

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.

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

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.

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.