foundation	Education	17%	II
Office of the Attorney General	Executive	67%	II
Department of Accounts	Finance	53%	II
Department of Health Professions	Health & Human Resources	50%	II
Department of Game & Inland Fisheries	Natural Resources	52%	II
No required audits performed or agency did not submit audit plan			
Dept. of Behavioral Health & Development Services	Health & Human Resources	No audit plan	I
Department of Labor and Industry	Commerce & Trade	No audit plan	II
Virginia Economic Development Partnership	Commerce & Trade	0%	II
Richard Bland College	Education	0%	II
The Science Museum of Virginia	Education	0%	II
Virginia Museum of Fine Arts	Education	0%	II
Virginia School for the Deaf & Blind	Education	0%	II
Department of the Treasury	Finance	0%	II
State Lottery Department	Independent	0%	II
Department of Criminal Justice Services	Public Safety & Homeland Security	No audit plan	II
Department of Emergency Management	Public Safety & Homeland Security	0%	II
Department of Fire Programs	Public Safety & Homeland Security	0%	II
Department of Military Affairs	Public Safety & Homeland Security	No audit plan	II
Virginia Information Technologies Agency	Technology	0%	II
Compensation Board	Administration	0%	III
State Board of Elections	Administration	No audit plan	III

Agency	Secretariat	% of required audits performed	Agency size (Group)[a]
Department of Business Assistance[c]	Commerce & Trade	No audit plan	III
Tobacco Indemn. & Community Revit. Comm.	Commerce & Trade	0%	III
Virginia Resources Authority	Commerce & Trade	No audit plan	III
Gunston Hall	Education	No audit plan	III
State Council of Higher Education	Education	0%	III
Department of Planning and Budget	Finance	No audit plan	III
Off. of Comp. Services for At-Risk Youth & Families	Health & Human Resources	0%	III
Virginia Foundation for Healthy Youth	Health & Human Resources	No audit plan	III
Virginia Museum of Natural History	Natural Resources	No audit plan	III
Center for Innovative Technologies[d]	Technology	No audit plan	III
Department of Rail & Public Transportation	Transportation	No audit plan	III
Motor Vehicle Dealer Board	Transportation	No audit plan	III
Agencies not required to perform audits			
Virginia Racing Commission	Agriculture & Forestry	Not applicable[e]	III
Frontier Culture Museum of Virginia	Education	Not applicable[e]	III
Virginia Commission for the Arts	Education	Not applicable[e]	III
Southwest Virginia Higher Education Center	Education	Not applicable[e]	III
Office of the Governor	Executive	Not applicable[e]	III
Office of the Inspector General	Executive	Not applicable[e]	III
Department of Historic Resources	Natural Resources	Not applicable[e]	III
Commonwealth Attorney's Services Council	Public Safety & Homeland Security	Not applicable[e]	III

Source: JLARC staff analysis of VITA's 2013 annual security report, 2014 employment data from the Department of Human Resources Management, and the Code of Virginia.

Note: The Code of Virginia and the most recent state government organization chart, dated January 1, 2013, list several additional agencies, institutions, and other entities that are not included in the VITA security report. This includes institutions of higher education, legislative agencies, and judicial branch agencies that are exempted from the state's IT security and risk management program requirements, as well as small entities that have their IT services provided through a parent or sister agency. The agencies, institutions, and other entities that are not listed in the VITA security report include: Assistive Technology Loan Fund Authority, Auditor of Public Accounts, Board of Bar Examiners, Christopher Newport University, Department for the Blind and Vision Impaired, Division of Capitol Police, Division of Legislative Services, Division of Legislative Automated Services, E-911 Services Board, George Mason University, Information Technology Advisory Council, Institute for Advanced Learning and Research, James Madison University, Joint Legislative Audit and Review Commission, Judicial Inquiry and Review Commission, Longwood University, New College Institute, Office of the Lieutenant Governor, Old Dominion University, Radford University, Secretary of the Commonwealth, College of William and Mary, University of Mary Washington , University of Virginia , Veterans Services Foundation, Virginia Agricultural Council, Virginia Board for People with Disabilities , Virginia Commercial Space Flight Authority, Virginia Commonwealth University, Virginia Commonwealth University Health Systems Authority, Virginia Community College System, Virginia Criminal Sentencing Commission, Virginia Department for the Deaf and Hard of Hearing, Virginia Geographic Information Network Advisory Board, Virginia Housing Development Authority, Virginia Military Advisory Council, Virginia Military Institute, Virginia Parole Board, Virginia Polytechnic Institute and State University, Virginia Port Authority, Virginia State Bar, Virginia State University, Virginia Tourism Authority.

[a] Group I agencies are agencies with 500 or more staff, as measured by full-time equivalents. Group II are agencies have 50 to 499 staff, and Group III agencies have 49 or fewer staff. [b] VITA's 2013 annual security report indicated that the Department of General Services (DGS) had completed only 33 percent of its audit requirement, but it appears that DGS has actually completed 100 percent of its requirement. The difference appears due to a miscommunication between DGS and VITA regarding how DGS systems are structured. VITA indicated that DGS did not resolve the misunderstanding until after the 2013 security report was published. [c] Effective January 1, 2014, the Department of Minority Business Enterprise and the Department of Business Assistance were consolidated into the Department of Small Business and Supplier Diversity. [d] The Center for Innovative Technologies is established under the Code of Virginia as the Innovation and Entrepreneurship Investment Authority. [e] Agency submitted plan that indicated it did not have any sensitive applications that required auditing.

Appendix D: Agency Response

As part of an extensive validation process, state agencies and other entities involved in a JLARC assessment are given the opportunity to comment on an exposure draft of the report. JLARC staff provided an exposure draft of this report to the following state agencies and entities:

- Office of the Secretary of Technology, and
- Virginia Information Technologies Agency.

JLARC staff also provided several additional parties with an opportunity to review selected sections of the report for technical accuracy. These included the Department of General Services, the Department of Human Resources, the Division of Legislative Services, the Office of the Attorney General, and the Virginia Employment Commission. Appropriate technical corrections resulting from their comments have been made in this version of the report. This appendix includes a written response letter provided by the Virginia Information Technologies Agency.

COMMONWEALTH of VIRGINIA

Samuel A. Nixon, Jr.
CIO of the Commonwealth
E-mail: cio@vita.virginia.gov

Virginia Information Technologies Agency
11751 Meadowville Lane
Chester, Virginia 23836-6315
(804) 416-6100

TDD VOICE -TEL. NO.
711

August 28, 2014

Mr. Hal E. Greer
Director
Joint Legislative Audit and Review Commission
Suite 1100, General Assembly Building
Richmond Virginia 23219

Dear Mr. Greer: Hal

Thank you for the opportunity to comment on the exposure draft of Virginia's Information Technology Governance Structure. On behalf of the staff at Virginia Information Technologies Agency (VITA), I want to thank Mr. Gribbin for his thoroughness and professionalism throughout the study. Although we will need additional time to fully review the report's recommendations, I would like to offer a few brief comments to supplement the feedback we gave Mr. Gribbin last week.

The creation of VITA represented an acknowledgement by executive and legislative leaders of the need for a business-like discipline in the management of IT services. VITA has achieved this and the other goals envisioned for the agency, including greater oversight and consistency in IT security, procurement, and project management. I want to thank Joint Legislative Audit and Review Commission (JLARC) for its acknowledgement of the benefits resulting from the creation of VITA. In no small part our successes reflect the combined efforts of VITA and our customer agencies, who together have made Virginia a nationally-recognized leader in the management of IT.

Looking ahead, the Commonwealth is faced with the twin challenges of maintaining current operations while simultaneously preparing to transition to the next phase of IT service provision. These endeavors will require the dedicated attention of executive branch leaders, policymakers, agency heads, IT staff, and others throughout the Commonwealth. To support these efforts, VITA will need to involve our customers and listen carefully to their individual needs, while also ensuring the Commonwealth's enterprise needs are met. Close collaboration with the legislature will also be essential. And as is the case with any agency, clear lines of communication, authority, and responsibility will also be required. VITA stands ready to play our part, and we will work with policymakers as they consider your recommendations.

I again, thank you for the opportunity to respond to this draft report, and I look forward to continuing our productive working relationship.

Sincerely,

Samuel A. Nixon, Jr.

c: The Honorable Karen R. Jackson, Secretary of Technology

AN EQUAL OPPORTUNITY EMPLOYER

JLARC.VIRGINIA.GOV

201 N. 9th Street, Suite 1100 Richmond, VA 23219