

Prepared Statement of

**Robert J. Brandewie
Director, Defense Manpower Data Center**

Before the House Committee on Veterans' Affairs

**Oversight Hearing on the Department of Veterans Affairs
Information Technology Infrastructure Reorganization**

June 28, 2006

Not for publication until released by the Committee

Chairman Buyer and Members of the Committee, thank you for the opportunity to appear before you today to discuss the data exchanges between the Department of Defense (DoD) and the Department of Veterans Affairs (DVA). I would also like to include an overview of our actions in identifying Active Duty, National Guard, and Reserve members whose information may have been present on a laptop computer stolen from a DVA employee's home and briefly discuss some of the data security measures we employ.

As a prelude to discussing the data exchanges, I would like to note that the Defense Manpower Data Center (DMDC) is the central repository of automated human resource information within DoD. We receive and maintain personnel data on Active Duty and reserve component military members, retired Service members, civilian employees of the Department, some DoD contractors, and many family members. This data is used as the basis for issuance of member and dependent ID cards, eligibility for benefits such as medical care, and to conduct operational programs such as identity management and the Montgomery GI Bill program. Thus, DMDC is at the center of most of the human resource information flowing between DoD and the DVA. It is important to note that other parts of the DoD also exchange information (for example medical records) with DVA, but that the most comprehensive exchanges occur between DMDC and DVA. These exchanges are very basic to providing an improved experience for the veteran and also to coordination of benefits between the two Departments. These exchanges have been going on for more than 25 years.

The purpose of the data exchanges between DVA and DMDC are twofold—to provide information to the DVA on currently serving and recently separated individuals who are eligible for DVA benefits and services, and to competently administer programs in both agencies that benefit Service members, former Service members, and their families. In accordance with the Privacy Act, these data exchanges are disclosed in various Computer Matching Agreements and are in the Federal Register under Systems Notices S322.10 and S322.50. The exchanges can be categorized as follows:

- **Data for administering educational programs:** Data is exchanged on participants in both the Active Duty and Selected Reserve Montgomery GI Bill programs. Data exchanges are also being initiated for Guard and Reserve personnel who served in support of a contingency and for the National Call to Service programs recently established by the Congress.
- **Data for administering insurance programs:** Data is exchanged on medically retired members with service disabilities and recently separated Reservists so they can be notified of their eligibility for Veteran's Group Life Insurance.
- **Data for assessing post-war illnesses:** Data is exchanged on separated Active Duty members and Guard/Reserve members coming off Active Duty who have served in the first Gulf War and in Operations Iraqi Freedom/Enduring Freedom for purposes of post deployment medical assessments.
- **Data for prevention of fraud, waste, and abuse:** Data is exchanged to ensure correct pay amounts and offsets for veterans receiving DVA compensation benefits as well as to prevent the member from inappropriately receiving compensation from DoD and DVA simultaneously.
- **Data to estimate veteran population and expedite delivery of benefits:** Data is provided to DVA on Active Duty enlisted and Guard/Reserve accessions so DVA can establish a skeletal record at time of entry and verify their DoD affiliation. DMDC subsequently provides DVA with additional detailed information at the time a member separates or retires.

Data exchanges with the DVA, although long standing, have been expanded in breadth in recent years and an effort to consolidate the exchanges began in earnest about three years ago. Close cooperation and increased exchanges of information have also received encouragement from the Congress and the Administration. Public Law 107-347 established the Office of Electronic Government in the Office of Management and Budget (OMB). OMB oversees the President's Management Agenda and had an agenda initiative in 2002 to ". . . improve coordination of health care and eliminate potentially duplicative budgeting by sharing data between VA and DoD." Additionally, the President's Management Agenda directed efforts to make the transition from DoD to the DVA seamless – " Transition should be seamless from the veteran's perspective and could be made seamless through data sharing between VA and DoD,

as well as within VA” (page 70). Public Law 108-136 established an interagency committee known as the DVA-DoD Joint Executive Council to direct joint coordination and data sharing efforts between the two Departments. As a result, DoD and DVA have been working an initiative to obtain full interoperability between appropriate DVA and DoD automated systems to enhance the transfer of data and the delivery of benefits. At the current time, some information is flowing machine-to-machine between DMDC and the DVA's One VA initiative known as the VA/DoD Identity Repository (VADIR). All data exchanges are scheduled to be consolidated and near real-time in 2008.

DoD believes that there is great value to current Service members and veterans in the close cooperation, evidenced by these data exchanges, that has developed between DoD and the Department of Veterans' Affairs. However, it is equally important that the exchanges are done with the utmost attention to security to ensure no unauthorized disclosure of information. Current DoD policy requires that Privacy Act and other sensitive but unclassified information be protected while being transmitted. DoD and DVA have taken a number of steps to ensure that the information we exchange remains safe from unauthorized disclosure. In keeping with DoD policy, in June 2003 DMDC established a policy that all data exchanges that contain privacy protected information would be done using secure technologies. These technologies include data encryption, the use of Virtual Private Networks (VPN), and the use of commercial secure transfer services like Connect:Direct. This policy would apply both to information transfers within the Department and between sister agencies. The DVA was a partner in the implementation of secure transfer and we have continued to add security to our transfer process. Most recently both agencies migrated to a new version of Connect:Direct - Secure+. This product adds data encryption services to its existing secure transfer technology.

I will now turn and discuss our actions resulting from the theft of data on a laptop computer from a DVA employees' home. On June 1, DMDC was requested to match the Social Security Numbers (SSN) of individuals that may have been present on the stolen computer against current Active Duty and Reserve and Guard personnel files.

The stolen data may have included data extracted from the DVA's Beneficiary Identification and Records Locator Subsystem or BIRLS file. We knew that the accession data we provide to DVA was included on the BIRLS database and began working with DVA Headquarters and their Austin, TX center. On June 2, Austin sent us 19.6 million records—those with SSNs—from the compromised BIRLS extract over a secure connection. Over the weekend of June 3-4, we matched SSNs from the 19.6 million BIRLS extract records against our master database of about 27 million records and found a large number of Active Duty, National Guard, and Reserve members in the BIRLS extract.

On June 5, we validated our work by matching the two large datasets once again and early on June 6 confirmed the results. The numbers were provided to the leadership of DoD and to DVA on June 6 and SSN level detailed records were provided to each of the Military Services on June 8. We also received from the DVA's Austin center about 6.8 million records from the BIRLS extract file that did not have SSNs and have matched a few of them to Active Duty, Guard and Reserve members. In addition, we used the data provided by VA to identify other members of the DoD community (civilian employees, retirees, etc.) potentially impacted by the data loss. We also examined the impact on dependents of DoD members.

Over the next several days, we worked with DVA to refine the list of SSNs that were stolen. They indicated that some SSNs on the BIRLS extract were not compromised and some SSNs not on BIRLS were. They provided these new datasets to us and we refined the list of individuals whose data was stolen. The final numbers show about approximately 1.1 million currently serving Active Duty, 415, 000 Guard, and 633,000 Reserve members were potentially impacted. Of these, about 146,000 Active Duty, 34,000 Guardsmen, and 25,000 Reservists are currently serving in Operation Enduring Freedom or Operation Iraqi Freedom.

We continue to work closely with the VA on mitigation efforts with respect to the compromised information. Our leadership in the Office of the Under Secretary of

Defense (Personnel and Readiness) has given their full support and we have offered the resources of the DMDC where they can be helpful. In spite of this tragic loss, it is important to reinforce the point that there are many benefits to the current data exchanges between the two Departments, they are done securely, and they result in better service and benefit delivery for Service members and veterans.

Mr. Chairman I thank the committee for the opportunity to report on data exchanges between the DoD and the DVA and would welcome the opportunity to answer any questions.