

**Post-Hearing Questions
Concerning the April 4, 2001, IT Hearing**

**For
The Department of Veterans Affairs**

**From
The Honorable Steve Buyer
Chairman, Subcommittee on Oversight and Investigations
Committee on Veterans Affairs
U.S. House of Representatives**

1. Please describe technological, organizational, and cultural challenges the VA faces in implementing an Enterprise IT Architecture.

The technological challenges that VA faces in implementing an Enterprise Architecture are integrating VA's legacy, stovepipe systems that have been developed over many years and assuring that VA's infrastructure and telecommunications wide area and local area networks have the capabilities needed to make business information available to all who need it. The organizational challenge is to have the three Administrations with their specific and diverse missions develop the business processes that will ensure common information and business needs are shared across VA's business lines. The cultural challenges derive from VBA's centralized management style and VHA's decentralized form of management and heavily ingrained professional biases and traditions. An additional challenge arises from the need for reaching agreement on standard data definitions.

2. Until a candidate for the Department CIO is confirmed by the Senate, who will ensure that the requisite VA IT leadership and management will be carried out to address IT management issues raised by GAO?

An Acting CIO has been appointed who has as his only function the management of the Department's information technology assets, both existing and proposed. This individual reports to the Secretary on all matters involving information technology (IT), in full spirit of the Clinger-Cohen Act. The day-to-day management of the Department's information technology is being administered and carried out by a fully dedicated staff that answers to the Acting Chief Information Officer. This is the same staff that will provide support to the VA CIO, when he or she is confirmed by the Senate.

3. What will the reporting relationships be between the Department Chief Information Officer and the Administrations' Chief Information Officers?

The VA's CIO determines and sets IT policy for the entire Department; policy the Administrations are obliged to follow. The Administrations' CIOs take their technical direction from the Departmental CIO. Currently, the Administration CIOs report to their respective Administration management. They serve their Administration by representing their needs and best interests to the Departmental CIO while they carry out IT policy as determined by the Departmental CIO. If at any point the best interests of the veteran or the Department of Veterans Affairs are not being served I am prepared to change this reporting mechanism.

4. What will be the roles and responsibilities of the VA cyber security executive and to whom will he report? Will he have responsibility for Department-wide security issues?

The VA Associate Deputy Assistant Secretary for Cyber Security has overall responsibility for information security in the Department and reports to the Chief Information Officer. His role is primarily that of VA Information Security Officer empowered to issue and enforce policy, procedure, and guidance. In addition, his tasking is to manage those activities, which for reasons of efficiency and cost-effectiveness, are best performed at the highest level. Examples include security training and education, public key infrastructure (PKI), virus defense, intrusion detection, incident handling, risk assessment, security architecture, and certification/accreditation. He is also tasked with the leadership role in VA's information security community, ensuring cooperation of Administrations and Staff Offices.

5. What is your plan to ensure that VA's security policies, procedures, and guidance are up-to-date, comprehensive, and well communicated throughout VA's administration?

The Cyber Security Office (CSO) has issued overall information security policies and procedure handbooks. In addition, specific policies for the security of external connections, account and password management, and for limited personal use of government resources have been issued. Two additional policies will soon be issued: Public Key Infrastructure (PKI) and security certification and accreditation.

The project to revamp VA's security policies is in process already. All directives, handbooks, and procedures under the purview of the CSO are currently under review. Based on current laws, executive policies, input from oversight organizations, and VA's risk posture, all will be prioritized, created or revamped, and issued over the next six months. Security enforcement procedures and policies are also included in the comprehensive review.

In addition, the CSO will work with their Administration and Staff Office security colleagues to ensure that policies, procedures, and guidance are understood and disseminated to all employees. The mechanisms for these communications are the Security Subcommittee of VA's CIO Council and the lower-level VA Information Security Working Group. Further, the CSO has a training and awareness program that includes an on-line security awareness course required for all VA employees, contractors, and volunteers. The Department awareness program also includes brochures, posters, and log-on bulletins. The program also provides on-line training for VA's Information Security Officers (ISOs). A VA Critical Incident Response Capability (VA-CIRC) ensures that warnings of potential threats are communicated to VA offices and that local incidents are reported and analyzed.

6. How do you plan to ensure that policies, procedures, and guidance for the performance of risk assessments on a continuing basis or when significant changes occur as well as on how these risk assessments should be conducted are developed and communicated throughout VA's administrations.

One of the first orders of business in the Cyber Security Office is to establish a formal process for identifying Department security assets and for recording their security status. A continuous and periodic process of facility and system review, as established under the Government Information Security Reform Act (GISRA), will provide the metrics to determine the effectiveness of the Office's plan. This continuous review will determine if adequate risk assessments are conducted by Department "systems' owners". If the reviews indicate that inadequate risk assessments are being performed, the Cyber Security Office will work with their Administration or Staff Office counterparts to resolve the problems. Issues of chronic problems with risk assessments, or any other security program component, will be brought to the attention of the respective Administration or Staff Office leadership for resolution.

7. VA has a computer security incident reporting and response system. However, there is no mechanism for routinely analyzing security incident records.

Do you plan to establish policies and procedures for the routine analysis of the incident reports generated by the reporting system? How will you ensure that these analyses are done on a regular basis?

The Cyber Security Office has already noted your concerns with the VA Critical Incident Response Capability's (VA-CIRC) active response to incidents. The office will establish an active process for analyzing incidents and potential incidents. These analyses will be undertaken on a regular basis as well as in response to real-time events. We think that analyzing incidents is merely the second step in responding to them. Our CIRC will soon feature policy and procedure to detect incidents, analyze them, and mount an appropriate defense.

8. How will the VA ensure that general access control and operating system weaknesses are reviewed and analyzed?

As previously noted, a continuous and periodic process of facility and system review, as established under Government Information Security Reform Act (GISRA), will provide the metrics to determine the security status of VA's access controls and operating systems.

9. GAO testified that no in-process reviews or post-implementation reviews have occurred since September 2000. Why hasn't the VA performed these reviews? More specifically, why didn't VA do any in-process or post-implementation reviews on projects that have had problems before, such as the VETSNET/C&P Replacement Effort?

The guidelines for conducting an in-process review are specified in VA's *Information Technology Capital Investment Guide*. This guidance states that an in-process review (IPR) is initiated when the CIO Council wants to answer specific questions relative to an ongoing project's performance; the Department's CIO requires additional information; or management from an Administration or a Key Staff Office requires additional information concerning an IT initiative. During Fiscal Year (FY) 2001, when specific information was required on an IT investment by either the CIO Council or the Department's CIO, a briefing was requested from the Administration or Key Staff Office. Based on the outcome of this briefing, a decision would be made as to whether a formal IPR was required. In FY 2001, the CIO Council and the Department's CIO decided that the information provided during each briefing adequately addressed all concerns about the IT investment. One exception was an IPR requested on VA's E-Commerce IT investment. The Office of Information and Technology (OI&T) still plans to execute this review during FY 2001. VA also initiated in FY 2001 an

expanded Capital Investment Review Program. This program integrates the use of contractors and VA staff. The contracted support will concentrate on conducting In-Process (IPRs) and Post-Implementation Reviews (PIRs) for approved capital investment proposals. VA staff will conduct PIRs from a random sampling of those IT investments approved by the Department's CIO. Three IT investments have been scheduled for a PIR. OI&T plans to execute these reviews in FY 2001. Two of these PIRs (The Image Management System (TIMS) and Compensation & Pension Training Performance Support System (TPSS), specifically address components of VETSNET, and one addresses a major IT investment (National Enrollment) being executed by the Veterans Health Administration.

10. When will we see the plan for VA's enterprise architecture? What steps will you take to ensure that this plan is completed? When will the plan be forwarded to Congress?

VA's Enterprise Architecture Plan is currently scheduled to be completed by August 1, 2001. Developing this plan has highest priority. VA will bring in world-renowned experts to work with the key business people to do this. In addition, top level staff will be assigned to the project to assure its completion. The plan will be forwarded to Congress as soon as it has the Secretary's approval.

11. Mr. Secretary, do you support the use of the Decision Support System at VHA? If so, how will you ensure that VHA achieves a full return on its investment in DSS? If not, why do you not support DSS use?

I fully support the use of DSS by VHA as a systems tool for aiding improvement in management of VHA. I have testified to the Committee on Oversight and Investigations that it is necessary to increase the accountability of VHA management to ensure that the resources provided by the Congress and this Administration are effectively and efficiently used. This can only be accomplished if VHA becomes more data-driven in its decision-making and commits itself to detailed analysis of its patient care and administrative systems. The same commercial software that supports DSS, which VHA has implemented, is used by management in over 1,400 hospitals and health care systems worldwide.

I will require the Under Secretary for Health to provide me a semiannual progress report on the utilization of the DSS. In this report, I will require that auditable evidence be provided showing progress made in achieving standardization within the DSS.

Additionally, I will require detailed evidence that increasing use of the system is being made to improve patient care and administrative practices. I will expect that within two years the system will have only small variances in compliance with the published system standardization guidance and that all VISNs can demonstrate substantial and material use of DSS' information.

12. GAO says that DSS use at your medical centers continues to vary despite the benefits demonstrated by those sites that now use DSS. How do you plan to improve DSS use throughout VHA?

We acknowledge that despite the demonstrated benefits that many sites currently enjoy as a consequence of using DSS, a number of sites across the system have been lagging in their use of DSS. The successful integration of DSS into the daily decision making processes of networks and medical centers will require two distinct, but not separate, lines of action. These actions will focus on communication and education and upon the integration of DSS data into the ongoing business decision processes within VHA.

The communication and education effort will focus on the successes, benefits and processes employed by DSS users both within and outside the VA health care system. We will benchmark and highlight successful applications of DSS data in patient care delivery and health care administration venues. Our focus will not only be on health care administration managers at the VISN and facility levels, but also on the clinicians involved in the direct delivery of health care.

In addition, we are identifying a variety of internal business processes which will benefit from the use of DSS data. Understanding which business processes will benefit from the use of DSS data and redesigning these processes to incorporate DSS data will send a clear message to all VHA management that we expect DSS to meet our information needs. Some examples of work currently in progress include the conversion from VHA's Cost Distribution Report to DSS data and the introduction of DSS data in the VERA allocation model. Other areas under review include the use of DSS data for sharing agreement negotiations, the use of DSS data as variables in development for local billing charges, and the use of DSS cost and workload data for VA's annual enrollment level decision analysis process.

13. Since top management support is critical to successful DSS implementation and use, how will you set the expectation that DSS will be used throughout VHA?

I agree that top management support is the key to success in all-important initiatives. Let me assure you that the Under Secretary for Health and I are in agreement about the potential benefits of DSS. For this reason, the Under Secretary for Health is preparing a plan for meeting the expectations he and I have with regard to DSS information use. The objective of this plan is to define and use measurable criteria to evaluate individual senior managers in their support and use of DSS.

14. Mr. Secretary, has the VETSNET pilot given you sufficient confidence in the new system to proceed to full implementation? If so, what steps will you take to ensure that VETSNET does successfully proceed to implementation?

I have directed that we will conduct an independent audit of the overall system before VETSNET becomes fully operational. This audit will provide me with the assurance that this system will meet all the security, functional and performance tests we have set for it. If VETSNET passes this audit, we will go forward with its implementation on our current schedule.

15. VBA Systems Modernization began in 1986 and has spent at least \$400 million to date with few benefits. How can long-term efforts with such limited results efforts be avoided in the future?

I have pledged not to spend any new funds on information technology until an Enterprise Architecture has been defined that ends "stove-pipe" systems design, incompatible systems development and data collection that does not yield useful information. I believe that developing this plan, which has my highest priority, will help us avoid efforts that offer only limited results.

**Post-Hearing Questions
Concerning the April 4, 2001, IT Hearing**

**For
The Department of Veterans Affairs**

**From
The Honorable Vic Snyder
Ranking Democratic Member,
Subcommittee on Oversight and Investigations
Committee on Veterans Affairs
U.S. House of Representatives**

1. According to various documents you provided, all status reports on VETSNET since July 2000 reported "Problems: Project in Trouble." As of January 5, 2001, only Project Management had improved to "Significant Issues Exist." Given the length of time this project has been in development, please explain why a "Project in Trouble" should be continued.

As a result of the use of the Project Management Methodology and the associated terminology such as "Problems: Project in Trouble," VETSNET has received a greatly improved management focus. I believe that the current VETSNET management plan addresses many of the past problems that resulted in such evaluations. In addition to these successes, which we believe validate our approach, ratification of the VETSNET strategy was obtained last year through an independent verification and validation of the VETSNET approach and technology by an outside contractor.

VBA is working to transform its methodology for development of new information systems, and to institutionalize those processes that will enhance the likelihood of success. VBA's Office of Information Management was recently reorganized to align the applications architecture function with the ongoing VETSNET and related development work at the St. Petersburg Regional Office. This will ensure that the VETSNET architecture will be adhered to as the standard development platform for all applications utilizing the VBA corporate database. Additionally, VBA is implementing configuration management technology throughout its major development projects. Configuration management enables more efficient software development through management and reuse of software code components, resulting in better software products. Finally VBA OIM is participating in a Department-wide effort to analyze and describe a VA Enterprise Architecture. This will result in better management of information

system and coordination of information technology efforts throughout the agency. A developmental task force has been appointed and is investigating project management software that all components of the Department can use to share information.

2. In the VETSNET Pilot, approximately 10 “handpicked, vanilla” original compensation award cases were to have been established in the St. Petersburg Regional Office. Our understanding is that small number was too large. Also, what do you mean by “handpicked” and “vanilla”, and what is the status of the VETSNET pilot?

In February 2001, the Veterans Benefits Administration (VBA) successfully piloted the processing of claims utilizing the VETSNET system. Ten veterans were paid using the pilot version of the VETSNET award and accounting system. This pilot effort tested all phases of VETSNET processing from claims establishment through Rating Board action to award payment and accounting. These veterans will continue to receive their monthly benefit checks through the VETSNET system. These successes have demonstrated that VETSNET is a viable system for processing C&P claims.

Ten veterans consented to be a part of this “pilot.” The claimants were veterans of the Army, Navy and Air Force. Collectively, their service covered World War II, the Vietnam era and the Gulf War. The age range of the claimants is 23 to 79 years old. Disability evaluations ranged from 10% to 50%. Two of the awards included additional benefits for dependents. Nine veterans were entitled to retroactive payments totaling \$12,998. The total monthly recurring payment is \$2,782.

The ten pilot cases were “handpicked” in that they were called and asked to participate in the new payment system, and they had to elect Electronic Funds Transfer (EFT) for their payment. The status of the pilot is that it is operational and every month these 10 veterans are receiving their payment through VETSNET.

3. Why will the pilot only use “original award cases”?

The pilot “original award cases” were completely and successfully processed using the new software. The conversion process from the Benefits Delivery Network (BDN) to VETSNET is not yet complete. We used “original award cases” because they would not require a conversion from BDN to VETSNET.

4. After so many years and so many millions of dollars, what is this pilot supposed to prove?

The most significant aspect of the pilot is that it proves we can pay successfully using a system other than the BDN methodology. As a result, we are confident that we can run in parallel until the new methodology is completely tested and the conversion process is complete. Therefore, the pilot has already successfully proved that the software that will be used to generate ratings, record decisions, generate and authorize the awards and make payment is completely functional.

5. VA cannot tell us how much money it has spent on VETSNET. Can you tell us how many employees have worked only on VETSNET since they started work at VA?

Since inception of the effort in 1996, VA has expended approximately \$20 million on VETSNET. Included in this amount are payroll funds to support an average of 14 full-time employees. None of these employees have worked only on

VETSNET since they started work at VA. All have been reassigned to VETSNET, having been previously employed throughout VBA in other capacities.

6. Describe the VETSNET responsibilities currently being handled by Hines.

Hines is responsible for the database conversion from Benefits Delivery Network to VETSNET, and for defining and developing batch and interface processing. Hines also has responsibility for operational management of the VETSNET hardware. Additionally, and more significantly, a core group at Hines is learning the new software language and methodology.

7. The institutional expertise resident at Hines is essential to maintain the current payment systems for 3.2 million veterans per month, but for further development of VETSNET also. It would appear after so many years of work, VETSNET continues to be a drain on the remaining staff at Hines. It appears that a significantly diminished staff at Hines has been assigned significantly more responsibility, not just for paying benefits to America's disabled veterans, but for VETSNET as well. Is the VA doing anything to support Hines with its responsibilities?

Hines is and will continue to be an important resource. Therefore, we have taken several steps to ensure Hines continues to fulfill its assigned responsibilities. For example, we have merged the Hines Benefits Delivery Center and System

Development Center into one organization. One benefit of this measure is increased flexibility to assign resources to tasks performed by Hines. We have also prioritized the workload consistent with resources available at Hines. We have also committed to providing Compensation and Pension (C&P) business staffing support to Hines to ensure the development of functional requirements for the conversion and transfer from BDN to the new system.

8. In a November 1, 1993 hearing before the Subcommittee on Compensation, Pension, and Insurance, VA said VETSNET would “replace the existing BDN (Benefits Delivery System).” It has not done so. In a June 8, 1998 report, the SRA consulting firm worried that “conversion of BDN data” for VETSNET may corrupt the database”. If VETSNET does not, “meet all of the security, functional, and performance requirements” you have set for it, will this be the final evaluation?

As I indicated in my testimony, I will not throw good money after bad. If VETSNET does not pass the independent audit I have ordered, we will develop a plan to extend the life of our current systems and immediately begin to develop a replacement system.

9. How many dedicated information security officers does the VA have now? How many are you planning to hire?

VA has an extensive community of information security staff. These include facility and Staff Office/Program Office Information Security Officers (ISO), their respective Alternate ISOs (sometimes multiple at facilities), security program office staff, and contractors. Every VA facility is required to have a full-time or primary-time ISO. The approximate number of ISOs and Alternate ISOs is 580. The overall security community is larger when security program offices are considered. Note that with the exception of ISOs, many of these positions are part-time. Our GISRA review process will identify the prevalence of full-time ISOs at VA facilities. Based on these analyses, the Cyber Security Office will provide direction to those facilities not having full-time ISO positions to establish the position.

10. Will the new Security Czar have only the authority to promulgate policies, or also be able to enforce them?

The VA Cyber Security Office plans to work with all levels of VA to enhance our enforcement capabilities. Specifically, it will work closely with VA's Office of the Inspector General (OIG) and with high-level VA staff officials and Administration

leaders to use existing enforcement capabilities in the interest of information security. The Cyber Security Office will have the ability not only to promulgate policies but also to determine compliance therewith. Where non-compliance is found, appropriate action will be taken.

11. How seriously do you take the IG's Penetration Review, which seems to indicate considerable vulnerability and possibility of fraud and tampering?

The VA Cyber Security Office recognizes and respects the OIG's work in the information security arena and specifically their penetration studies. We take their Reviews as primary evidence for the development of our overall security plan. In fact, OIG's studies validate our own findings and experiences. We look forward to working closely with OIG in the interest of protecting the Department's information assets.

12 What level of confidence do you have that a new system at Austin will act as well as what you now have in Hines?

We currently have a high level of confidence that Austin can successfully perform the operational part of this new system. The decision to do this at Austin is consistent with our efforts to accomplish data center consolidation. However, we will not become dependent on this arrangement until we have conducted extensive testing and run the new system in parallel with the old. Also, Hines will continue to perform functions that ensure the successful applications payment process and other necessary activities such as configuration and data base management.

13. Austin uses a computer tape backup system that major corporations have considered obsolete for 5 or more years. Today, major corporations use remote mirroring technology, which provides simultaneous backup on a parallel system. Until Austin can get up-to-date, shouldn't the VA plan to use Hines for backup?

Many corporations do use remote mirroring technology for mission-critical applications requiring near 100 percent availability, data mirroring, and data replication. However, many corporations also still utilize the same or similar computer tape backup systems that are utilized at Austin and other VA computing centers. There are significant cost considerations to be weighed when deciding upon an enterprise-wide backup and storage approach. Remote mirroring and/or replication require significantly higher investments in hardware, software, and telecommunications. This may be appropriate in some cases, while tape technology may meet business requirements for other business applications. As a fee-for-service provider under the VA's Franchise Fund, the

Austin Automation Center (AAC) provides services to VA and other government agencies through the execution of customer agreements, accompanied by performance service level agreements (PSLAs). Current customer agreements and PSLAs do not contain requirements that necessitate remote mirroring or replication services. However, the AAC is strategically positioned to provide such services should they be required. The AAC has the technology that can easily support data mirroring and replication, either locally or remotely.