

**Questions for the Record
From Chairman Steve Buyer
Subcommittee on Oversight and Investigations
Committee on Veterans Affairs
October 6, 2004**

Hearing on VA' Smart Card Initiative(s)

Question 1: How many VA smart card projects or demonstrations have been initiated in the last 10 years? How much money has been spent on each of these projects and demonstrations? How many of them have been implemented and are still in existence?

Response: Two VA smart card projects or demonstrations have been initiated in the last 10 years:

a. The Authentication and Authorization Infrastructure Project (AAIP) is an OMB approved project with a 5 year budget of \$172 million. The project provides for the One-VA ID card based on a smart card form factor, and is compliant with the mandates of HSPD-12, issued by the White House on August 27, 2004. In FY04, the project expended approximately \$26 million. Most of these funds were targeted at infrastructure, systems, issuance stations, and smart card stock along with technical support costs.

b. The One-VA Express Card pilot ran from January to May 2001. This pilot involved two locations, Iron Mountain, MI and Milwaukee, WI. The purpose was to determine if the best and most cost effective technology to make registration and clinical data available between medical facilities in real time was to use a) the smart card or b) a network centric technology available through VistA. Expenditures for the pilot were \$5.3 million. Approximately 40,000 cards were issued. This pilot was not implemented nationwide because the network-centric approach using VistA was preferred and found to be more cost effective.

In addition, VA has in place two other card projects, neither of which contains a computer chip:

a. The Veterans Identification Card (VIC) Replacement Project replaces existing veteran identification cards that display sensitive veteran information and utilizes aging hardware that is failing and can not be repaired.. The primary purpose of project was to remove visible personal identifying information (such as SSN and date of birth) from face of cards to protect veterans from identity theft. The photo of veteran was enhanced from black and white to larger color image. The VIC Project was a result of the halt of the One-VA Express Card project. To the extent possible, the VIC project re-used One-VA Express Card software developed for the project and learned from the work done during the pilot.

VIC is a "dumb" card, not a smart card. VIC is able to reuse existing software for the workstation application, Vista, and the National Card Management Directory from the One-VA Express project with some modifications. National deployment began August 30, 2004 and will be completed in November 2004. Estimated total volume of cards produced is 2.5 million in the first year of production and 1 million in subsequent years. First year production budget is \$3.5 million that includes funding for 2 workstations and camera configuration for each medical center and the external card vendor production costs for the 2.5 million cards. Funding in subsequent years will be covered by the Health Eligibility Center budget.

b. The Miami VA Medical Center swipe card pilot was started in August 2003 and is currently being conducted. This pilot was designed to validate the use of one specific technical solution in an effort to collect data on physician acceptance of an automated timekeeping system, obtain feedback from physicians on the use of the technology, and to provide guidance concerning timekeeping processes for part-time physicians. Already planned expenditures for the system of readers and cards were expedited so no additional, unbudgeted funds were used. Staffs involved in coordinating the pilot have done this as a collateral duty. No additional staff or contractors were hired to support the effort. Approximately 60 cards issued. The technology was evaluated and found to function successfully at providing data on physician entrance and exit. It also is compatible with AAIP technology.

Question 2: Under what circumstances would a VA employee be required to provide fingerprint and/or iris scan identification?

Response: Currently the only biometric captured is a digital photo, which is accomplished to comply with the requirements of the Common Certificate Policy (www.cio.gov/ficc). This is the same digital photo that is printed onto the cards. Unless emerging federal policy (FIPS-201) requires otherwise, VA does not plan to collect fingerprint and/or iris scan templates.

Question 3: Who makes the determination about the issuance of a smart card?

Response: Smart card issuance is only authorized when an appropriate, designated management official requests that a credential be issued.

Question 4: How many smart card projects are currently underway? Where do these projects reside? Are they all within the IT department?

Response: One smart card project is currently underway and that is the AAIP Project managed by the Office of Cyber and Information Security, Office of the Assistant Secretary for Information and Technology.

Question 5: How much money has VA spent on its smart card projects in the last 10 years?

Response: VA has spend \$35.3M on smart card projects in the last 10 years; .AAIP - \$30M from FY03 – FY 04; and One-VA Express Card Pilot - \$5.3M from 01 FY 01 – 05 FY 01.

Question 6: Why did it take three years to address and implement additional safeguards after a \$6 million compensation and pension fraud case was uncovered at the Bay Pines, Florida Regional Office?

Response: Following discovery of the fraud case, the Under Secretary for Benefits (USB) requested the Office of Inspector General's assistance in identifying internal control weaknesses that might facilitate or contribute to fraud in the compensation and pension (C&P) benefits program.

The OIG audited internal controls for adjudication and payment of C&P benefits at the St. Petersburg Regional Office. The July 2000 OIG audit report made 15 recommendations with 26 independent reportable action items to strengthen internal controls. The recommendations generally addressed areas such as physical and electronic security of sensitive files and records; access and security controls for VBA's benefit payment system, the Benefits Delivery Network (BDN); and employee conflict of interest.

VBA took prompt action to strengthen procedural controls for the adjudication of claims of former employees, relatives, and veteran service organization (VSO) employees. Action was taken to ensure VBA and VSO employee claims folders were transferred to the VARO of jurisdiction and properly secured. VARO directors are required to certify this process annually. Certification is also required annually to ensure that all employee relatives have been identified and records of family members have been appropriately transferred and electronically secured.

The Under Secretary for Benefits advised all employees about the expectations of employee conduct and avoidance of conflict of interest and instituted an annual all-employee ethics training program.

VA also took action on the OIG's recommendations to strengthen the system audits and controls of the BDN. However, a number of the recommended changes to the BDN were determined to be infeasible because of the antiquated architecture of this complex system and the resource levels that would be required to make the recommended changes. VA therefore put new interim controls in place and committed to making the recommended changes in the Modern Award Processing System, a major component of the BDN replacement system known as VETSNET.

The OIG's recommendation from the St. Petersburg audit that VBA establish a system control to prevent release of payments greater than \$15,000 without the authorization of a third person was among those determined to be infeasible because of the antiquated BDN system architecture. However, following discovery of the Atlanta case, VBA took additional steps to strengthen the integrity of the compensation and pension program by immediately instituting a mandatory large payment verification process. Effective in September 2001, regional office directors are responsible for verifying and certifying the propriety of all retroactive payments of \$25,000 or more. Since the start of this review, nearly 58,000 payments totaling over \$2.8 billion have been reviewed through this process. The process is audited by the OIG through their Combined Assessment Program Reviews and VBA C&P Service site visits. The system-generated third-person authorization process as recommended by the OIG is included in the design of the VETSNET Modern Award Processing System.

Of the 26 internal control action items recommended by the OIG following the audit of the St. Petersburg Regional Office, 21 have been fully implemented and are considered closed by the OIG. Of the remaining five action items, two are awaiting OIG's validation of VBA's report that they have been fully implemented. A third action item is expected to be closed by the OIG by the end of calendar year 2004. The remaining two action items recommend system controls to restrict adjudication of employee claims to only the regional office of jurisdiction and automation of the third-person authorization process for large payments. These two action items are included in the design of the Modern Award Processing System.

Question 7: When will VBA implement a VA smart card with biometrics that could specifically preclude the internal employee fraud that occurred in Bay Pines, Atlanta and Manhattan?

Response: The Veterans Benefits Administration (VBA) will implement the standard VA smart card approximately six months after deployment of Windows 2003 servers and Active Directory. The deployment of Windows 2003 servers and Active Directory must be completed first as a necessary precursor to successful use of this type of smart card. It is currently envisioned that the standard VA smart card will be a smart card with PIN (personal identification number). This type of smart card is consistent with government-wide practice to accomplish control and monitoring of sensitive information, work stations, physical facilities, etc.

This advanced security technology as we currently understand it would not have precluded the internal employee fraud that occurred in Bay Pines, Atlanta, or Manhattan as the employees involved in these cases were authorized to perform the system functions used to perpetrate their criminal activities. As recommended by the OIG, VBA has already implemented changes to the Benefits Delivery Network and its replacement system (Modern Award

Processing/VETSNET) to make SSN the employee corporate identifier and link transactions to SSN.

Question 8: Assuming that smart card technology will allow a user to log on to a PC, will the user, after the initial log on, still be required to enter various additional passwords to access other systems or applications (for example, VISTA, CPRS, MyHealtheVet)?

Response: The One-VA ID Card issued through the AAIP project does provide for network based logon using digital credentials. However, the initial deployment of the AAIP card at the first VHA test site (Fayetteville, AR) will allow the user to log onto the network, but will not provide additional sign-on capabilities.

The AAIP project team is testing a "simplified sign-on" process, which when implemented, will allow users easy sign on to applications such as VistA, CPRS and MyHealtheVet. Once testing is complete and successful, this functionality will be implemented in the pilot test sites. After logon, and depending on the status of system integration efforts, users will be able to concurrently logon to other applications. This may occur through web interfaces, or through other forms of single sign on (SSO) technology. Currently, SSO technologies are under a prototype review to specifically identify implementation requirements. Initial results are expected in Q3 of FY05.