G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 2, 2001

The Honorable Steve Buyer
Chairman, Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

Subject: Veterans Affairs: Subcommittee Questions Concerning the Department's Information Technology Program

Dear Mr. Chairman:

This letter responds to your April 12, 2001, request that we provide answers to questions relating to our testimony of April 4, 2001.[1] During that testimony, we discussed the status of the Department of Veterans Affairs' (VA) efforts to address numerous information technology challenges, including filling its chief information officer (CIO) position, improving computer security, and refining its processes for selecting, controlling, and evaluating its information technology investments. Your questions, along with our responses, follow.

1. What has been the impact for the VA lacking a dedicated CIO?

Appointing a permanent CIO is critical to the success of VA's information technology (IT) program. CIOs play an essential role in driving management processes to help control system development risks, better manage IT spending, and succeed in achieving real, measurable improvements in agency performance. Without such an official, VA lacks the level of leadership and focus needed to assist the Secretary and his executive management team in effectively identifying and responding to departmental IT challenges and in using IT to help realize improvements in the department's programs and operations.

VA faces long-standing and critical IT challenges and concerns. Our prior reports and testimonies have highlighted weaknesses in the department's efforts to develop an enterprise architecture, improve computer security, improve IT investment management, and implement and use key information systems. Each of these weaknesses has significant implications for the department, and when considered collectively, they reflect a critical need for the immediate and sustained attention of a CIO.

[1] *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist* (GAO-01-550T, April 4, 2001).

In particular, as a key figure in applying technology to improve fundamental business processes and operations, a CIO can play an essential role in facilitating VA's implementation of an enterprise architecture. Without such an architecture, the department lacks fundamental guidance for developing mission-critical systems and achieving the appropriate integration of systems through common standards—which are necessary if VA is to successfully realize its "One VA" vision.

Further, a CIO is vital to the success of VA's information security management program. Despite taking constructive steps to address recognized computer security weaknesses, the department nonetheless needs a stronger management focus to resolve lingering departmentwide security problems. Dedicated CIO and other senior management attention is needed to help ensure that policies and guidelines adequately address the security of the department's interconnected computer environment and other key components of security management, such as risk identification and mitigation. Sustained management attention is also necessary to confirm that security-related activities are periodically monitored, tested, and evaluated, and that appropriate corrective actions are taken, when called for.

VA has also been challenged in managing its IT investments. To its credit, the department has improved its processes for selecting, monitoring, and managing its investments; however, the lack of demonstrated performance in implementing key parts of its investment guidance—such as reviewing on-going and completed IT projects through in-process and post-implementation reviews—deprives VA's top management of vital information needed to evaluate the effectiveness of these efforts and to make critical decisions regarding their development and implementation. Given VA's substantial IT budget and resources, the CIO should have a major role in ensuring that the department's processes for leading, managing, and controlling IT investments are fully instituted and adhered to throughout the department.

2. In GAO's opinion, which Departments have effective CIOs? What makes them effective? How are these CIOs empowered?

Our work to date has not included specific reviews of the effectiveness of other departments' CIOs. However, we have recently issued a report on the effectiveness of CIOs in several leading private and public organizations, which highlights a number of factors contributing to CIO successes.[2] Among these critical success factors are the following:

- Senior executives in the organizations embrace the central role of technology in accomplishing mission objectives and include the CIO as a full participant in senior executive decision-making. The top executives of these organizations determine how a CIO best fits within existing or new management tiers to guide technology solutions, and CIOs are chosen to match the organizations' needs.

- Effective CIOs have legitimate and influential roles in partnering with top managers to apply IT to business problems and needs. While the placement of the CIO position at an

[2] *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations* (GAO-01-376G, February 2001).

executive management level in the organization is important, successful CIOs earn credibility and produce results by establishing effective working relationships with business unit heads.

- CIOs structure their organizations in ways that reflect a clear understanding of business and mission needs. Along with business processes, market trends, internal legacy structures, and available IT skills, this structure is necessary to ensure that the CIO's office is aligned to best serve the needs of the enterprise.

- CIOs work effectively with their executive peers to jointly produce a vision that encompasses educating senior managers on the strategic value of IT, providing advice and direction, and setting expectations of what can be achieved. CIOs also participate on executive committees and boards that provide forums for promoting and building consensus on IT strategies and solutions.

These success factors and their underlying principles illustrate the extent to which the work of a successful CIO must extend throughout the enterprise. In particular, they highlight the role that senior executives play in creating an effective management context for their CIOs, as well as the CIOs' responsibilities for building credibility and organizing information technology and management to meet business needs. While the CIO has specific responsibilities that he or she must execute, it is clear from our studies of these organizations that successful CIOs rely extensively on both vertical and horizontal relationships within the enterprise to ensure that their duties are carried out most effectively.

3. GAO's testimony addressed the vulnerability and weaknesses of VA's IT security. What are the five most important issues the Secretary must instruct the new IT security czar to fix or begin to address in the next 60 days? How about in the next 180 days?

There are a number of critical IT security issues that VA must address to safeguard its assets, maintain the confidentiality of sensitive information, and ensure the reliability of its data. Consistent with our prior recommendations, the most important issues that the Secretary of Veterans Affairs should instruct the new IT security executive to begin addressing within the next 60 days include the following:

- Assess the status of actions taken to correct security weaknesses identified by VA's inspector general, GAO, VA management, consultants, or other external organizations. For those weaknesses reported as closed, independently validate that the actions taken have corrected the weaknesses. For those that remain open, take steps to implement a plan that sets priorities and requires corrective action within a reasonable timeframe.

- Review progress in implementing the actions in VA's departmentwide information security management plan. Assess all planned near- and long-term actions to ensure that they continue to be valid and monitor the progress of each action against established milestones.

- Meet with the security officers for each of the administrations and their key components, as appropriate, to (1) begin to develop communication lines and coordination efforts between security functions, as a means of integrating security across all VA component organizations, and (2) assess opportunities to build on existing computer security initiatives. In September 2000,[3] we reported that VA organizations had independently acted to improve computer security, but these efforts were not coordinated as part of a departmentwide program. We noted that these organizations had developed certain guidance and oversight processes relating to key security management areas that could provide VA a starting point to expedite the development of departmentwide policies and procedures for assessing risk, monitoring access activity, and evaluating the effectiveness of information system controls.

- Review the computer security management of VA's wide area network. Currently, authority over operation of parts of the network is decentralized among 10 system administrators, providing the opportunity for security vulnerabilities to arise through the practice of implementing varying levels of security controls. Verify that overall network security is tested, including network security for each administration and central office. To complement this effort, implement a departmentwide intrusion detection program to better protect the network from unauthorized access.

- Require each of VA's key facilities to assign a full-time security officer. In our prior reviews at VA, we noted that most medical facilities did not have full-time security officers.

Beyond these near-term issues, there are other security weaknesses that VA should address within the next 180 days. We have previously reported on and made recommendations related to these weaknesses.[4] Actions needed to address these weaknesses include:

- Developing policies and guidance on how and when risk assessments should be conducted, and defining the level of risk assessment required for system changes.

- Updating the department's security policies and guidance to adequately address the security of its interconnected computer environment and developing technical security standards for VA's system and security software.

- Establishing a mechanism for routinely analyzing security incident records. Such a practice could provide VA with an additional process for proactively identifying and responding to other system security vulnerabilities. In addition, the information could be used to enhance security controls.

---

[3] *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration* (GAO/AIMD-00-232, September 8, 2000).
[4] GAO/AIMD-00-232, September 8, 2000, and *Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-5, October 4, 1999).

4. *What are the major obstacles the VA faces in coming up with an integrated, department-wide enterprise architecture? Why is this so difficult for the VA?*

The major obstacle that VA faces in its attempts to develop an enterprise architecture is the lack of business and senior management involvement in and support for such an architecture, coupled with each administration believing that it needs its own. VA's CIO organization has not yet gained business-level and senior management support for the enterprise architecture development effort. Doing so is critical since the architecture will serve as a roadmap to achieving the agency's mission and performing core business functions within an efficient technology environment. Not only does VA's CIO organization need senior management to articulate its vision, and the business lines to document their business processes, information flows, and data needs, but it also needs senior management support to institutionalize the use of the enterprise architecture once developed.

However, VA's efforts to develop an architecture have, to date, been limited mostly to CIO and IT staff. As we testified in May 2000,[5] VA's previous efforts to develop an integrated, departmentwide architecture resulted only in the development of a technical architecture. We further stated that VA should initiate a new architecture development effort that incorporates the business lines as well as the IT components. The subcommittee agreed with our recommendation and requested that VA develop a plan, with milestones, for completing that architecture.

Despite VA's statement in its August 2000 Enterprise Architecture Plan that the cross-agency effort would involve both business and IT staff, its subsequent efforts were handled almost exclusively by IT staff. Concerned that VA's business lines were not adequately integrated in prior efforts to develop the architecture, VA's Secretary has now requested that business managers be included in any new development efforts.

5. *VETSNET has taken over 10 years to conduct a pilot test to process 10 pre-selected "vanilla" claims. In GAO's opinion, how long will it take VETSNET to get up to speed on 3.2 million claims payments?*

At this time, it is not possible to state when the Veterans Service Network (VETSNET) will be capable of processing the approximately 3.2 million compensation and pension payments made to veterans and their families each month. The project has progressed in some areas; for example, the Veterans Benefit Administration (VBA) completed implementation of the rating board automation tool in November 2000, and completed development and testing of four other key software components at the end of January 2001. However, the department needs to address several important issues before the compensation and pension replacement system can be successfully implemented.

---

[5] *Information Technology: Update on VA Actions to Implement Critical Reforms* (GAO/T-AIMD-00-74, May 11, 2000).

Although VBA has established a schedule that calls for deploying the compensation and pension replacement system in July 2002, it has not yet completed an integrated project plan and schedule incorporating all the critical areas of this system development effort. Such a plan is necessary for determining what project activities need to be accomplished and when, and for measuring VBA's progress in meeting the development milestones. Moreover, given previous delays in developing this project, such a plan is essential to helping VBA earn confidence in its ability to successfully proceed with this development effort.

Further, VBA still has to define a strategy for its most complex remaining effort—converting data from the old system to the new compensation and pension replacement system. According to project officials, successfully converting the data will require the involvement of compensation and pension business-line staff who have significant knowledge of the business processes and data needs and can provide necessary input into decisions regarding the system's design, development, and implementation. However, the data conversion effort has already encountered delays due in part to the lack of business-line support.

6. *GAO's testimony indicates that weak management has allowed lingering department-wide security problems. Which management team is accountable for not addressing this issue? What vulnerability issues must the Secretary address with specific instruction within the next 60 days?*

Responsibility for managing the security of VA's computers and data has resided with the department-level CIO, in coordination with administration heads, assistant secretaries, and other key officials. In addition, the Veterans Health Administration's (VHA) medical centers also have responsibility for securing their local systems. However, VA's difficulty in selecting a permanent CIO restricted its ability to effectively deal with departmentwide security issues. The senior executive recently installed to oversee the department's security program will now have a critical role in addressing VA's security challenges.

Issues that VA's Secretary needs to address within the next 60 days include

- defining the role and responsibilities of the security czar and empowering this official with the authority to ensure that the overall security management program is fully implemented departmentwide,

- requiring the security czar to periodically brief the Secretary on plans for improving information security and on progress in implementing these improvements,

- holding all senior managers accountable for ensuring strict compliance with security directives, as the lack of line management accountability is one reason security has not received adequate attention within VA, and

- ensuring that adequate resources are available to implement the actions necessary to improve security.

7. *VA published an updated guide for capital investment in information technology in October 2000. Is the VA following its own guidelines in its IT investments?*

VA's information technology capital investment guide addresses a number of shortcomings that we previously identified with the department's investment management process. Nevertheless, VA has not yet demonstrated that it is implementing key parts of this guidance. For example, the department has included guidance for conducting in-process and post-implementation reviews. These reviews are essential for aiding the department in controlling and evaluating IT investments. Consistent with our prior recommendations, the guidance stipulates that completion dates be included in VA's in-process review plans and that the results of post-implementation reviews of capital investment board-level projects be provided to VA's CIO Council. In addition, the guidance requires VA to conduct quarterly execution reviews of approved IT capital investments to help identify projects experiencing cost, schedule, or performance problems.

However, since September 2000, the department has not scheduled or conducted any in-process or post-implementation reviews, and the director of VA's Information Resources Management (IRM) Planning and Acquisition Service told us that the department has not conducted an IT execution review since June 2000. At the time of our testimony, the department indicated that it intended to conduct one in-process review and three post-implementation reviews. However, it had not established plans or a schedule showing when these reviews would be performed.

VA's IT investment guide reiterates the department's Directive 6000 requirement to maintain complete and accurate data on all personnel and nonpersonnel costs associated with IT activities. However, the department lacks a uniform process for tracking its IT expenditures. Without such a cost-tracking mechanism, VA may lack data needed to monitor and evaluate investments individually and strategically, provide feedback on the projects' adherence to strategic initiatives and plans, and allow for review of unexpected costs or benefits resulting from investment decisions. The director of VA's IRM Planning and Acquisition Service indicated that the department will begin using a new numbering system within its current financial management system, which should enable the department to compile reports on approved capital investment expenditures beginning in fiscal year 2002. However, until its new financial management system is implemented—estimated in October 2004—the department may continue to lack the capability to track complete personnel costs for capital investment projects and all expenditures for smaller IT projects.

8. *In May 2000, the former Chairman of this Subcommittee requested that the VA provide a plan with definitive milestones for completing an integrated department-wide information systems architecture. I understand this has been accomplished. Has the GAO seen this plan?*

We have neither received nor reviewed a plan from VA containing definitive milestones for completing an integrated, departmentwide information systems architecture. Rather, in August 2000, VA provided us with a document that contained high-level estimates of the time required to complete certain elements of the departmentwide architecture. However, this document did not contain any definitive dates for completing the various elements or the departmentwide architecture as a whole. Moreover, the document stated that a contractor chosen to develop the architecture would be expected to deliver a work plan that identified the methodologies and milestones for completing the development tasks. At this time, we are not aware that this effort has been performed.

9. *How much money has the VA spent on VHA's Decision Support System? How many VISNs still do not utilize DSS? Which ones? How many medical centers do not use DSS? Which do not? Why haven't they implemented DSS?*

According to VA estimates, it has spent approximately $261 million to develop and operate DSS from fiscal year 1992 through fiscal year 2000. Additionally, VA has reported that it expects to spend about $50 million to operate DSS in fiscal year 2001.

In following up with DSS coordinators for those VISNs that previously reported not using DSS, we were told that VISN 20 is the only veterans integrated service network that is still not using the system to support its decision-making—although some of its facilities (i.e., medical centers and clinics) do currently use the system. For a VISN to use DSS, all of its medical centers must process their clinical and financial data in the system in a similar manner. However, the VISN 20 DSS coordinator indicated that because DSS data are organized and maintained differently by that VISN's various facilities, the data cannot be compared and thus are not readily usable for decision-making at the VISN level. For example, the coordinator explained that in maintaining primary care data in DSS, the medical centers within VISN 20 will only include data in their DSS primary care departments that pertain to primary care work, while a community-based outpatient clinic may include data that extend beyond primary care work.

DSS has been implemented in all of VA's medical centers since October 1998. Nonetheless, as we testified in September 2000[6] and last month, the medical centers were not using the system for all the purposes that VHA intended. Our most recent work did not include assessing all medical centers' current uses of DSS. However, we did review a DSS processing report, dated March 31, 2001 (the most recent report available), which indicated that all medical centers except the Anchorage Health Care System have completed their processing of fiscal year 2000 data.[7] Further, according to the VISN 20 DSS coordinator, the Anchorage Health Care System does not currently use the system. She explained that the medical center records about 50 percent of its costs (i.e., those costs associated with its fee-for-service program) in a health system module that does not feed data into DSS. As a result, capturing these costs in DSS requires two separate data entries—one that feeds data into DSS

---

[6]*VA Information Technology: Progress Continues Although Vulnerabilities Remain* (GAO/T-AIMD-00-321, September 21, 2000).

[7]The report further indicated that only three DSS sites—the Erie, Pennsylvania, and Tomah, Wisconsin, medical centers and the Chicago Health Care System—had not begun processing fiscal year 2001 data.

and another that records costs in a fee-based category. The official stated that these data entry requirements resulted in the medical center falling behind in processing DSS data.

-- -- -- -- --

Dr. Snyder's questions, along with our responses, follow.

10. What must the VA do to provide effective, seamless "One-VA" service to America's veterans and their families?

Information technology is essential to VA's ability to effectively serve the veteran population and is the cornerstone of the department's vision of providing seamless services to veterans and their families. Integral to this vision is the effective and efficient use of current and emerging technology to support the department's business operations and improve overall customer service delivery. Despite its numerous investments, however, the department's IT infrastructure continues to include many standalone and stove-piped systems that do not interface or share information across the department, and thus are inconsistent with the premise of "One VA."

To provide the "One VA" services that it envisions, the department will need to immediately focus on two critical areas. First, as we have previously discussed, VA must complete the process of hiring a permanent CIO. Having a permanent CIO is essential to ensuring that the department's IT resources are effectively managed and that the benefits of its investments are fully realized. Second, the department must ensure that sustained attention is given to implementing an enterprise architecture that will drive the development and implementation of integrated IT investments across the department. Without strong leadership and a clearly defined infrastructure, VA jeopardizes its vision of providing seamless and more efficient service to its customers, and positions itself to continue developing systems in a manner that is neither efficient nor effective.

11. Would you describe VBA's VETSNET project and estimate how much money and how many employee labor years the agency has allocated to VETSNET-type efforts over the past ten or more years?

VETSNET consists of a series of projects, begun in 1986, aimed at replacing VBA's aged Benefits Delivery Network. VBA had anticipated that VETSNET, when completed, would allow real-time access to claims information and provide veterans service organizations and other entities greater access to compensation and pension benefit data.

Two of the major projects initiated under VETSNET were the education 1606 replacement project and the compensation and pension replacement project. VBA discontinued the education 1606 replacement project in November 1997 after spending approximately $3 million on the initiative and without delivering a product. As our prior reports and testimonies have discussed, VA is continuing its effort to develop the compensation and pension replacement project. However, over the years, we and others have reported on problems that VA has encountered in completing the project. For example, we noted that the project was begun before VBA had fully developed its business requirements, and

subsequent project delays resulted from confusion over the specific requirements to be addressed. The project has missed several key milestones, including its original May 1998 completion date and a revised date of December 1998. In 1999, VBA modified its strategy for developing the project, with the intent of incorporating software developed outside the original project, including the rating board automation software tool (which was later modified to become Rating Board Automation 2000) and the Claims Automated Processing System (which was redeveloped into Modern Award Processing-Development, or MAP-D).

We have faced difficulty estimating the funds and staff years expended on VETSNET over the last 15 years because VBA does not directly track in-house staffing costs on a project basis. Rather, VBA estimates costs based on the number of staff reportedly assigned to the project multiplied by a site average cost. VBA also does not track costs incurred at its 58 regional offices for work related to systems development. Nonetheless, in reviewing past and current budget data, we determined that, over the last 15 years, VBA has spent at least $400 million[8] on systems modernization projects that are now included under the VETSNET initiative. These costs cover the development of the VETSNET hardware environment and certain applications, such as the Veterans On-line APPlication (VONAPP).

12. What improvements in veterans' service delivery have been derived from VETSNET?

Many of the VETSNET components, including the compensation and pension replacement effort, have not yet been completed. As a result, few service delivery improvements have been realized to date. However, one new capability that has helped improve service delivery to veterans is VONAPP. Specifically, VONAPP offers veterans the ability to complete applications for compensation and pension, vocational rehabilitation, and education benefits at their homes, thus eliminating the need to visit a regional office. In addition, the application is transmitted to VBA electronically rather than by mail, thus also helping to reduce processing time.

Further, in November 2000, VBA implemented the Rating Board Automation 2000 software for the compensation and pension replacement project, which was expected to assist veterans service representatives in rating benefit claims. However, according to a VBA official, some regional offices have indicated that, rather than improve service delivery, use of the software tool has resulted in longer processing times. The Undersecretary for Benefits recently suspended the requirement for regional offices to use the software tool until the department has reduced its claims backlog. At this time, we have not collected specific information from VBA demonstrating how this tool has actually performed.

13. Should VA call a halt to further development of the VETSNET project?

VBA needs to carefully assess the current VETSNET/compensation and pension project to determine whether it is capable of producing an acceptable return on investment. As we have previously noted, this project has suffered from numerous problems and schedule delays, which threaten the overall success of the initiative. Responsibility for project success is not

[8]This amount was spent between fiscal year 1986, when VBA first began modernizing its systems, and fiscal year 2000. Fiscal year 2001 costs are not included in this figure.

limited to VBA, however, and the department needs to do more to monitor the progress of this initiative. Specifically, VA needs to strengthen its management oversight to ensure that the project is meeting milestones, is not exceeding costs, and is consistent with the "One VA" information technology environment that the department envisions. VA's IT capital investment process includes control mechanisms, such as in-process reviews, to help the department identify and respond to problems encountered in developing and implementing its projects. However, VA has not conducted an in-process review for the VETSNET/compensation and pension project since 1998.

Even if the results of such an assessment are positive, VBA will still need to perform certain tasks before it can successfully complete this project. As previously noted, VBA needs to develop detailed, integrated plans with milestones and costs as a means of determining what project activities need to be done and when, and for measuring the progress of this initiative. VBA also needs to ensure that the project obtains the needed support from the compensation and pension business line. Finally, VBA needs to review critical IT management processes, such as its software testing and evaluation activities, to ensure that its capabilities are at the appropriate level to achieve reliable results.

14. What is your assessment of top management's commitment and support of information technology, and upon what do you base that assessment?

Indications are that top management is committed to and strongly in support of information technology as a critical tool for providing seamless services to veterans and their families. The VA Secretary has testified that resolving the department's long-standing technology problems is a priority, and has declared a moratorium on new IT spending until the department has defined an enterprise architecture. Further, the recent hiring of a senior executive to oversee the department's information security management program and the ongoing search for a CIO suggest that the Secretary is strongly committed to and in support of improving the department's information technology program. However, the success of these efforts depends on the extent to which the Secretary and his executive management remain focused on and involved in addressing the critical IT challenges that VA faces in the months ahead.

-- -- -- -- ---

We provided a draft of this letter to VA officials. Their comments have been incorporated where appropriate.

We are sending copies of this letter to the Secretary of Veterans Affairs and other interested parties. Should you or your staff have any questions on matters discussed in this letter, please contact me at (202) 512-6257. I can also be reached by e-mail at mcclured@gao.gov.

Sincerely yours,

David L. McClure
Director, Information Technology
Management Issues

(310416)