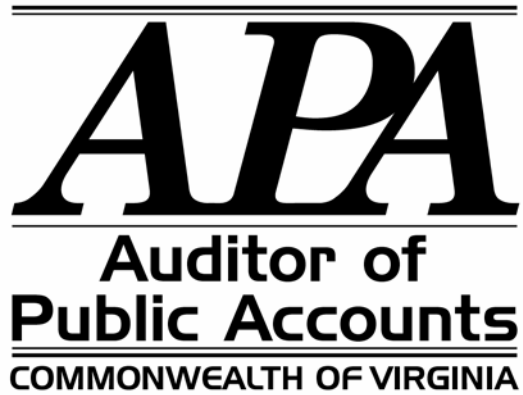
# REVIEW OF
# INFORMATION TECHNOLOGY GOVERNANCE AND VIRGINIA INFORMATION TECHNOLOGIES AGENCY OPERATIONS

**APRIL 2006**



# EXECUTIVE SUMMARY

The Code of Virginia established the Information Technology Investment Board (Board), the Chief Information Officer (CIO), and the Virginia Information Technologies Agency (VITA) as largely responsible for the Commonwealth's IT governance. IT governance involves establishing policies and standards that all Commonwealth agencies must follow.

The purpose of our audit was to identify areas where the Board, the CIO and VITA can improve the qualitative aspects of fulfilling IT governance statutes, referred to as legislative intent. As a result, our audit examined the statutes in context of whether the Board, the CIO and VITA have realized the potential that the legislation created, not whether they explicitly met the statutes. Where appropriate, our report recommends actions that the Board, the CIO and VITA can take as they move forward in developing strong IT governance.

Since beginning operations in 2003, the Board, the CIO and VITA have performed a significant amount of work effort towards improving the Commonwealth's IT governance. However, their ability to realize the legislative intent of these statutes has been slow due to competing priorities with VITA's IT operations that have demanded attention and resources. Specifically, VITA management and staff, the CIO, and Board have spent significant resources arranging and establishing the Commonwealth's relationship with Northrop Grumman, a company hired to manage and operate the Commonwealth's IT infrastructure beginning July 1, 2006.

The Board, CIO and VITA have experienced delays in fully meeting the potential of their responsibilities because of the time required to create a new entity, competing priorities and the almost nine months spent in hiring a CIO. During this delay, certain factors external to VITA set the early agenda for the Board, the CIO and VITA by default. It appears that the Board, CIO and VITA now have the direction to increase their momentum in meeting the legislative intent of their statutory responsibilities.

Under the current model, VITA staff have a conflict between their operational function, which is customer-service oriented, and their need to support the Board and CIO's governance function. The dual responsibilities sometimes add confusion regarding how VITA staff and Commonwealth agencies view VITA's role. The Board and CIO should improve this inherent conflict by increasing the Board's direction and involvement in IT governance, allowing governance issues to be communicated by the Board, or the CIO rather than VITA; thereby, separating this function from the VITA staff performing IT operations functions.

In April 2006, the Board approved the Commonwealth's IT Strategic Plan, which VITA staff prepared with the assistance of representatives of other State agencies. To realize the potential of this plan, it is important that the Board, the CIO and VITA clearly communicate it to state agencies and explain how they should use it to develop their agency IT strategic plans. For the plan to affect agencies systems development requests and their related budgets in the future, the Board, the CIO and VITA must work jointly with the Secretaries of Finance and Technology and the Department of Planning and Budget to incorporate this IT strategic plan into the Commonwealth's performance budgeting process.

- TABLE OF CONTENTS -

## OVERVIEW

### Reason for Audit

The Commonwealth has continued its efforts to consolidate its information technology (IT) from individual executive branch agencies into the Virginia Information Technologies Agency (VITA), headed by the Chief Information Officer (CIO). The purpose of this audit is to understand and evaluate the areas of strategic planning, project management, security, and contracting consultants. We have previously audited the security and project management areas and this report serves as a follow-up and more in-depth review of certain aspects of these areas. As in earlier audits of VITA, this report will make recommendations, where appropriate, to improve processes and control. This audit also includes a follow-up on recommendations from our previous audits and reports the status of corrective action taken by VITA.

### Description of Organization

Since VITA's creation in 2003, management has completed the consolidation of the three predecessor agencies, the Department of Information Technology, Information Planning and Virginia Information Provider's Network (VIPNet), with no disruption to continuing services. VITA has also undertaken the consolidation of the Commonwealth's executive branch networks, communications and information technology equipment.

To facilitate the consolidation of services, maintenance of equipment, infrastructure and supporting functions, VITA identified the need to seek outside assistance. Thorough a Public Private Educational Infrastructure Act proposal, VITA has elected to engage Northrop Grumman to provide this array of services. VITA anticipates that starting July 1, 2006 and by July 1, 2009, that Northrop Grumman will have completed a transformation of its IT infrastructure from an ownership-based operation to a service-provider arrangement, allowing the Commonwealth to achieve and maintain an IT infrastructure that will keep current with evolving technologies.

This agreement requires Northrop Grumman to finance this infrastructure transformation, absorb current Commonwealth employees or temporarily manage those who do not become part of the agreement, and maintain the infrastructure in accordance with industry standards during the life of the agreement. VITA and Northrop Grumman staff are managing this transfer of operations.

Concurrent with the creation of VITA was the creation of Information Technology Investment Board (Board), which has responsibility for hiring the Chief Information Officer (CIO), who is the agency head of VITA, overseeing VITA, but more importantly setting the Commonwealth's strategic vision and overseeing the IT application development within the Commonwealth. Using VITA staff, the Board addresses its broad Commonwealth statutory responsibilities. Since the Board is a citizen board, the speed and implementation of these responsibilities depends on the support that VITA staff provides.

Both VITA management and staff, and the Board have spent significant resources of time and direction in arranging and establishing the Commonwealth's relationship with Northrop Grumman. The Board has also committed resources to meet its broader mission and statutory responsibilities; however, as the report indicates, although the Board has laid some of the groundwork for meeting their responsibilities, significant work remains.

Part of the delay in fully meeting their responsibilities comes from the time required to create a new entity, competing priorities and the almost nine months spent in hiring a CIO. During this delay, certain factors external to VITA set the early agenda for the Board, CIO and VITA by default. It appears that the

Board and the VITA now has the direction to increase their momentum in meeting the legislative intent of their statutory responsibilities.

Our previous reports titled, "Virginia Information Technologies Agency," provided descriptions of the Information Technology Investment Board (Board), CIO, VITA, the Project Management Division (Division), and certain security programs and we have chosen not to repeat that information in this report. Instead, we encourage the reader to review the previous reports, available electronically at www.apa.virginia.gov.

## Areas of Review

Our audit focused primarily on activities in the areas of IT strategic planning, project management, security, and contracting consultants. We discuss our work and results within report sections dedicated to these specific areas. Our audit objectives were to determine that:

- The CIO and Board have fulfilled their statutory responsibilities and legislative intent relative to IT strategic planning, see Section I;

- VITA has fulfilled its statutory responsibilities and legislative intent relative to project management, see Section II,

- The CIO and VITA have fulfilled their statutory responsibilities and legislative intent relative to security and that such security services can be adequately described when outsourced later this year, see Section III;

- VITA has adequate procedures relative to contracting consultants, see Section IV; and

- The CIO, the Board, and VITA have taken adequate correction action relative to prior audit findings, see Appendix A.

## INTRODUCTION FOR SECTIONS I AND II

### Objectives and Methodology

The objectives of our audit of IT strategic planning and project management were to determine that the CIO, Board and VITA have fulfilled their statutory responsibilities and legislative intent relative to IT strategic planning and project management. We approached our audit of these objectives by reviewing applicable sections of the Code of Virginia and examining documents such as the Joint Legislative Audit and Review Commission's (JLARC) 2002 report titled, "Systems Development in Virginia" and Governor Warner's IT Strategic Plan, both of which led to legislation creating VITA and the Project Management Division (Division).

We met with JLARC staff to discuss our understanding of their report recommendations on project management. The Department of Planning and Budget provided us information on the strategic planning and the process used to prepare the Governor's budget for systems development projects. We also met with the Council on Virginia's Future to understand their role in defining the Commonwealth's strategic business plan. Finally, we met with management and specialists from VITA's Project Management Division to understand their policies, procedures, and operating activities. We examined documents from all of these sources as necessary.

### History and Background

In November 2000, JLARC directed staff to review information systems development and procurement by State agencies. The review was the result of concerns about problems with the procurement and development process and apparent waste of funds on systems never deployed. JLARC presented their report and recommendations in December 2002.

The release of JLARC's report coincided with an initiative by Governor Warner to implement his IT Strategic Plan for the Commonwealth. This plan called for moving IT from a decentralized, agency-by-agency process to a centralized operation. Consequently, the Secretary of Technology and JLARC staff worked together to draft legislation to create VITA and its Project Management Division (Division). The legislation supported both Governor Warner's plan to consolidate IT operations and the JLARC proposal to implement processes and controls to improve the Commonwealth's systems development. The legislation was approved and effective beginning July 1, 2003.

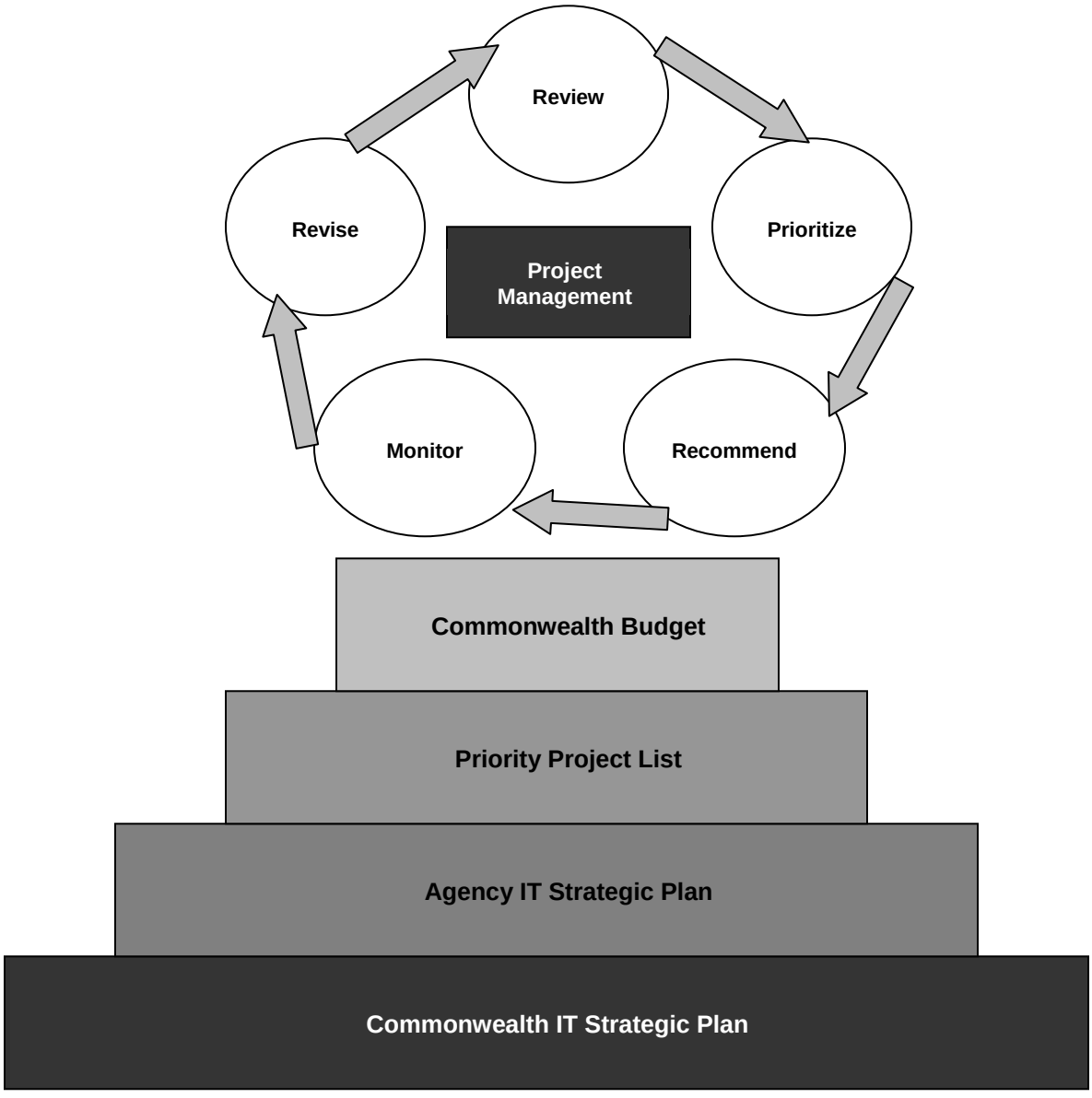
#### *Understanding the Legislative Intent as Established in the JLARC Report*

Since our audit objectives were to determine that the CIO and VITA has fulfilled their statutory responsibilities and legislative intent relative to project management, we reviewed the JLARC report to understand their recommendations. JLARC's report and recommendations were an important factor in enhancing Commonwealth IT project management and we believe it is the best source for interpreting the legislative intent behind the statutes.

The JLARC report recommended the creation of the Information Technology Investment Board (Board) to set strategic priorities, a full-time CIO to lead the development and planning of information systems, a more effective approval and oversight process for new systems, and a new funding mechanism to pay for major statewide or general fund agency projects. The report also recognized the need to develop stronger systems development expertise and increase agency support and improved IT strategic planning to link the plan to the agency business needs.

We prepared Exhibit 1 below to show how we interpret JLARC's recommended process for project management and to provide a baseline for legislative intent. Their process envisioned building from the foundation of strategic planning up to the active monitoring of systems development projects. We used this exhibit while planning and conducting our audit work and throughout this report, we compare this baseline to current strategic planning and project management processes. We also make recommendations that we believe will help the Commonwealth will bring current processes more in line with the legislative intent.

**Exhibit 1 – JLARC Recommended Process to Improve Systems Development**



JLARC envisioned a process where each process would build upon on another and support a Commonwealth –wide approach to IT investments. Below we provide a summary description of each process presented in Exhibit 1.

Commonwealth IT Strategic Plan

JLARC recognized that the existing strategic plan for technology did not establish clear guidelines for prioritizing projects across agencies. They recommended the development of a Commonwealth IT Strategic Plan that would provide long-term IT goals. JLARC also recommended that the Secretary of Technology, with the CIO's assistance, develop a two-year Commonwealth IT Strategic Plan based on agency strategic plans and a CIO analysis of statewide or multi-agency project priorities.

We discussed this bottom-up approach with JLARC. They acknowledged their recommendation used the Commonwealth's budgeting and strategic planning process in existence in 2002 and substantial changes have occurred in the State's strategic budgeting approach. JLARC recognized that the approach they originally recommended is now inappropriate given the creation of the Council on Virginia's Future and their role in setting the Commonwealth's business strategic plan. They agree that today they would recommend an IT strategic plan to support the Commonwealth's strategic plan and that agency strategic plans be aligned to these plans

Agency IT Strategic Plan

Based on the JLARC's review, the Commonwealth needed an effective strategic planning process to direct the information systems development process. Looking to strategic planning best practices, agencies should develop their IT strategic plans to support identified business needs. With the envisioned Commonwealth IT Strategic Plan in place, agencies would understand the Commonwealth's IT priorities and goals and align their agency IT plans to the Commonwealth's plan.

Priority Project List

An independent Board would be established and given responsibility for overall IT investment decisions. By considering the Commonwealth's priorities, this Board and CIO, would be in a unique position to evaluate individual agency IT strategic plans from a statewide perspective. This would eliminate duplicative systems by evaluating individual projects for enterprise opportunities and encourage coordination and collaboration among agencies. Procedurally, the Board and CIO would receive project proposals in the agency IT strategic plans and rank the projects in order of priority based on how they support overall Commonwealth goals identified in the Commonwealth IT Strategic Plan.

Commonwealth Budget

The prioritized project list would assist the Governor and General Assembly in determining which projects to fund. The JLARC report offered several alternatives to include biennial funding up to a cap amount, issuing bonds, direct appropriation to a central technology fund, and a revolving loan fund to help agencies pay for new systems.

Project Oversight

A group of project management specialists, organized into a Project Management Office, would provide monitoring and oversight tasks and work closely with agencies in a support role for active projects. These specialists could assist agencies in planning and developing a business case and aid in procurement and identify situations requiring specialized skills. The Project Management Office would establish project management standards, provide training programs to agency project managers, and develop a clearinghouse to exchange best practices.

One important role of the project management specialist would be to provide an ongoing assessment of projects and provide reliable, unbiased reports to the Board and CIO. With this oversight, problems could be identified and addressed quickly and contribute to an effective project management and oversight structure.

***Understanding Current Strategic Planning and Project Management Processes***

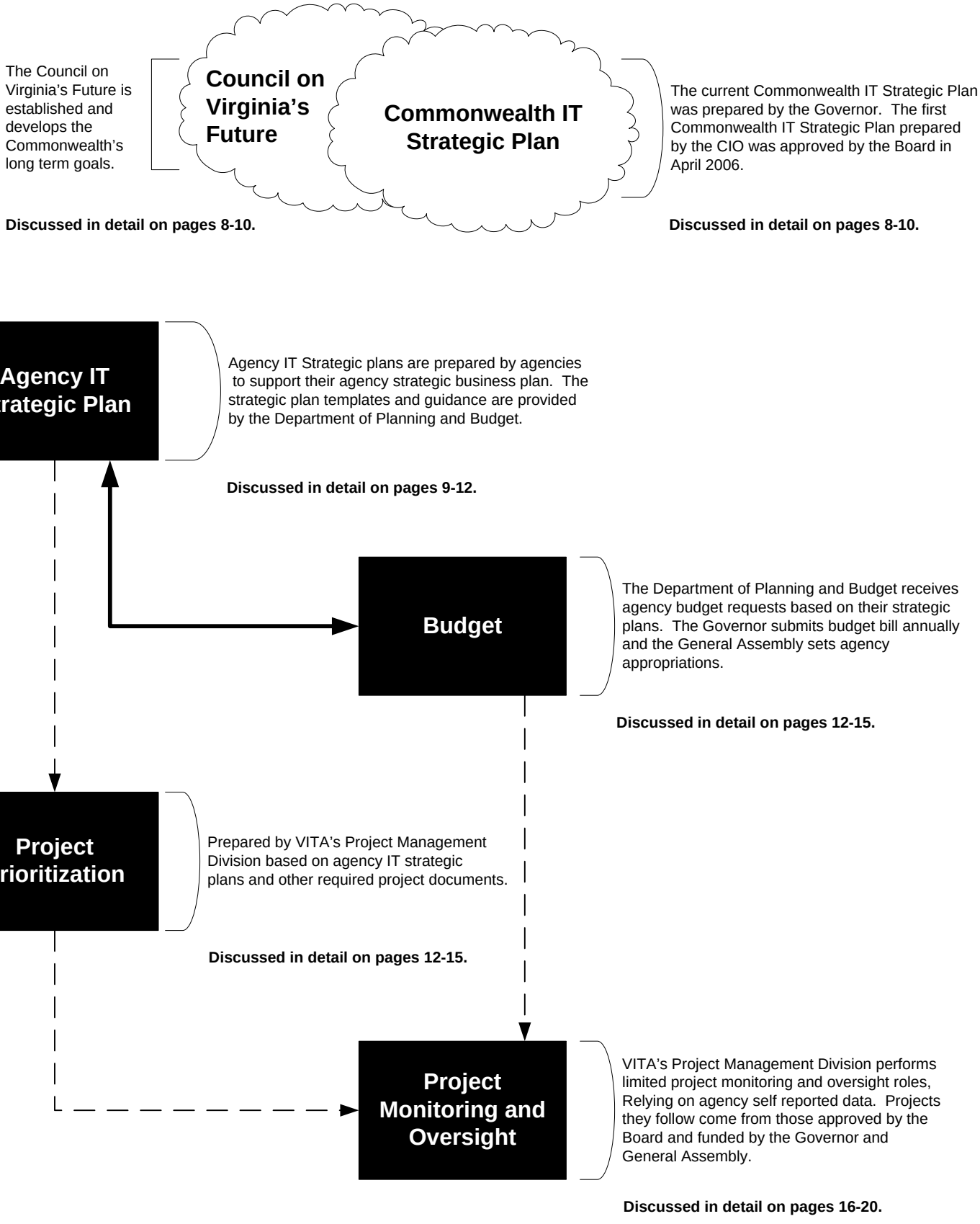
Similar to Exhibit 1, which represents JLARC's vision, we have provided the following Exhibit 2 as a high-level view of how strategic planning and project management currently works in the Commonwealth.

One of the most significant differences that we observed when comparing JLARC's vision to how current processes actually work is that current processes involve several agencies or individuals and do not rely or build upon the same information or framework.

As a result, the Commonwealth has not achieved the strategic planning or systems development methodology recommended by JLARC and expected when the legislature established the CIO, VITA, the Board, and the Division. We believe the 2003 legislation that created VITA contains the elements necessary to realize the JLARC approach but on several levels, the Commonwealth has failed to implement fully the legislation.

In Sections II and III, we will discuss in more detail how the Commonwealth currently operates, compare current operations to the legislative intent, and recommend strategic, governance and operational changes.

Exhibit 2 – Current Strategic Planning and Project Management Processes



## SECTION I – IT STRATEGIC PLANNING

### Commonwealth IT Strategic Planning Efforts

As enacted by the 2003 General Assembly, the Code of Virginia gives the CIO responsibility for monitoring trends and advances in technology to support the development of a comprehensive, statewide, four-year strategic plan. This reflects a longer-term focus than originally envisioned by JLARC and is more in line with strategic planning best practices. The Code of Virginia also requires that the CIO annually update the Commonwealth IT Strategic Plan and submit it to the Board for approval.

#### *2002 - 2006 Commonwealth IT Strategic Plan*

The CIO inherited the Commonwealth IT Strategic Plan issued September 2002 by Secretary Newstrom on behalf of Governor Warner, developed prior to the issuance of JLARC's report or the creation of VITA. This plan provided guidance for the future of IT in the Commonwealth, focusing both on economic development related initiatives as well as operational initiatives within state government. This plan remained unchanged until Spring 2005, when it underwent a partial update, despite the Code of Virginia required annual update.

While the CIO headed the update effort, the update only addressed half of the original eight initiatives over which VITA had direct responsibility. The CIO identified the remaining initiatives as being the responsibility of the Center for Innovative Technology and reflected them in their goals and priorities for 2005. The goals, objectives, and initiatives presented in the update closely aligned to the VITA business plan.

Due to the VITA-centric focus of this update, the plan did not meet the legislative intent of serving as the building block for agency IT strategic planning as shown in Exhibit 1. The updated plan focused on VITA's accomplishments and next steps in fulfilling their business plan, rather than Commonwealth-wide initiatives. Thus, other than providing agency awareness of major VITA initiatives that might impact their internal planning, this update did not provide the strong direction for IT priorities the legislation intended.

#### *2007 - 2011 Commonwealth IT Strategic Plan*

With the completion of the 2005 update, the CIO announced work was beginning on the second edition of the Commonwealth IT Strategic Plan, with Board approval of the final draft scheduled for Spring 2006. To support this process, VITA staff held a series of stakeholder workshops in Fall 2005, gathering information concerning technology, economic and political trends in the Commonwealth. The workshop findings served as the basis for a two-day strategic planning retreat in early January 2006 to develop a rough draft of the Commonwealth's IT strategic mission, vision, goals, objectives, and initiatives. The retreat involved members of the Board, selected agency and local government IT representatives, VITA management, and the Council on Virginia's Future.

Retreat participants had difficulty reaching consensus on the mission and vision statements for the IT strategic plan. Discussions held with participants during the workshop and at later meetings reflected a lack of awareness of the Commonwealth's strategic direction. We believe that retreat participants would have benefited from a brief discussion of the Commonwealth's strategic business direction, as defined in the Council on Virginia's Future's Roadmap, and how the IT strategic plan should relate to that plan. Further, we believe that business representatives should have been included as participants rather than primarily including IT representatives. By adding a business perspective to the discussions, participants may have been more successful defining the mission and vision.

VITA staff then formed a second workgroup to refine the retreat products into the new Commonwealth IT Strategic Plan. This smaller group retained an IT representative make up and also struggled with the ultimate goal for the plan. Several participants made comments that they could not see whether the workgroup's draft plan was the Commonwealth's IT Strategic Plan or VITA's operating plan. After some discussion, the group agreed that the plan should be the Commonwealth's plan and made efforts to remove the VITA-oriented approach and reinforce a Commonwealth-wide perspective.

The participant's struggles and challenges in reaching consensus, and then their late realization that the plan should represent the Commonwealth, reveals an inherent conflict within the roles of the CIO. The CIO is responsible for governance and providing strategic direction, standards, and policies and procedures to manage the use of Commonwealth IT. VITA staff supports the CIO in this governance role. The CIO is also responsible for Commonwealth-wide IT operations and he serves as the VITA Director whereby many of the standards, policies and procedures are executed by VITA staff on behalf of agencies.

These roles often conflict and create a tenuous relationship between VITA and the agencies it serves. On one side, VITA staff is directing the agencies as to how they are to manage their internal operations to protect the Commonwealth's interests. On the other side, VITA staff is focused on customer service and meeting the needs of the agencies in a satisfactory manner.

Agencies have expressed confusion and frustration over VITA's roles, resulting in agencies not trusting VITA's motives in providing IT governance. Some agencies fear that VITA's governance is solely a means to establish further control, since VITA already controls agency IT operations. This attitude impacts the quality of information agencies pass to VITA, as well as the methods with which VITA attempts to execute its legislative responsibilities.

**Recommendation 1**

*We recommend that the Board and CIO work to address the inherent conflicts caused by the CIO's dual role in IT governance and IT operations. The Board should consider increasing its direction and involvement in the functions of IT governance, allowing governance issues to be communicated by the CIO or the Board rather than VITA; thereby, separating this function from the VITA staff performing IT operations functions.*

*Under this model, the operations function would continue its customer-service orientation to meet agency IT operational needs primarily through enforcing the Northrop Grumman comprehensive agreement. Staff supporting the governance function would support the Board and CIO responsibilities to improve Commonwealth best practices and create efficiencies. The governance function would focus on creating policies and standards and making systems development investment decisions that are in the best interest of the Commonwealth as a whole.*

The final IT Strategic Plan for 2007-2011 approved by the Board on April 6, 2006, appears to have successfully created a Commonwealth-oriented plan, more so than the Spring 2005 plan update. Further, it cites the Council on Virginia's Futures Roadmap as providing the Commonwealth's strategic business direction and provides a link between the identified IT goals and the Roadmap's business objectives.

However, we believe the process could have worked more efficiently and possibly more effectively by staff addressing the alignment of the Commonwealth's IT Strategic Plan with the Roadmap at the beginning of the January strategic planning retreat rather than the end of the strategic planning process.

Additionally, including government business representatives outside of IT as participants would have helped to emphasize the strategic planning best practice of business direction driving IT decisions.

Further, for the 2007-2011 Commonwealth IT Strategic Plan to impact agency IT strategic planning, the Board and the CIO will need to provide leadership to ensure the plan is communicated and emphasized to the agencies. Leadership is also needed to ensure that the Council on Virginia's Future's Roadmap continues to serve as the foundation for the IT strategic plan and that all other strategic planning activities build sequentially off this foundation; that is, the Agency IT Strategic Plan, Prioritized Projects Report, and the Commonwealth Budget.

**Recommendation 2**

*We recommend that the Board and CIO ensure their work continues to supports the Council on Virginia's Future Roadmap. Further, as the Board and CIO execute their Commonwealth IT strategic planning responsibilities, they must ensure staff place the Council on Virginia's Future Roadmap as the guiding principle for the process and understand that their work is intended to support the Commonwealth not just those things over which VITA has control.*

**Recommendation 3**

*Finally, the Board and CIO should develop and execute a communications plan, highlighting the Commonwealth's IT Strategic Plan and how it affects the agencies. By increasing agency awareness and buy in for the plan, the CIO will help the Commonwealth to execute the plan and ensure it has the intended impact on agency IT strategic planning.*

JLARC envisioned that agencies would use the Commonwealth IT Strategic Plan to develop their agency IT strategic plans. Below we discuss the agency strategic planning activities and recommend changes that are necessary to ensure agencies use and build from the Commonwealth's plan.

## Agency IT Strategic Planning

The Code of Virginia requires each agency to develop a strategic plan for its operations and charges the Department of Planning and Budget (Planning and Budget) with developing the guidelines governing the creation of those strategic plans. The Code of Virginia further directs the CIO to develop procedures, in consultation with the Planning and Budget, to integrate IT strategies into the Commonwealth's strategic planning and performance budgeting processes. The strategic plans should be the foundation and justification for agency budget requests.

VITA worked with Planning and Budget in Winter 2005 to integrate IT strategic planning into the agency strategic planning process. Planning and Budget issued their Agency Planning Handbook in May 2005, and it incorporated certain aspects of IT into the strategic planning process. However, we do not believe that the approach succeeded and several factors ultimately affected the integration attempted during 2005.

### *Current Agency Strategic Planning Process*

The first factor that affected the integration of IT into the strategic planning process is an ongoing disconnect that exists within the overall agency strategic planning process. Specifically, while agencies

created and published a document they called a strategic plan in Summer 2005, this document is in reality a performance-based budgeting tool, and nothing more.

The guidance provided within the Planning and Budget Handbook reflects this fact. The Handbook instructs agencies to organize the plan based on the new performance based Appropriation Act funding structures. The Handbook promotes a two-year or biennial horizon to the strategic plan and requires agencies to update the plan based on General Assembly actions. While the plan's organization may be appropriate, strategic planning best practices envisions a time horizon of at least four years. In fact, the Council on Virginia's Future Roadmap time horizon is infinite.

Further, the plans developed under the Handbook provided a direct tie into and support for the Governor's requests for funding. This approach confuses performance budgeting with strategic planning and makes short-term funding requirements a priority over long-term needs. In fact, this approach encourages agencies to ignore long-term needs in favor of short term funding requirements.

The agency strategic plan for the Department of Accounts provides a good example of this disconnect. Given the significant amount of attention placed on recent public-private partnership proposals to replace the Commonwealth's administrative systems, one would have expected to see the need to replace the current financial system, CARS, identified as a specific need within Accounts' strategic plan. However, given its size and the level of funding required to complete such a project, Accounts did not include a CARS replacement as one of their strategic planning initiatives because they did not believe the project would receive funding. Yet, this need is exactly what an effective strategic plan would highlight, regardless of whether money was available.

Strategic planning should provide a long-term plan for business operations. If the Planning and Budget documents were truly long-term strategic plans, agencies could stabilize their IT needs rather than changing their IT needs annually if they believe the Governor will fund them. Since VITA has historically relied on the biennial agency plans to compile and prioritize IT projects, significant changes to priorities occur annually as the budget documents change.

**Recommendation 4**

*As agencies refresh their strategic plans and the Board finalizes the Commonwealth's IT Strategic Plan, we recommend that the Board, CIO, Secretaries of Finance and Technology, and the Council on Virginia's Future, direct VITA and Planning and Budget staff to work together to identify ways to improve the agency strategic planning and IT investment decision process. They should address the need for long-term focus within strategic planning and identify ways to connect a long-term strategic plan with the biennial performance budget needs. Further, this process should not ignore long-term needs, even when short term funding plans cannot address the need.*

The second factor that affected the unsuccessful integration of IT into the strategic planning process was the IT summary section included in the Planning and Budget Handbook. While the Handbook introduced a new IT summary section to bring the concept of IT more into the body of the agency strategic plan, not all agencies understood or used this section as intended. VITA staff believed the information that agencies would provide in this section would justify agency IT initiatives and provide the link between agency business goals and their system development requests. Most of the agency plans that we and VITA staff reviewed were not robust enough to provide this link.

The third factor that affected the unsuccessful integration of IT into the strategic planning process was that required due dates for agencies to complete their strategic planning submissions to Planning and Budget and VITA were incompatible. To have sufficient time to analyze and prioritize projects for the Board priority project list, VITA's Project Management Division (Division) required agencies to identify and report their major IT projects by May 31st. Planning and Budget did not require agencies to submit their strategic business plan and budget requests until July 15th.

This incompatible timing de-emphasized the link between an agency strategic business plan and IT strategic plan. Strategic Planning best practices state business needs and goals should drive IT decisions, yet agencies needed to make IT decisions before they fully defined their business needs and goals. Further, by requiring project information before agencies completed their strategic plans, agencies did not provide the Division with quality information. Agencies poorly defined their major projects or did not identify them in time. This in turn impacted the quality of the priority project report as well as the Board and CIO's awareness of agency projects.

**Recommendation 5**

*VITA and Planning and Budget must ensure agencies understand how their individual IT strategic plans support the Commonwealth's Strategic Plan and likewise how their proposed IT projects should support the Commonwealth's overall IT goals and objectives. VITA and Planning and Budget should consider incorporating in the Handbook a section that addresses this alignment overall, describing how the Council on Virginia's Future's Roadmap drives to the Commonwealth's IT Strategic Plan and how agency plans should align with both. Additionally, VITA and Planning and Budget should revise the Handbook instructions to improve the IT summary section and the IT strategic plan appendix.*

**Recommendation 6**

*VITA should consider changing their current deadline for receiving agency IT projects to better align with the agency's strategic planning cycle. If VITA and the Board implement our recommendations relative to prioritizing projects made later in this report, the process should be more efficient and require less lead-time, allowing this deadline to change.*

## Project Prioritization and Funding

JLARC's report acknowledged that some worthy projects never receive funding while agencies with larger operating budgets can often afford to develop systems without making a specific budget request. By eliminating agency or secretarial bias and ranking projects relative to their importance to the Commonwealth, JLARC felt that the Commonwealth could better use its limited financial resources. JLARC proposed a process for an unbiased Board to rank projects across the Commonwealth from highest to lowest priority. Then, appropriations could focus on funding the highest priority projects first.

The key to quality ranking is having an understanding of the Commonwealth's business priorities and ensuring strategic planning focuses efforts on meeting those priorities as noted in the JLARC model. Therefore, the Commonwealth's IT Strategic Plan must stay aligned with the Council on Virginia's Future's Roadmap and agencies must align their strategic plans as well. As a result, VITA will be able to rank IT initiatives proposed in the agency strategic plans and consider initiatives across the Commonwealth. The next section will discuss the prioritization process further.

### *Current Project Prioritization Process*

The Code of Virginia requires that the Board annually submit of a list of recommended technology investment projects and priorities for funding such projects to the Governor and the General Assembly by September 1. The Board has met the deadline each year for submitting their priority project report, also referred to as the RTIP, but this report has not met the legislative intent as envisioned by JLARC.

As discussed earlier, the priority report is the bi-product of agency IT strategic plans and we have two concerns that emerge. First, the prioritized projects do not support Commonwealth goals because agencies have not prepared IT strategic plans and related projects using the Commonwealth's IT Strategic Plan as a foundation. Second, agency IT strategic plans are not strategic plans at all, but are instead performance budget documents that support agency IT budgets for the biennium. This results in unfunded long-term needs that never make it on the priority report.

To meet the legislative intent, the priority report should represent long-term project needs that help achieve the Commonwealth's IT Strategic Plan. If the report could achieve this result, the Governor, General Assembly, CIO and Board could use the priority report to support funding priorities. However, currently the report is only a snapshot of projects that agencies believe the Governor and General Assembly will fund and only looks out two years into the future.

We recommended earlier that the Board, CIO, and Secretaries of Finance and Technology direct their staff to work together to improve agency understanding and use of the Commonwealth's IT Strategic Plan as a foundation for developing their individual plans. We believe there is also a significant amount of work that Planning and Budget must do to make agency plans represent strategic plans rather than only budget support documents. If these groups succeed and linking these process, only then will the priority report will be useful and effective as a budgeting tool.

### *The Priority Project Report*

The current priority report format is not conducive for decision-making. We found areas requiring additional information and layout improvements that could make the report easier to understand. We have verbally shared many of our recommendations with the Division and the following are some of those comments.

- Since VITA prepares the priority report from agency IT strategic plans the report only includes projects that the agency would like to have funded in the current biennium. As the Commonwealth improves strategic planning to look beyond the current biennium and focus on Commonwealth goals, we believe the priority report should also incorporate a long-term focus. Decision makers would benefit from having estimated annual project costs over the project's life rather than only estimates for the next biennium. This would ensure that decision makers are aware of long term funding needs before starting a project that they may not be able to fund for in future years. This approach is similar to the Planning and Budget's Six-Year Capital Outlay Plan. This model reports the current year costs and each subsequent year for ten years.

- The current report only prioritizes new projects and includes a separate list of those projects previously prioritized and in need of continued funding. We believe the report should prioritize both new and ongoing projects in one list and show their annual funding needs. This would provide decision makers with an understanding of all funding needs before committing to start new projects. It would also give

decision makers a perspective of how active projects rank in comparison to new priorities and whether an active project should be suspended in order to fund a higher priority project.

- The 2005 priority report contains more information than required by the Code of Virginia, such as unnecessary listings and excess narrative. This information takes one staff person approximately 5 months to gather, prepare, format, and proofread, taking this staff away from project monitoring and oversight responsibilities. Recently, the Division has been considering how to reduce the amount of data within the next priority report, but expects to continue to include the supporting information on the web. Although this will decrease the length of a printed report, gathering the information to prepare it for the web will continue to require the same level of Division staff resources.

**Recommendation 7**

*We recommend that the Board and Division revise the priority project report to present estimated annual project costs over the project's life to better inform decision makers of future funding needs. The Division should consider using Planning and Budget's Six-Year Capital Outlay Plan as its reporting model.*

**Recommendation 8**

*In addition, consideration should also include simplifying the report to include one prioritized list of both active and new projects recommended for funding. We also recommend that the Board consider the cost-benefit of including, either in the report or on the web, the additional lists and narratives that are not Code of Virginia required. Using these staff resources elsewhere could be more effective in other areas of the Division, such as project monitoring and oversight.*

### *Commonwealth Budget*

The priority report has not had the desired impact of driving technology investment decisions by the Governor or the General Assembly. We continue to find projects not in the priority report that receive funding and other high priority projects that receive no money.

The Board has acknowledged that it has had minimal impact on the funding of IT projects and set a goal for the priority report to become the primary driver for technology investment decisions in the 2007 budget process. While we commend the Board on setting this goal, the Governor and General Assembly are ultimately responsible for and have authority over the Commonwealth's budget.

To realize this goal the Board must implement our earlier recommendations to affect change in the Commonwealth's strategic planning process. Unless the Planning and Budget requires agencies to develop long-term strategic plans rather than budget documents, the priority report will continue to contain inadequate information. As a result, the priority report will continue to have no impact on funding decisions.

**Recommendation 9**

*We recommend the Board initiate communication with the Governor and General Assembly to determine how the priority report can become a useful decision making tool. If the Board cannot make the report useful to the Governor and General Assembly for making funding decisions, the effort involved in prioritizing these projects is futile.*

*If the Board cannot adopt the report to meet the needs of the Governor and General Assembly, the Board should consider recommending that the General Assembly eliminate the priority reporting requirement from the Code of Virginia.*

***Technology Funding Sources***

In addition to the priority report, JLARC recommended and the Code of Virginia provides for a Technology Fund to pay for systems development projects. JLARC suggested that in lieu of budgeting funds directly to agencies, the Governor and General Assembly could appropriate moneys to the Technology Fund and the Board allocate the funds to priority projects.

Early in the creation of VITA, the Secretary of Technology emphasized that VITA would generate savings that could be deposited to the Technology Fund to pay for IT projects. We believe the early association between savings and the Fund resulted in many viewing the Fund as a viable method to pay for projects, but only if VITA achieved savings. In reality, there are other alternatives to provide money into the Technology Fund.

As one alternative, the Governor and General Assembly could provide appropriations to the Fund and budget the related projects in a manner similar to the current capital outlay budget process. In another alternative, the Governor could authorize Planning and Budget to transfer appropriations from individual agency budgets to the Technology Fund. In both alternatives, the Board could authorize the disbursement of these funds to pay for agency projects after the agency demonstrates specific requirements, such as a sound business case.

JLARC envisioned the Technology Fund as providing a reliable funding source and enabling the priority project report to become the driver for technology investment decisions. To realize the full benefit of strategic planning and project prioritization, the Board should continue to pursue options, such as the Technology Fund, that would provide a reliable funding source for technology initiatives.

**Recommendation 10**

*The Board, CIO, Secretary of Finance and Secretary of Technology should direct VITA staff and Planning and Budget staff to work together to evaluate and report back to them on alternative funding mechanisms for IT projects. VITA and Planning and Budget should consider the 2003 JLARC recommendations, which envisioned a capital funding structure using bonds or other debt instruments, the appropriation of money directly to a central technology fund, a revolving loan fund, or a combination of alternatives. The purpose of exploring funding alternatives is to provide reliable funding for projects and enabling the priority listing to become the driver of technology investment decisions in the Commonwealth.*

## SECTION II - PROJECT MANAGEMENT

### Project Monitoring and Oversight

JLARC's report had envisioned a Division, comprised of project management specialists, which would oversee, support, and assist in the planning of information systems development for all agencies and across the Commonwealth. These specialists would work closely with agencies to understand their mission, goals, constraints, funding, and objectives. They would assist agencies but also provide unbiased recommendations and information to the CIO and Board regarding project requests and activities at agencies.

Overall, the Division has established an organizational structure, hired some project management specialists, developed a project manager training and testing program, and issued an extensive Project Management Standard. The Division has been responsible for reviewing agency IT strategic plans, gathering project information and preparing the priority project report, recommending projects for approval by the CIO and Board, and providing limited monitoring activities. Below we will review various Division activities relative to monitoring and oversight where we believe PMD has not fully met the legislative intent provided by JLARC.

#### *Assistance and Support of IT Projects*

The Division is required to provide ongoing assistance and support to state agencies and public institutions of higher education in the development of IT projects. Relative to this requirement, JLARC suggests that having project management specialists assigned to work on specific secretariats would increase their understanding of their assigned secretariat's business needs. They would be able to identify quickly whether proposed projects meet the business needs, and quickly identify and report ongoing assessments to the Board on a regular basis. JLARC envisioned that the Division could assist agencies in all facets of systems development including planning activities, the development of business cases, and assisting with contract negotiation.

Organizationally the Division has one director, one manager, and six project management specialists (specialist). The manager performs a supervisory function in addition to monitoring some projects. The specialists work on projects based on their backgrounds, other tasks assigned, agency track records, and the volume, size, and complexity of projects within the Secretariat. In addition to project monitoring and oversight, specialists also work on Division projects such as the developing policies and procedures, reviewing agency budget requests, preparing reports for Board meetings, and developing the annual priority project report, known as the RTIP.

We interviewed the Division manager and three specialists regarding their weekly responsibilities and found that in an average week they are able to spend about 50 percent of their time actively overseeing and monitoring. Specialists have other activities they perform, such as preparing Board reports, but we believe these activities have affected the specialist's time to work with and understand agencies as envisioned by JLARC.

In their limited time, one way the specialists provide oversight and monitoring is by reviewing documents that agencies prepare. The specialists generally provide a high-level review of those documents for reasonableness and consistency. We found that except for a few Division practices, each specialist monitors projects differently. For example, some specialists actively attend project team meetings at agencies while others work more from document reviews. Since the specialists are looking for different things, their reviews are subjective and based on the specialists experience and background.

The Division has recognized the problems caused by not having written procedures for how specialists conduct their monitoring and oversight. They have paid a vendor about $100,000 to develop and document Division policies, procedures, and review methodologies in a Project Management Oversight Program Guideline. The Division is currently reviewing the draft Guideline and expects to have it fully implemented by July 2006, contingent upon increased staffing levels, due to significantly increased procedures.

The Division chose to contract out the Guideline's development rather than create it in-house due to existing staffing shortages. In our 2004 VITA audit report, we found that the Division hired consultants to perform independent verification and validation (IV&V) reviews of projects in lieu of hiring full-time Division staff that could have completed the reviews much cheaper. At that time, we concluded that the Division was not meeting their monitoring and oversight responsibilities and recommended that they focus on hiring more full-time staff to perform work rather than relying on more costly consultants. We continue to make this recommendation.

**Recommendation 11**

*We again recommend that the Board and CIO authorize and that the Division fill vacant full-time positions as a more cost effective approach to hiring vendors. Not only would this provide more resources on a daily basis, it would reduce costs to the agencies that are eventually paying for these services.*

*Full-time specialists could develop on-going working relationships with the agencies throughout the project development life-cycle, which is generally several years. Having these specialists in-house would make them available to the CIO and the Board at all times to give independent updates on the project and recommend project suspension if there were project management concerns.*

Currently, much of what the specialists do to monitor projects comes from agency self-reported information as required by the Project Management Standard. While their reviews look for some items such as schedule variances, the specialists generally do not review and question the quality and accuracy of the self-reported information.

For example, while the specialist may compare the current project schedule to the baseline schedule, they generally do not review the schedule in detail to determine that it includes all tasks that they believe are necessary to successfully complete the project. In another example, the specialist may monitor current project expenses to the baseline budget, but do not determine that the agency is properly tracking and including all project costs in their reported expenses.

If implemented properly, the Project Management Oversight Program Guideline should help to provide guidance and consistency to specialists when monitoring IT projects. It should also establish more rigor and force specialists to be more active in their projects.

***Reporting on Project Status***

Periodically the Division summarizes the status of IT projects in a report that the Board requested. The Project Status Report begins primarily from information contained in the Division's Dashboard, which is a web-based application where agencies must self-report their project's status. Specialists review the self-reported data, but rely primarily on it unless there is clear and convincing evidence that it is wrong. Before the Division completes the status report, they meet with APA staff, who provide feedback. Although the

Division does not change their report based on the APA meetings, they do indicate APA comments on the report so the Board will understand when differences of opinion exist. We believe this unwillingness to modifying the self-reported status reflects a weakness in the Division's monitoring and oversight program.

The Division has stated on several occasions that the APA and specialists have different opinions on the status of projects because both groups serve different roles in the process. The Division feels that as independent auditors, the APA, can express their opinion on the quality of project management or on the likelihood that a project will succeed or fail. However, as a division of VITA, the Project Management Division must be customer service oriented and prefer to work with agencies to agree when a project is in trouble. The Division's customer service approach is further complicated, in their mind, by the fact that as an internal service fund agencies pay for the Division's services.

The Division has carried this perception into their draft Project Management Oversight program Guideline they plan to implement. It describes the IT oversight process as being a beneficial service and not as an audit process focused on identifying problems and assigning blame. JLARC's report envisioned that the specialist would be able to quickly identify and report project status assessments to the Board on a regular basis, identifying those projects at risk for failure. Meeting this legislative expectation is in conflict with the Division's view of their role.

**Recommendation 12**

*Earlier we recommended that the Board and CIO fix the inherent conflicts caused by VITA's governance and operation roles. The Project Management Division is one example where this conflict has affected their ability to effectively perform their work and report unbiased opinions to the Board regarding the status of their project. After the Board and CIO address these conflicts, we recommend that the CIO meet with the Project Management Division as well as other VITA divisions affected by the separation of governance and operations to ensure they understand their purpose, responsibilities, and how the changes impact their work.*

*We believe the Division can assist agencies but also report their opinions on the status of projects successfully. The fact that agencies pay for services does not mean that the Division must be customer focused. Agencies often pay for security vulnerability assessments and audits, activities that are not generally customer focused but rather standards and best practice focused.*

***Review, Recommendation, and Approval of IT Projects***

The Division is required to assign project management specialists to review and recommend IT proposals based on criteria the Board defined using references in the Code of Virginia, as listed below:

i) degree to which the project is consistent with the Commonwealth's overall strategic plan;
ii) technical feasibility of the project;
iii) benefits to the Commonwealth of the project, including customer service improvements;
iv) risks associated with the project;
v) continued funding requirements; and
vi) past performance by the agency on other projects.

JLARC suggested that by having project management specialists assist in the project approval process, they could combine technical expertise with an understanding of their assigned secretariat's business needs, allowing for more informed decision-making.

The Division is also required to implement the approval process for IT projects. Relative to this requirement, JLARC suggested that the CIO and the Board approve all projects for planning and development based on criteria. The reason for this criteria and process is to ensure projects have a strong business case and to increase project visibility.

Generally, the Division has used criteria to evaluate projects. However, the Code of Virginia's first evaluation criterion requires that the project support the Commonwealth's IT Strategic Plan. As noted earlier in the report, specialists cannot effectively evaluate this criterion because the agency IT strategic plans are not based on a larger Commonwealth IT Strategic Plan, which is driven by Commonwealth-wide business objectives. We provide a recommendation earlier in the report that we believe will fix this issue in the future.

To effectively evaluate the remaining criteria, the Division would need a full staff of project management specialists who are actively involved with secretariats and agencies. These specialists would need to possess an understanding of the Commonwealth's strategic direction, an in-depth understanding of agency missions and needs, an appreciation of other similar agency needs where enterprise opportunities may exists, how the agency is funded, and inherent risks both in agency operations and in systems development.

Again, this year, the Division continues to be understaffed and has a number of vacant positions. In addition, the Division has experienced turnover, which causes them to shift resources and require the specialists to work with agencies and projects that are unfamiliar to them. Finally, specialists spend a significant amount of time preparing reports, such as the priority project report and project status report and we believe there are opportunities to make these administrative tasks more efficient.

The consensus among the specialists is that each could do a more thorough job of keeping on top of issues and trends affecting agencies if they had more time to do so. We are concerned that staffing shortages and turnover have contributed to specialist's inability to gain an in-depth understanding of their assigned agencies and their system needs and abilities. If specialists are not working closely with agencies, secretaries, and projects, the Division will not achieve JLARC's vision.

We are concerned that specialists have relied heavily on agency self-reported data and are not knowledgeable enough to question agency project documents or deny agency system request. As an example, specialists rely on agencies to identify and execute opportunities to collaborate with other agencies or create enterprise systems. Instead, we believe that the specialists should have enough awareness to identify these opportunities and push them as an initiative. We are also concerned that specialists cannot effectively identify when to recommend that the CIO modify, terminate, or suspend a project because they may not be sufficiently involved.

By relying on agency self-reported data, specialists may miss entire projects that agencies fail to report. During the year, we have found several agencies that are actively pursuing projects without telling the Division or have broken the project into small modules to avoid the Divisions thresholds for review. In all instances, we have notified the Division, but we believe this is further justification for why they must actively monitor their agencies projects and understand their business activities.

Potentially the Project Management Oversight Guideline that the Division hopes to implement in July 2006 will cause specialists to be more involved with their agencies and projects. However, the Division does not plan to fully implement the Guideline until they hire more staff.

**Recommendation 13**

*In addition to fully staffing vacant specialist positions as recommended earlier, we also recommend that the Division examine their administrative tasks, ensure they are having the desired impact, and find ways to make them more efficient or drop them altogether.*

*To fulfill their purpose of improving project management and identify enterprise and collaborative opportunities to make the Commonwealth more efficient, they cannot continue to operate by reviewing self-reported data. We recommend that the Division take an active role monitoring their projects and independently verify and assess agency self-reported data. The Division must encourage their specialist on how to challenge agencies on whether enterprise and collaborative opportunities exist rather than relying on agencies to indicate whether or not they can work together.*

We reviewed four projects that received planning and development approval during the year for the purpose of ensuring agencies turned in required documentation and that the specialists followed standard project planning and development approval processes. To this end, we requested and reviewed all available project documents, any evidence that the specialist reviewed the documents, and all available letters and emails between the agency project manager and the specialist.

Overall, we did not find sufficient evidence of the specialists review and assessment of project documents. The Division has no procedures that require the creation and retention of review notes and important communications, which makes it difficult to understand the history of the project, any questions the Division may have raised or risks they may have identified.

**Recommendation 14**

*We recommend that the Division's policies and procedures require that specialists retain project files, whether hardcopy or electronic, of all agency project documents, review notes, and agency communications.*

*Maintaining organized project files and notes will ensure a smooth transition and allow any specialist to get up to speed quickly should a specialist resign or the project be otherwise assigned to a different specialist.*

***Project Suspension and Termination Procedures***

The CIO has the authority in the Code of Virginia to modify or suspend major IT projects as the result of periodic reviews. Additionally, the CIO may recommend to the Board the termination of projects.

We found that the Division has no written procedures and criteria that they use to recommend that the CIO modify, suspend or terminate a project. Since specialists provide their insight to the CIO regarding the status of projects and also provide recommendations to the CIO if a change in status is necessary, we believe they should document their criteria and process.

**Recommendation 15**

*We recommend that the Division establish written criteria and procedures for recommending that the CIO modify, suspend or terminate a project. Having written criteria and procedures will provide specialists with a baseline understanding of project related issues that could result in such a recommendation.*

## SECTION III - SECURITY

### Objective and Methodology

Our audit of VITA had two overall objectives:

- to determine that VITA has fulfilled their statutory responsibilities and legislative intent relative to security and

- to determine that VITA has adequately described their security services and therefore has the documentation of the services for transfer to Northrop Grumman later this year.

Our audit test work focused on the legislative intent behind the Code of Virginia sections applicable to VITA Security as well as provided a review of security over critical infrastructure and operating systems operated by VITA for certain Commonwealth agencies and the IT governance role of VITA. Additionally, we performed a follow-up on prior year findings related to the 2004 SAS 70 and the 2005 Review of Security Controls audits.

We approached our audit by reviewing applicable sections of the Code of Virginia, interviewing security and customer services employees, and examining standards and documents to gain an understanding of policies, procedures, and operating activities over VITA's security functions. We also reviewed planning activities to determine VITA's readiness to transfer operational security functions to Northrop Grumman.

### History and Background

The legislation creating VITA called for the CIO to be responsible for the following areas:

1. develop policies, procedures and standards for performing security audits of government databases and data communications; and designating a government entity to oversee, plan, and coordinate the conduct of these audits;

2. receive reports of security incidents and take action as necessary convenient or desirable;

3. develop policies, procedures and standards for assessing security risks and determining the appropriate measures; and

4. develop policies and procedures for managing IT by state agencies and institutions, and developing statewide technical and data standards to promote efficiency and uniformity.

The CIO assigned the responsibility for the first three items to Security Services. The final task will require both Security Services and VITA customer service operations involvement to complete.

The Board-adopted Commonwealth IT strategic plan paints the picture of a Commonwealth-wide "to-be" environment for security, including the development of a statewide IT security program. This program should facilitate a consistent level of IT security across the Commonwealth to protect IT assets, attain high-level IT security skills, communicate IT security alerts and best practices, and respond to and recover from cyber attacks.

### *Changes under Northrop Grumman Agreement*

With the creation of VITA as an agency, VITA assumed responsibility for IT operations, including ownership of all IT assets and management of the operations of all IT infrastructure components, such as desktops, servers, mainframes, and routers, for customer agencies that VITA serves. These agencies consist of the Executive Branch agencies; excluding the Colleges and Universities. Collectively, we will reference these as VITA IT infrastructure throughout this section of the report. Beyond these operational duties, the Code of Virginia requires VITA to provide IT security governance to all Commonwealth agencies and institutions.

We have recommended previously in Section I that the CIO and Board consider separating VITA's IT governance and IT operations to help VITA staff understand their role and improve the way they operate. Relative to security, VITA has organizationally separated the security governance and operational roles. However, we believe that this distinction may not be discernible outside of VITA central office but by turning over IT security operations to Northrop Grumman on July 1, 2006 this distinction should be clearer.

Under the agreement, Northrop Grumman will take responsibility for IT operations, own all IT assets as refreshed over the next three years, and manage the operations of all IT infrastructure components, such as desktops, servers, mainframes, and routers for customer agencies that VITA serves. The majority of current VITA staff either will become Northrop Grumman employees or will remain VITA employees but Northrop Grumman will provide technical direction to these employees. VITA, however, will retain responsibility for IT security governance for the Commonwealth as well as for the VITA IT infrastructure to include oversight of IT security functions performed by Northrop Grumman.

While we believe this arrangement can be successful, it is critical that VITA improve their IT security governance role. Starting July 1st, VITA must give Northrop Grumman clear direction regarding needed security controls over VITA IT infrastructure, which Northrop Grumman must implement as part of operations. If VITA does not provide adequate information, there is a risk that the controls that Northrop Grumman implements will not provide adequate security to protect VITA IT infrastructure.

### *Status of VITA IT Infrastructure Security*

We continue to have concerns about VITA's ability to identify and meet the security needs for their IT infrastructure as they continue to operate in an agency-focused rather than Commonwealth-focused approach to security. Additionally, we found that VITA has yet to meet their security responsibilities as outlined in the Code of Virginia.

VITA's responsibility to act on behalf of the Commonwealth will become critical with the transition to Northrop Grumman. However, VITA has yet to accomplish some important strategies, as detailed throughout this report, that will allow VITA to communicate the security needs of their IT infrastructure to Northrop Grumman. VITA cannot continue to function by focusing on individual agency's environment or division projects, but must instead work together for the benefit of IT security needs of the Commonwealth and must accomplish their strategies.

The following outlines additional specific details that support our overall concern about the status of IT security.

**VITA Security Services**

The Code of Virginia states that the CIO shall direct the development of policies, procedures, and standards for assessing security risks and determining the appropriate security measures. The Code of Virginia also requires VITA to develop and adopt policies, standards, and guidelines for managing IT by state agencies and institutions; and to develop statewide technical and data standards for IT systems to promote efficiency and uniformity.

We reviewed the Security Services section of VITA's agency strategic plan, as submitted to Planning and Budget. As discussed in Section I of this report, agency strategic plans serve primarily as a budgetary tool that supports biennial budget requests and do not provide a long-term time-frame necessary to serve as a true strategic plan. However, in light of no other strategic plan, we used this one for our audit. Relative to this plan, we found that although it contained security strategies such as developing statewide policies and procedures, it did not contain the detailed plans necessary to achieve these strategies, such as responsible parties, deadlines, and specific actions. While we recognize that this plan is effective through 2008, giving VITA some time remaining to address the strategies, we believe VITA should finalize certain strategies such as developing security standards that are customized for customer agencies before the transition to Northrop Grumman.

As discussed above, Security Services does not have a detailed business plan that describes what work they need to do, when they must do the work, and who must do it, in order to develop their policies, procedures, and standards. While lacking a business plan, Security Services has taken on a number of initiatives this past year such as drafting a revised security standard, a matrix of security roles and responsibilities, and templates to gather agency information security needs.

For example, VITA's memorandum of understanding that establishes security relationships with the agencies it serves contains a security matrix appendix that specifies VITA responsibilities and customer agency responsibilities. Security Services has worked on an initiative to update the security matrix to clarify specific responsibilities and their due date. Simultaneously, VITA was revising their security standard. To comply with the standard, VITA and customer agencies must share information and we believe the security matrix should serve as the appropriate tool to identify the required information and responsible party. However, since the security matrix update and security standard initiatives were not consistently coordinated initiatives, a documented crosswalk between the draft standard and the security roles and responsibilities matrix was not completed.

We are concerned because Security Services does not have a written, detailed plan that outlines all their initiatives, priorities, deadlines, and responsible parties. Without a detailed plan, we cannot determine:

- how individual initiatives fit into overall VITA security objectives;
- that VITA's management understands and has approved the overall approach;
- how Security Services holds staff accountable for deadlines; and
- how Security Services may conclude that they have issued or have plans to issue standards that promote efficiency and uniformity over all IT security functions.

As a result, Security Services is at risk of working on initiatives that do not support their business objectives. In addition, Security Services may perform work that is unnecessary while not addressing other important needs.

**Recommendation 16**

*We recommend that Security Services detail, document, and approve an operating plan to direct their daily and long-term business decisions. Such a document should also consider how initiatives relate and ensure that responsible parties coordinate and that deadlines work together to support an overall goal and those deadlines are pertinent to the needs of customer agencies and the Commonwealth. We also recommend that VITA management consider how the transition to Northrop Grumman will affect Security Services' role in IT security governance. Such analysis should include the necessary organizational changes and reflect those changes in Security Services operating plan.*

## Commonwealth Technology Standards

Security Services has struggled to finalize security standards timely. For example, Security Services has been working for over a year to create a revised Commonwealth of Virginia security standard that improves upon the roles and responsibilities of the existing Commonwealth of Virginia security standard, COV ITRM SEC 2001-01.1. We reviewed and participated in meetings with VITA and other agencies to discuss their first draft of the revised standard. Generally, the participants agreed that the first draft was inflexible, overwhelming, and needed significant revisions. Security Services has continued to revise the draft, taking it through several iterations. They expect to issue a final standard by July 2006.

In another example, Security Services has been working for over a year to create a Database Security Audit Standard. Again, we have reviewed and participated in meetings to discuss drafts of this standard and Security Services has been slow to get it finalized as it is dependent on the Security Standard.

**Recommendation 17**

*We recommend that Security Services develop a defined timeline for the finalization and distribution of all outstanding standards to move VITA in becoming compliant with the Code of Virginia and VITA's agency strategic plan. These standards include, but are not limited to, the revised IT security standard and the security audit standard. In addition, we recommend that Security Services include the development of new policies and the updating of existing policies as part of their detailed operating plan.*

### *Universally Applied Procedures*

VITA continues to make efforts to bring its operational areas into compliance with security best practices and standards but it has failed to adequately develop, distribute, and enforce uniform procedures to protect the technology infrastructure owned by VITA.

For granting administrator access to mainframes in the Richmond Plaza data center, Computer Services grants administrator access to their employees for performing system maintenance on the mainframe computers; however, we found that Computer Services does not have written procedures that outline administrator access monitoring processes. For example, while Computer Services periodically monitors administrator access, they have no written procedures that outline responsible party, deadline, and documentation requirements for this process. In another example, Computer Services does not have written procedures that require a periodic review of users with administrator access to find those that no longer need such access. Without written procedures, VITA management cannot understand and approve the Computer Services' management of administrator access nor can they hold staff accountable. The absence of such

procedures also prevents Customer Services from implementing consistent procedures to its customer agencies.

In another example, VITA has implemented appropriate hardware and software change management procedures relative to their Richmond Plaza data center that address prior year audit findings. However, Customer Services has not applied these procedures as implemented in the data center to the customer agencies it serves.

Our testing of administrator access and change management was limited to the Richmond Plaza data center. However, Customer Services has not yet consistently documented the procedures used in the data center nor have they universally applied their data center procedures to the customer agencies. As a result, the procedures that VITA staff currently follows for customer agencies are not uniform and primarily follow the procedures the agency had when they controlled their own infrastructure. This lack of uniformity creates inefficiencies since VITA staff must operate against different procedures. It also creates risk to VITA's IT infrastructure since some agencies may have inadequate procedures that jeopardize the whole.

Soon the responsibility for monitoring, documenting, and approving hardware and software changes will transfer to Northrop Grumman. Likewise, Northrop Grumman will be responsible for granting their employees administrator access and monitoring when access is no longer appropriate. In response to hardware and software changes, VITA and Northrop Grumman have initiated a joint project to develop a procedures manual, including change management, which will also include the Commonwealth's infrastructure beyond the Richmond Plaza data center. The project completion date is 90 days after transition. However, until then, Northrop Grumman will rely upon the procedures already in place at VITA.

**Recommendation 18**

*We recommend that Service Management Organization adopt uniform procedures that apply to all aspects of VITA's infrastructure, not only the Richmond Plaza data center. The procedures should comply with the revised security standard, be uniformly applied across VITA's IT infrastructure, and provide sufficient details so that outside parties, such as Northrop Grumman, can clearly understand the requirements. If Service Management Organization finds that an agency needs an exemption to the uniform procedures, they should enforce their existing exception policy and require that agencies and VITA document and approve the exception.*

***Continuity of Operations Plan (COOP)***

VITA does not have a comprehensive and adequate plan of action to restore VITA's critical IT infrastructure should a natural or man-made disaster occur affecting the Commonwealth. We found that VITA has a formal plan for the infrastructure components within the Richmond Plaza data center but our audits of various agencies have found that many agency plans are outdated or incomplete. Since VITA is now responsible for the infrastructure components of the agencies it serves, including those in the Richmond Plaza data center, they need to develop a comprehensive plan.

VITA began separate initiatives relating to the business impact analysis, risk assessment, and disaster recovery plan components of a COOP, one long-term and one short-term. However, the short term initiative places reliance on agency disaster recovery plans that, as noted above, may be outdated or incomplete.

- In January 2006, Security Services began creating templates that will provide guidance to customer agencies for completing a comprehensive business impact analysis and risk assessment document. Security Services continues to work on the draft documents and coordinate with the Virginia Department of Emergency Management. Therefore, the customer agencies' business impact analysis and risk assessments may not be consistent and comprehensive according to VITA's IT governance. Security Services began this initiative, as part of their IT governance role. Therefore, this initiative does not directly support VITA's efforts to develop a disaster recovery plan except VITA may later choose to use these guidance templates in their effort.

- Although Security Services has not issued the guidance templates described above, they proceeded with the creation and distribution of an information security template in March 2006. Security Services required customer agencies to complete this template for their high-risk systems and data as defined by the agencies' business impact analysis and risk assessment documents. Customer Services is using this information gathering process to assess whether adequate security controls are in place so that VITA can provide assurance to customer agencies. The need for VITA to develop a comprehensive COOP is not directly related to the information security template. VITA will begin this review process in May 2006 and, ideally, should complete the analysis of these templates before the transition. VITA has responded that this will be an ongoing effort with Northrop Grumman beyond the transition date.

- Independent of the information security template process described above, Customer Services established a phased approach in November 2005 to collect and analyze the disaster recovery plan for the agencies served by VITA. VITA has collected disaster recovery plans from all agencies it serves and has begun analysis of these plans based on regions. VITA will consolidate the regional plans into a VITA IT infrastructure disaster recovery plan that they will give to Northrop Grumman. Like the template, this plan has not sufficiently progressed to be complete by the transition to Northrop Grumman and VITA does not expect to complete a comprehensive disaster recovery plan compiled in accordance with standards until early 2008. The second phase of this initiative will have VITA revising their business impact analysis, risk assessment, disaster recovery plan and overall continuity of operations plan to include the entire infrastructure.

Best practices and existing VITA standards suggest that entities should first prepare their business impact analysis and risk assessment to determine what systems are most critical. The disaster recovery plan then supports the restoration of the most critical systems. However, VITA's current approach of collecting disaster recovery plans from customer agencies, which may not be based on a complete and accurate business impact analysis and risk assessment, does not follow their own standard. While it is the responsibility of customer agencies to identify their critical systems and necessary security requirements, VITA must collect and assess this information in order to develop a restoration process for VITA infrastructure collectively and not by individual customer agencies. Because VITA was slow to address their need to develop a disaster recovery plan for VITA infrastructure, VITA had to establish a data collection method that did not enable them to follow their own best practices. We understand that VITA used their current approach because of the need to identify customer agency expectations and to develop plans to respond to those expectations; however, they need to develop a long-term methodology that meets existing VITA standards and ensures they mitigate the Commonwealth's risk.

**Recommendation 19**

*We recommend that VITA continue their current effort to document as much COOP information as possible and subsequently provide such information to Northrop Grumman regarding the recovery of VITA's IT infrastructure in the event of a disaster. However, we further recommend that VITA begin preparing a detailed, written plan to complete a COOP in accordance with existing VITA standards.*

***Security Incident Response***

The Code of Virginia requires that the CIO shall promptly receive reports from executive branch departments and shall take such actions as are necessary, convenient, or desirable to ensure the security of the Commonwealth's databases and data communications. The Code of Virginia also requires the agency head of every department in the executive branch to report within 24 hours the following:

- All known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws.

- Other incidents compromising the security of the Commonwealth's IT systems have the potential to cause major disruption to normal agency activities.

VITA created a phased approach to meeting the Code of Virginia requirements for incident reporting. In January 2005, Phase I began when VITA created a separate group within Security Services to be known as Incident Management Response Team (response team). The response team is a group of professionals trained in security incident handling with a wide range of specialized technical training. Over this past year, the response team properly identified and defined the types of security events or incidents that agencies must report and continues to communicate this information to the agencies through emails, internet postings, and security meetings. The response team also receives security alerts from security organizations and vendors. The response team reacts to each alert or agency report on a case-by-case basis depending on the criticality and the perceived threat to the Commonwealth.

However, Security Services has no written procedures to describe the actions the response team must perform to address and respond to the security reports or alerts. Such procedures should include guidance for threat evaluation, research and response deadlines, and methods to communicate findings to the reporting agency and other agencies, as needed.

Phase II of the incident management program includes implementing an intrusion detection and prevention system framework for the VITA IT infrastructure. This phase will not begin until June 2006 but this date is dependent on the planned receipt of service fees to pay for expanded incident management services and the Northrop Grumman transition. While Security Services has plans for completing Phase II, they have not formalized their goals into a detailed plan that lays out the strategy to complete this phase.

**Recommendation 20**

*As recommended earlier, Security Services must develop a detailed operating plan to address all actions needed, implementation deadlines, and desired results for all of their operating functions, including completion of phase II of the incident management program. In addition to non-compliance with the Code of Virginia, Security Services' lack of an approved action plan may leave the Commonwealth technology assets at risk of security attacks.*

*The response team should also have documented policies and procedures for communicating security risks to the agencies. The approved plan should address communication methods and procedures, allowable response times, and documentation about the alert including agency and response team decisions about security risks.*

## SECTION IV – HIRING AND MONITORING OUTSIDE CONSULTANTS

VITA's supply chain management division oversees statewide IT contracts for all aspects of IT and maintains them on VITA's website. Agencies use the statewide contracts to obtain goods and services. The statewide contracts, especially those related to services, should be a starting point in the contracting process. Agencies that use consulting contracts must supplement them will additional statements of work that include deliverables, due dates, responsibilities, and payment information.

We selected five contracts used by VITA divisions to obtain contractual services. We found that two contained complete statements of work that described deliverables, deadlines, responsibilities, and payment amount. One contract contained only some of this information while the remaining two only provided general descriptions of work with no specific deliverables and due dates.

Missing or deficient statements of work can lead to overpayment for services and make the contractors work difficult to manage. Statements of work document a clear understanding of what work the contractor must perform, how long the work should take, and the performance expectation for receiving payment. We believe VITA staff would have a difficult time monitoring a contractor's work and ensuring that they are performing the work the necessary elements of a well-written statement of work.

### Recommendation 21

*We recommend that VITA revise their statement of work template that managers must complete before any services start and enforce its use. The template would require managers to document specific deliverables, deadlines, milestones, and indicate who at VITA must sign-off as approving deliverables before VITA pays any invoices. A complete statement of work will ensure the contractor understands the deliverables and their due date. Further, it would ensure VITA supervisors have a clear understanding of the scope of a contractors work and provides method to evaluate that the contractor is meeting it.*

## APPENDIX A – FOLLOW-UP ON PRIOR PERFORMANCE AND SECURITY AUDITS

VITA's Internal Auditor provides the Board with a periodic status report that shows VITA's corrective action plan and status of responding to prior audit recommendations. We review the status reports, which are available on VITA's website, to ensure the action plan is reasonable and that VITA is making timely and sufficient progress.

There are several recommendations from our prior reports, particularly related to establishing standards, policies, and procedures, where the responsible person has not completed the corrective action by the deadline. Where this has occurred or where we believe the action plan did not result in the desired change, we have included the theme of the original audit recommendation again in this audit report.

There are also some prior audit recommendations where, although VITA addressed the original concern, there is still related work that they need to perform. For example, in earlier reports we recommended that the Board and CIO prepare a Commonwealth IT Strategic Plan. Although VITA recently completed that plan, we have additional recommendations in this report to improve the process going forward and to ensure the plan has the desired affect at the individual agency level.

In yet other instances there are some recommendations that will be resolved on July 1, 2006 through VITA's IT Infrastructure Comprehensive Agreement with Northrop Grumman. For those recommendations, we consider the concern resolved and have not recommended any further action in this report.

## APPENDIX B - SUMMARY OF REPORT RECOMMENDATIONS

Recommendation 1

We recommend that the Board and CIO work to address the inherent conflicts caused by the CIO's dual role in IT governance and IT operations. The Board should consider increasing its direction and involvement in the functions of IT governance, allowing governance issues to be communicated by the CIO or the Board rather than VITA; thereby, separating this function from the VITA staff performing IT operations functions.

Under this model, the operations function would continue its customer-service orientation to meet agency IT operational needs primarily through enforcing the Northrop Grumman comprehensive agreement. Staff supporting the governance function would support the Board and CIO responsibilities to improve Commonwealth best practices and create efficiencies. The governance function would focus on creating policies and standards and making systems development investment decisions that are in the best interest of the Commonwealth as a whole.

Recommendation 2

We recommend that the Board and CIO ensure their work continues to supports the Council on Virginia's Future Roadmap. Further, as the Board and CIO execute their Commonwealth IT strategic planning responsibilities, they must ensure staff place the Council on Virginia's Future Roadmap as the guiding principle for the process and understand that their work is intended to support the Commonwealth not just those things over which VITA has control.

Recommendation 3

Finally, the Board and CIO should develop and execute a communications plan, highlighting the Commonwealth's IT Strategic Plan and how it affects the agencies. By increasing agency awareness and buy in for the plan, the CIO will help the Commonwealth to execute the plan and ensure it has the intended impact on agency IT strategic planning.

Recommendation 4

As agencies refresh their strategic plans and the Board finalizes the Commonwealth's IT Strategic Plan, we recommend that the Board, CIO, Secretaries of Finance and Technology, and the Council on Virginia's Future, direct VITA and Planning and Budget staff to work together to identify ways to improve the agency strategic planning and IT investment decision process. They should address the need for long-term focus within strategic planning and identify ways to connect a long-term strategic plan with the biennial performance budget needs. Further, this process should not ignore long-term needs, even when short term funding plans cannot address the need.

Recommendation 5

VITA and Planning and Budget must ensure agencies understand how their individual IT strategic plans support the Commonwealth's Strategic Plan and likewise how their proposed IT projects should support the Commonwealth's overall IT goals and objectives. VITA and Planning and Budget should consider incorporating in the Handbook a section that addresses this alignment overall, describing how the Council on Virginia's Future's Roadmap drives to the Commonwealth's IT Strategic Plan and how agency plans should align with both. Additionally, VITA and Planning and Budget should revise the Handbook instructions to improve the IT summary section and the IT strategic plan appendix.

Recommendation 6

VITA should consider changing their current deadline for receiving agency IT projects to better align with the agency's strategic planning cycle. If VITA and the Board implement our recommendations relative to prioritizing projects made later in this report, the process should be more efficient and require less lead-time, allowing this deadline to change.

Recommendation 7

We recommend that the Board and Division revise the priority project report to present estimated annual project costs over the project's life to better inform decision makers of future funding needs. The Division should consider using Planning and Budget's Six-Year Capital Outlay Plan as its reporting model.

Recommendation 8

In addition, consideration should also include simplifying the report to include one prioritized list of both active and new projects recommended for funding. We also recommend that the Board consider the cost-benefit of including, either in the report or on the web, the additional lists and narratives that are not Code of Virginia required. Using these staff resources elsewhere could be more effective in other areas of the Division, such as project monitoring and oversight.

Recommendation 9

We recommend the Board initiate communication with the Governor and General Assembly to determine how the priority report can become a useful decision making tool. If the Board cannot make the report useful to the Governor and General Assembly for making funding decisions, the effort involved in prioritizing these projects is futile.

If the Board cannot adopt the report to meet the needs of the Governor and General Assembly, the Board should consider recommending that the General Assembly eliminate the priority reporting requirement from the Code of Virginia.

Recommendation 10

The Board, CIO, Secretary of Finance and Secretary of Technology should direct VITA staff and Planning and Budget staff to work together to evaluate and report back to them on alternative funding mechanisms for IT projects. VITA and Planning and Budget should consider the 2003 JLARC recommendations, which envisioned a capital funding structure using bonds or other debt instruments, the appropriation of money directly to a central technology fund, a revolving loan fund, or a combination of alternatives. The purpose of exploring funding alternatives is to provide reliable funding for projects and enabling the priority listing to become the driver of technology investment decisions in the Commonwealth.

Recommendation 11

We again recommend that the Board and CIO authorize and that the Division fill vacant full-time positions as a more cost effective approach to hiring vendors. Not only would this provide more resources on a daily basis, it would reduce costs to the agencies that are eventually paying for these services.

Full-time specialists could develop on-going working relationships with the agencies throughout the project development life-cycle, which is generally several years. Having these specialists in-house would make them available to the CIO and the Board at all times to give independent updates on the project and recommend project suspension if there were project management concerns.

Recommendation 12

Earlier we recommended that the Board and CIO fix the inherent conflicts caused by VITA's governance and operation roles. The Project Management Division is one example where this conflict has affected their ability to effectively perform their work and report unbiased opinions to the Board regarding the status of their project. After the Board and CIO address these conflicts, we recommend that the CIO meet with the Project Management Division as well as other VITA divisions affected by the separation of governance and operations to ensure they understand their purpose, responsibilities, and how the changes impact their work.

We believe the Division can assist agencies but also report their opinions on the status of projects successfully. The fact that agencies pay for services does not mean that the Division must be customer focused. Agencies often pay for security vulnerability assessments and audits, activities that are not generally customer focused but rather standards and best practice focused.

Recommendation 13

In addition to fully staffing vacant specialist positions as recommended earlier, we also recommend that the Division examine their administrative tasks, ensure they are having the desired impact, and find ways to make them more efficient or drop them altogether.

To fulfill their purpose of improving project management and identify enterprise and collaborative opportunities to make the Commonwealth more efficient, they cannot continue to operate by reviewing self-reported data. We recommend that the Division take an active role monitoring their projects and independently verify and assess agency self-reported data. The Division must encourage their specialist on how to challenge agencies on whether enterprise and collaborative opportunities exist rather than relying on agencies to indicate whether or not they can work together.

Recommendation 14

We recommend that the Division's policies and procedures require that specialists retain project files, whether hardcopy or electronic, of all agency project documents, review notes, and agency communications.

Maintaining organized project files and notes will ensure a smooth transition and allow any specialist to get up to speed quickly should a specialist resign or the project be otherwise assigned to a different specialist.

Recommendation 15

We recommend that the Division establish written criteria and procedures for recommending that the CIO modify, suspend or terminate a project. Having written criteria and procedures will provide specialists with a baseline understanding of project related issues that could result in such a recommendation.

Recommendation 16

We recommend that Security Services detail, document and approve an operating plan to direct their daily and long-term business decisions. Such a document should also consider how initiatives relate and ensure that responsible parties coordinate and that deadlines work together to support an overall goal and those deadlines are pertinent to the needs of customer agencies and the Commonwealth. We also recommend that VITA management consider how the transition to Northrop Grumman will affect Security Services' role in IT security governance. Such analysis should include the necessary organizational changes and reflect those changes in Security Services operating plan.

Recommendation 17

We recommend that Security Services develop a defined timeline for the finalization and distribution of all outstanding standards to move VITA in becoming compliant with the Code of Virginia and VITA's agency strategic plan. These standards include, but are not limited to, the revised IT security standard and the security audit standard. In addition, we recommend that Security Services include the development of new policies and the updating of existing policies as part of their detailed operating plan.

Recommendation 18

We recommend that Service Management Organization adopt uniform procedures that apply to all aspects of VITA's infrastructure, not only the Richmond Plaza data center. The procedures should comply with the revised security standard, be uniformly applied across VITA's IT infrastructure, and provide sufficient details so that outside parties, such as Northrop Grumman, can clearly understand the requirements. If Service Management Organization finds that an agency needs an exemption to the uniform procedures, they should enforce their existing exception policy and require that agencies and VITA document and approve the exception.

Recommendation 19

We recommend that VITA continue their current effort to provide as much information as possible to Northrop Grumman regarding the recovery of VITA's IT infrastructure in the event of a disaster. However, we further recommend that VITA begin preparing a detailed, written plan to complete a COOP in accordance with existing VITA standards.

Recommendation 20

As recommended earlier, Security Services must develop a detailed operating plan to address all actions needed, implementation deadlines and desired results for all of their operating functions, including completion of phase II of the incident management program. In addition to non-compliance with the Code of Virginia, Security Services' lack of an approved action plan may leave the Commonwealth technology assets at risk of security attacks.

The response team should also have documented policies and procedures for communicating security risks to the agencies. The approved plan should address communication methods and procedures, allowable response times, and documentation about the alert including agency and response team decisions about security risks.

Recommendation 21

We recommend that VITA revise their statement of work template that managers must complete before any services start and enforce its use. The template would require managers to document specific deliverables, deadlines, milestones, and indicate who at VITA must sign-off as approving deliverables before VITA pays any invoices. A complete statement of work will ensure the contractor understands the deliverables and their due date. Further, it would ensure VITA supervisors have a clear understanding of the scope of a contractors work and provides method to evaluate that the contractor is meeting it.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

April 7, 2006

The Honorable Timothy M. Kaine
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Lacey E. Putney
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have completed a review of Information Technology Governance and Virginia Information Technologies Agency (VITA) Operations in the Commonwealth of Virginia as of April 7, 2006. We conducted our overall review in accordance with the standards for performance audits set forth in Government Auditing Standards, issued by the Comptroller General of the United States.

## Objectives

Our objectives for the review were to determine that:

- The Commonwealth Chief Information Officer (CIO) and the Information Technology Investment Board (Board) have fulfilled their statutory responsibilities and legislative intent relative to IT strategic planning.

- VITA has fulfilled its statutory responsibilities and legislative intent relative to project management.

- The CIO and VITA have fulfilled their statutory responsibilities and legislative intent relative to security and that such security services can be adequately described when outsourced later this year.

- VITA has adequate procedures relative to contracting consultants.

- VITA, the Board and CIO have taken adequate correction action relative to prior audit findings.

## Audit Scope

Our audit examined activities for the period December 15, 2004 through April 7, 2006, with a heavy emphasis on current activities due to the Commonwealth's transitioning environment under VITA. We focused primarily on VITA's operations in the areas of strategic planning, project management, security, and contracts.

## Audit Methodology

Our work consisted of management and departmental inquiries, gaining an understanding of processes and controls by conducting walk-throughs, examination of VITA's documentation, selection and tests of various samples, review of VITA's policies and standards, and meetings with the staff from the Joint Legislative Audit and Review Commission, the Department of Planning and Budget and the Council on Virginia's Future.

We discussed this report with the Chief Information Officer and VITA management at an exit conference on May 2, 2006.

## Audit Conclusion

Overall, we found that:

- The CIO and Board have fulfilled their statutory responsibilities but have not fulfilled the legislative intent relative to IT strategic planning.

- VITA has fulfilled its statutory responsibilities but has not fulfilled the legislative intent relative to project management.

- The CIO and VITA have fulfilled their statutory responsibilities but have not fulfilled the legislative intent relative to security and cannot adequately describe security services when outsourced later this year.

- VITA does have adequate procedures relative to contracting consultants.

- VITA, the Board and CIO have not taken adequate correction action relative to some significant prior audit findings relative to security.

Our report contains recommendations throughout to improve processes and controls. There is also a summary of all recommendations located in Appendix B.

AUDITOR OF PUBLIC ACCOUNTS

# COMMONWEALTH of VIRGINIA

**Virginia Information Technologies Agency**

Lemuel C. Stewart, Jr.
CIO of the Commonwealth
Email: cio@vita.virginia.gov

110 South 7th Street
Richmond, Virginia 23219
(804) 371-5000

TDD VOICE -TEL. NO.
711


May 12, 2006

Mr. Walter J. Kucharski
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Mr. Kucharski:

Thank you for the opportunity to comment on the APA's recently completed audit of selected functions in Commonwealth IT project management, strategic planning, and security. As you know, many of these functions are relatively new to state government, and we continue work with the other executive branch and legislative participants to refine and improve in-place activities even as we begin new initiatives and radically transform others.

In that vein, we appreciate the efforts of your staff to point out areas for improvement, both to us and to other players in the areas studied. I believe the dialogue between our respective staffs, as the initial drafts of your report went through extensive reviews and revisions, was productive and informative for all concerned. As a result, I believe our organizations have developed a much more extensive, mutual understanding of both the complexities of the areas studied and the key issues in achieving further improvements.

One of the benefits of your review has been the opportunity to step back and gain perspective on how far we have come and what we have learned from that journey to help us gauge expectations going forward. Building on and amplifying related points in your report, I suggest such key lessons include the following:

- While the legislation that was the focus of your audit created new centralized processes in IT strategic planning and implementation, those processes must coexist with other long-standing central operations—all of which in turn must operate in what remains a very decentralized decision-making environment. The authors of that 2003 legislation could not possibly have envisioned all of the adjustments and accommodations that have been (and continue to be) made to try to make all this "fit" as best as can be done. Looking back, the results of collective efforts to do that fitting and still remain true to the intent of the legislation are indeed impressive, gaining national prominence. We have learned good progress can be made but also that other priorities outside our domain—let alone just running the daily business of state government—require their own accommodations and realistic expectations of the rate of change in the future.

- New funding mechanisms must be recognized as a tool, not a panacea. Even with excellent collaboration among the various players, putting such mechanisms in place takes time, given the systems of checks and balances within and among the involved branches of government. And once in place, expectations as well as revenues must be managed. As you well know from negotiating your own annual work plan with the

General Assembly, value and risk are key determinants in where limited dollars are applied against what will always seem to be unlimited needs.

- Our partnership arrangement will continue moving us toward a more commercial model of providing IT services within government. That's a good thing in that it helps keep prices down and service levels up. It also means we'll be increasingly evaluating ourselves against evolving industry best practices and standards to determine how, when and where we make our investments in order to stay competitive. That's a much more dynamic, externally driven yardstick of expectations and performance than state government is used to applying.

Perhaps the most significant aspect of your report is that its focus is not primarily on compliance—whether *Code* requirements were met—but on opportunities to go beyond "good enough". I believe the entire VITA organization and its supervisory board have shown by their performance over the last three years their wholehearted dedication to VITA's motto, "expect the best". The changes in the state's IT arena over the last three years when compared to prior periods—going back 10, 20, even 25 or more years—are nothing short of amazing. And the IT Transformation about to take place over the next three years will be even more impressive.

I believe your report and the lessons we can take from the last three years offer valuable guidance for moving forward with a reasonable balance of ambition and expectations. We owe it to the many individuals in so many agencies across the state whose hard work has gotten us this far to cheer them on further by celebrating their accomplishments. And we owe it to the citizens and taxpayers of Virginia to continually strive to do even better.

Sincerely,

Lemuel C. Stewart, Jr.

c: The Honorable Aneesh P. Chopra, Secretary of Technology
Judy G. Napier, Deputy Secretary of Technology
Members, Information Technology Investment Board

# *COMMONWEALTH of VIRGINIA*

**Richard D. Brown**
Director

*Department of Planning and Budget*

1111 E. Broad St., Room 5040
Richmond, VA. 23219


May 16, 2006

Mr. Walter J. Kucharski
Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Dear Mr. Kucharski:

I received and reviewed your recent report on the status of information technology (IT) consolidation in the Commonwealth. I appreciate the opportunity to respond to your concerns and recommendations relevant to the Department of Planning and Budget. The focus of our review is on Recommendations Four, Five, and Six, and associated text.

First, I applaud your recognition of the Commonwealth's new strategic and service area planning process. Your acknowledgement of the state's performance-based budget approach shows the hard work performed by all executive branch agencies and many legislative and judicial agencies has not gone unnoticed. However, I am somewhat confused by your statement that agencies have not created strategic plans.

There are two sections to the planning process: the Agency Strategic Plan guiding the longer-term direction of the agency, including linkages to the Council on Virginia's Future's objectives, as well as IT planning; and the Service Area Plan which addresses performance-based budgeting, including operation IT plans. Since Service Areas are tied to the biennial budget, there is naturally a two-year horizon for the development of the Service Area Plan. This direct link is something that the strategic planning process has been trying to accomplish since the mid 1990's. Its sole purpose is to ground agency strategic planning efforts in the reality of available budgetary resources and make such efforts more realistic in terms of their ultimate stated goals.

In contrast, the agency portion of the strategic plan includes the longer term vision and direction of the agency which is supported by the shorter-term direction in the Service Area plans. Though not explicitly stated in our strategic planning handbook, training and subsequent guidance prescribes a four-year planning horizon for the agency strategic plan component, with flexibility for a longer timeframe, if necessary. Accordingly, if there is confusion over these two

elements, I am more than willing to make my staff available to further explain the process to you. But, I do not agree with the assertion that "agencies do not have strategic plans." They have both: Agency Strategic Plans and Service Area Plans.

Second, I think it would be helpful if the APA were to better define what is meant by a "best practice" in strategic planning. Per your own research there is no one standard for the development of performance management systems. The Federal Government has a model, state and local governments have varying methods, and international and academia approaches are even more varied. However, none of these are singularly recognized as a set of best practices to be emulated.

The approach Virginia has developed contains those elements deemed necessary for success by the executive and legislative branches of government. In 2004 and 2005, our process was painstakingly developed and implemented by a team of agency representatives, including the APA. The intent of this work effort was to develop a set of "workable practices" for Virginia. Your participation in strategic planning, IT strategic planning and reengineering activities as well as that of the other agencies were directed toward that end.

Finally, I strongly concur with the conclusions you have drawn regarding IT planning in the state. Accordingly, DPB and VITA are presently in discussions to improve how IT planning data are captured, to better link such data to agency strategic plans, and to better communicate the process to agencies. However, as you point out, the CIO is legally guided by a set of dates and information types that are different than those legally set out for the budget development process. Until this is changed, the Code of Virginia will continue to be obstacle against distinguishing long-term IT needs from short-term operational needs.

Again, thank you for the opportunity to review your report. I hope you find our suggestions helpful.

Sincerely,

Richard D. Brown

cc The Honorable William H. Leighty
The Honorable Jody M. Wagner

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

INFORMATION TECHNOLOGY
INVESTEMENT BOARD MEMBERS

As of March 2006

James F. McGuirk II, Chairman

| | |
|---|---|
| Aneesh P. Chopra | Walter Kucharski |
| Jimmy Hazel | Mary Guy Miller |
| Hiram Johnson | Scott Pattison |
| Kenneth S. Johnson, Sr. | Len Pomata |

Alexander Y. Thomas

CHIEF INFORMATION OFFICER

Lemuel C. Stewart