Statement of Ronald R. Aument
Deputy Under Secretary for Benefits
Before the
House Committee on Veterans Affairs
June 29, 2006

Mr. Chairman and Members of the Committee, thank you for the opportunity to provide testimony on data security in the Veterans Benefits Administration (VBA).

As a result of the most unfortunate theft of data from the home of a VA employee, VBA is conducting a thorough examination of every aspect of our information security program, our processes, and our procedures to ensure that sensitive veterans' data is neither mismanaged nor used for any unauthorized purpose. This statement outlines the security measures VBA had in place prior to May 3, 2006, what we have done to communicate with veterans about the data theft, and additional steps we have taken regarding our data security policies and procedures. It also specifically addresses the security of the data feeds between VBA and DoD.

We take the privilege of serving veterans very seriously, and we have taken direct and immediate action to address veterans' concerns and to restore their confidence.

IT SECURITY POLICIES AND INITIATIVES PRIOR TO MAY 3, 2006

VBA has incorporated security into its information systems and processes to support the delivery of veterans benefits. VBA has extensive, well-articulated policies and procedures governing information access requests, auditing, and rules of behavior. These policies and procedures pertain to all VBA employees,

as well as to those individuals, including consultants, to whom VBA authorizes access to VBA systems and data.

Responsibility for all IT security policy was centralized to the Department's Office of Cyber and Information Security, which reports directly to VA's Chief Information Officer. Implementation of IT security policy and procedures in VBA is through a three-layer organizational assignment of responsibilities. The Information Security Officer (ISO) at each regional office is responsible for the execution and oversight of IT security policy and procedures. The Network Support Centers (NSCs) provide oversight of regional office (RO) compliance with IT security policy and procedures and expert advice to the RO ISO community and IT staffs on technical issues. The VBA IT organization in Headquarters provides the technological support that implements IT security and procedures on the computer applications and systems managed for VBA.

All 58 VBA ISOs nationwide, as well as the employees of the Network Support Centers and VBA Headquarters security staff, were detailed to the VA Office of Information and Technology on May 1, 2006, as part of the implementation of the VA IT reorganization. They will be permanently assigned to that office on October 1, 2006.

Under the IT reorganization, VBA business lines retain an important support role in the internal management of IT security. VBA continues to be responsible for managing data, its use and disposition. We fully understand the importance of securing access to our systems as required by the FISMA and Certification and Accreditation (C&A) processes. VBA business lines are responsible for authorizing access to VBA computer applications at the appropriate security levels. True business "need to know" must be established, and compliance with the various legal requirements of the Privacy Act, Freedom of Information Act, Privacy Act Systems of Records, and memorandums of agreement must be determined before access is authorized.

The standard configuration of VBA servers and desktop and laptop computers is centrally controlled. Updates are deployed automatically to maintain quality assurance and security. When a server or workstation is connected to the network, the VBA standard configuration is automatically loaded.

There is also a secure technology solution in place for individuals requiring access to VBA systems from outside our controlled LAN environment. That solution requires external users to access VBA systems through the One-VA Virtual Private Network (VPN) to a Centralized Terminal Server. The One-VA Virtual Private Network (VPN) allows remote users to access VA systems in a secure environment. In addition, the computers used for VPN access must be protected through the use of the Office of Cyber and Information Security approved anti-virus and "personal firewall" software prior to using VPN. The use of this software is required for VPN access to protect the VA network from communications containing potentially malicious software. VPN data communications are encrypted.

The One VA Terminal Server, located in the VBA-controlled computer room, contains all the files, programs, and database information. VBA outbased workers, as well as authorized Veterans Service Organization (VSO) representatives, use this capability. Additionally, the Veterans Information Portal provides secure, encrypted user access to Loan Guaranty applications for internal and external users.

VBA has established rules-of-behavior policies that comply with VA requirements and govern the use of IT systems and capabilities maintained by or for VA. All users authorized to access VA systems through Local Area Networks or through the One VA Virtual Private Network are required to sign VBA-specific rules of behavior. VBA rules of behavior have also been developed for

employees authorized to use government-owned laptop computers. These VBA rules of behavior ensure all users of VA IT resources are aware that any system potentially contains valuable and sometimes sensitive government and/or personal information, which must be protected to prevent disclosure, unauthorized changes, and loss.

Individuals are granted systems access by delegated approving officials who determine access levels based on the employees' work requirements. Prior to being given access permissions, each individual requesting access to a VBA information system must sign a certification of receipt and understanding of the VBA-specific rules of behavior governing the use of VBA IT resources. The rules of behavior advise users that misuse of government systems, mishandling of veteran data, or unauthorized disclosure of sensitive information could result in disciplinary action up to and including termination of employment. During regular site visits, VBA's Network Support Centers review user security folders maintained by the ISOs to ensure signed rules of behavior are in the folders.

User password construction requirements and expiration limits for all VBA applications comply with VA requirements. Additionally, users must complete both security and privacy training. The Secretary recently directed that all employees sign a Statement of Commitment and Understanding on completion of the training, confirming their understanding of the training, their commitment to protecting sensitive and confidential information, and the consequences for noncompliance.

VBA also has a formal process for requesting data extracts from VBA information systems. A Project Initiation Request (PIR) is a request to the VBA Office of Information Management (OIM) for information technology services initiated by both VBA and VA entities. The PIR is prepared primarily by a sponsor organization to notify OIM of a new system requirement, a modification or change to a requirement, an enhancement to an existing system, or a request

for a data extract or match. For example, VBA provides 15 different extracts from the Beneficiary Identification and Records Locator System (BIRLS) to internal VA organizational elements as well as external agencies. Data is matched and/or extracted from BIRLS for purposes such as identification of inactive claims folders eligible for retirement to a storage facility; verification of veteran status for Department of Education benefit applicants; identification of VA employees in the PAID system who are also veterans; death matches with the Veterans Health Administration and the Social Security Administration; investigations by the Office of the Inspector General; and research projects by the National Academy of Sciences Institute of Medicine. Additionally, there are four interfaces or data feeds into BIRLS: two from the Defense Manpower Data Center for new servicemembers and reservists and to provide retired pay information; one from the VBA Benefits Delivery Network (BDN) claims processing system to update BIRLS based on recent BDN record changes and transactions; and one from the Veterans Assistance Discharge System (VADS) for recent separatees. Each extract and interface was established through a formal VBA approval process. Modification of any data provided electronically is prohibited.

In 2005, VBA issued a detailed directive for Information Security Officers (ISOs), who are critically important to data security. ISOs manage local access control to IT resources, conduct security audits, and are the focal point for incident reporting in a VBA facility. The VBA internal controls process requires local systematic analyses of operations. RO directors certify annually that their facilities are in compliance with VBA directives.

VBA Network Support Centers also conduct annual surveys of IT operations and security controls, policies, and procedures at their client ROs within their geographical area of jurisdiction. The primary purpose of these on-site security visits is to ensure that the ROs are adhering to all VA, VBA, and

other federal security directives and handbooks and that deficiencies identified in previous CAP reviews are remediated.

VBA completed the Federally mandated certification and accreditation (C&A) of 97 application systems on schedule in August 2005. We will maintain C&A through a 3-year C&A update cycle.

The VA Office of Inspector General (OIG) regularly conducts independent examinations of VBA operations. For example, through the Combined Assessment Program (CAP), OIG examines all RO business processes, including adherence to information security policies and directives. We have reviewed all IT and security-related findings and recommendations made during FY05 and FY06 OIG CAP Reviews. The majority of identified deficiencies are remediated during the time the OIG is still on site. Recommendations that cannot be remediated immediately are referred to the Network Support Center (NSCs) to ensure appropriate and timely remediation. Action has been completed on all recommendations made by the OIG during the CAP reviews, and all recommendations have been closed by the OIG.

The Department has improved controls through the establishment of the Office of Cyber and Information Security (OCIS); VBA continues to update and enhance internal policies and procedures. In 2002, VBA issued comprehensive directives for IT Systems General Security Requirements (April 2, 2002) and Benefits Delivery Network Privacy and Security (August 28, 2002). These policy directives were revised and updated January 6, 2004. On January 28, 2005 we distributed another handbook that provided all VBA Information Security Officers with detailed guidance regarding their duties and responsibilities for RO security operations.

As part of our ongoing efforts to strengthen IT security, VBA has successfully tested its disaster recovery procedures for 29 of 31 major

applications, and has invested in a fully redundant system to provide disaster recovery for the Benefits Delivery Network (BDN). The system has been installed, and a test of the recovery of all BDN applications was completed in September 2005. The test will be repeated yearly.

VBA is in the process of completing the final two core applications of the VETSNET system, which will replace the legacy Benefits Delivery Network system for delivery of compensation and pension benefits. VBA continues to build security and appropriate audit trail capability into VETSNET. VETSNET applications utilize journal tables in the corporate database to retain the sequence of events that change the records for each veteran and claimant record. Every corporate database table containing veteran and claimant data has an associated journal database table. Every VETSNET application transaction that changes veteran and claimant data is journaled. Journal information includes the state of the record prior to the change, the change made, the user enacting the change, the station from which this change occurred, and the date and time the change was entered.

Specific Business Line Access Issues

In all VBA's benefits systems, veteran data is protected by VBA security policy and IT system and application security controls. Programmatic access controls restrict access according to the specific veteran record level of sensitivity and the authority of the individual accessing the data.

Veterans Service Organization (VSO) Access to Veterans' Information

VSOs are strong partners in VA's mission, providing advice and representation to millions of veterans and their dependents each year. The law permits VA to disclose information on specific VA claimants to "duly authorized" VSOs. In performing their duties, the VSOs routinely access sensitive VA information regarding their clients. Claimants or beneficiaries must sign a power of attorney to allow a VSO to obtain access to their records.

VSO representatives who are co-located at VBA sites, as well as many VSO representatives who work at non-VA facilities, have access to some of the same IT systems which VA employees access. These systems are restricted so that VSO representatives can only access information regarding their organization's clients, and only if they have a power of attorney. In addition to VA's procedures for safeguarding sensitive information, the Veterans Service Organizations themselves have procedures for controlling access and dissemination of such information. The One-VA Virtual Private Network (VPN) allows remote VSO users to access VA systems in a secure environment.

Outbased Employees

VBA has a significant number of employees who are required to be out-based by the nature of their positions and who must have personally identifying information for VA beneficiaries available to them in order to carry out their responsibilities. Employees working in the field and at outbased locations are needed in almost all of VBA's business lines.

Field examiners make periodic home visits to incompetent VA beneficiaries and their fiduciaries to assess their competence, adjustment, and personal welfare. Education Compliance Survey Specialists and Education Liaison Representatives travel to schools to review student records. VR&E Counselors are located in more than 120 outbased locations, providing improved access to veterans in communities distant from our regional offices. Loan Guaranty's Monitoring Unit performs oversight of VA lender operations through a program of performance audits conducted on site at lenders' offices and at their home office in Nashville. We ensure that our outbased offices have the same level of security that our Local Area Network (LAN) environment offers in VA facilities. Employees such as Field Examiners who often work out of their homes access VA systems through the One VA VPN.

QTC Medical Examinations

Since 1998, VBA has contracted with a private vendor, QTC Medical Services, Inc., to perform approximately 16% of our disability examination workload. This program was initiated under the authority of P.L. 104-275 and has become a standard program since that time to supplement the need for disability examinations at ten regional offices.

The data used by QTC for medical examinations is entered into the Veterans Examination Request Information System (VERIS), maintained on VBA's Intranet server by Veterans Service Representatives at the ten regional offices and their Benefits Delivery at Discharge (BDD) sites. Each night, the VERIS server compiles an encrypted file that is transferred to QTC for downloading into QTC's password-protected internal network.

For claims that require the examiner to review medical documentation, the regional offices ship the claims folders by FedEx. QTC scans and prints the medical documentation and sends the information to the examiner using USPS overnight priority mail. When the examiner has completed the examination, the documentation is shredded. QTC is responsible for returning the claims folders within five days of the completed appointment and uses UPS ground services for shipping.

The contract requires that QTC post the completed examination reports on a secure website and only provide access to VBA-authorized users. QTC employees e-mail VA employees through the use of VPN and have access only to VBA's Exchange e-mail server.

Vocational Rehabilitation and Employment Contract Counselors

The Vocational Rehabilitation and Employment program utilizes contract counselors to supplement and complement the work performed by VA counselors. These contract counselors do not have access to VBA computer

systems or any VR&E computer applications. Contract counselors are provided with paper copies of veterans' VR&E records from the Counseling/Evaluation/ Rehabilitation (CER) files. These records do contain veterans' personal information. Contract agreements contain specific clauses regarding privacy and security, in which the contractor commits to secure all information. In addition, many of the contract counselors are Certified Rehabilitation Counselors and are held to the Code of Professional Ethics from the Commission on Rehabilitation Counselor Certification, which directly addresses the confidentiality of client records. VR&E Officers are responsible for ongoing audits of contractor work.

Loan Guaranty Contractors

Electronic data transmissions between Loan Guaranty Service and its contractors, Ocwen and Countrywide Home Loans (CHL), are via a secure communications network. Both Ocwen and CHL have documented and tested procedures and policies regarding control and release of information. These range from restricted access to the use of internal audit and oversight groups who monitor compliance. There are also external audits conducted to monitor compliance. Both contracts include specific requirements that charge the contractor with data and system security. VA audits these contractors, as do auditors both internal and external to the companies.

ACTIONS TAKEN TO INFORM VETERANS ABOUT THE DATA THEFT

VA has taken aggressive action to notify veterans and to respond to their inquiries regarding the data theft. Upon learning of the data theft, VBA developed a plan for staffing and training regional office public contact teams, working extended hours, and enhancing our telephone system capacity. We contracted with the General Services Administration to provide commercial call center services to answer veterans' calls about the loss of personally identifiable information. VBA staff met with contractors to set expectations and to review procedures. A VBA employee is on site at each contracted call center location to provide assistance and guidance. Scripted responses to potential questions

were developed for the call centers and regional office public contact staff. These scripted questions and answers have been updated as we learn more about the situation and gain experience with the nature of the concerns expressed by the callers.

Since our veterans are increasingly using the web and e-mail, we established a single center to respond to these queries and to ensure uniform, correct information is delivered.

We also updated and strengthened procedures for handling veterans' requests to change address and direct deposit information to ensure proper verification of identity of the individual requesting the change. In an average month, we receive in excess of 40,000 requests from VA beneficiaries to change their financial institution and/or address.

TECHNICAL AND POLICY CHANGES SINCE DATA LOSS INCIDENT

In March of this year, just prior to the data theft incident, we started the process to accelerate implementation of Public Key Infrastructure technology (PKI) throughout VBA. PKI will provide a common utility for VA to support more secure electronic transactions and e-mail. It will allow VBA users to more securely send veteran-sensitive information (social security number, medical conditions and diagnostic codes, etc.) to VHA and other VA elements.

Since the May 3 security incident, VBA has supported the Secretary's direction to accelerate the annually required Privacy Awareness and Cyber Security training. VBA's previously issued training directives required training to be completed by the end of the fiscal year. All VBA employees are now required to complete these training programs by June 30, 2006.

VBA is also examining the data and systems used to test applications prior to deployment to ensure that any veteran data required for applications testing or data analysis is properly protected or scrambled to prevent disclosure.

We have compiled a list of all VBA databases that contain sensitive information and all interfaces or data feeds that update these databases. We have compiled reports from each program and staff office regarding what VBA data is released to other VA and external entities. We have compiled all documented policies and procedures that govern the release of this information. A VBA work group has been tasked with assessing all current VBA policies and procedures related to the release of data protected by the Privacy Act. The work group will then provide recommendations to improve protection of the data to include periodic recertification of the business need for the release.

Effective June 7, in accordance with the Secretary's direction, VBA suspended all work-at-home and flexiplace arrangements for employees directly involved in disability claims processing. Field station managers were ordered to immediately recall these work-at-home and flexiplace employees to VA offices and to ensure they returned all claims folders and computer equipment when they came back into the office. Those employees who adjudicated claims at their homes or other non-VA work sites will now do all claims work requiring claims files in regional offices. This suspension of work-at home and flexiplace arrangements involving claims adjudication will continue while VBA evaluates various solutions to protect sensitive data transported to and from offices, particularly by work-at-home and other flexiplace employees. We are reviewing existing policy, directives, and letters regarding work-at-home and flexiplace. We are also developing a standard work-at-home and flexiplace agreement to ensure all employees absolutely understand their responsibilities to safeguard sensitive data.

VBA has procured encryption capability for laptop computers. We are also considering expanding the use of "terminal servers" as a means of reducing or eliminating the amount of information stored locally on a remote user's workstation. Under the "terminal server" configuration, remote users are restricted to only displaying and updating documents on their computer screens. All of the users' data and documents are created and maintained on a terminal server at a VA facility. In conjunction with VA's Office of Cyber and Information Security, we are also participating in the evaluation of a centrally managed encryption solution for computers and removable devices.

VBA Information Security Officers are required to review all users' access and privileges at least quarterly, or when a job change occurs that may require a different level of access with local business managers. Accounts on all systems are disabled after 90 days of inactivity and deleted after 180 days of inactivity. As a result of the data breach, the Secretary tasked all administrations to inventory current users of their information systems and provide a single database that contains these records. VBA is executing the Secretary's direction to centrally identify all individuals who have access to sensitive information.

We are also working with the Office of Acquisition and Materiel Management to reinforce strong control of the shipping of records containing personally identifiable information. This includes review of tracking procedures, signature requirements and expedited shipments.

DoD DATA FEEDS

The VA/DoD Joint Executive Council (JEC) was established as a result of the President's Management Agenda. This council is charged with enhancing coordination and resource sharing between VA and DoD and satisfying the reporting requirements of Public Law 97-174 and Public Law 108-136. VA and DoD together have made substantial progress toward data sharing strategies

essential to demographic data exchange and data synchronization. Additionally, we continue to make progress toward simplifying registration and enrollment of veterans, as well as the way we manage contact with veterans throughout their lifetime.

DoD data is delivered to VBA via secure transmission, using commercial software products and a direct computer-to-computer connection. The software is called Connect:Direct Secure+, and is a file transfer utility that has enhanced security options such as mutual authentication, data encryption, and cryptographic message integrity checking. We use this software when sending and receiving files from the Defense Manpower Data Center (DMDC).

VA is fully committed to the uninterrupted delivery of benefits to those who are returning or have returned from the battlefield and are transitioning into our VA system. We recognize the importance of securing the information shared with our DoD partners.

Our mission is to serve veterans and to provide benefits to the best of our ability. IT is an essential tool that helps us serve veterans better, faster, and more thoroughly. However, the rapid rate of technological advances, while offering improved and expanded benefits delivery, also presents an ongoing challenge to VA to keep pace with security and privacy demands. IT can make our service better and faster, but the vulnerabilities increase just as fast. We must and will do what is necessary to protect, as well as to serve, our veterans.