STATEMENT OF

WILLIAM F. TUERK

UNDER SECRETARY FOR MEMORIAL AFFAIRS

DEPARTMENT OF VETERANS AFFAIRS

BEFORE THE

HOUSE COMMITTEE ON VETERANS' AFFAIRS

JUNE 29, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for the opportunity to provide an overview of the actions that the National Cemetery Administration (NCA) has taken, is taking, and will take to ensure that sensitive personal information of veterans and their beneficiaries is safeguarded.

NCA IT INFRASTRUCTURE

As background, security has always been a very important part of NCA's Information Technology (IT) architecture. We have incorporated best practices from both the public and private sectors into our system, network, and application designs, and our ongoing policies and procedures. With guidance from the Department's Office of Cyber Information and Security (OCIS), NCA has pursued a strategy of continuous improvement for the security of its information systems. We have standardized policies and procedures governing information access requests, auditing, and rules of behavior. These policies and procedures apply

to all NCA employees, and to non-NCA employees who are granted access to NCA systems and data.

NCA has a centralized architecture for its information systems. All data is housed at the NCA's Regional Data Center in Quantico, Virginia and at NCA's IT "backup" site in Culpepper, Virginia. Access to the system is provided through one of two portals: via NCA's "in-house" data network; or via VA's Virtual Private Network (VPN). NCA staff, including field staff at NCA's 123 national cemeteries, access the "in-house" NCA data network directly in the course of their day-to-day activities. VPN access is used primarily by non-VA entities, *e.g.*, State Veterans Cemeteries or Department of Defense or Interior national cemeteries, to whom we have made NCA management systems available to facilitate their cemetery operations. Both access methods require a user ID and password to authenticate to the network and a separate user ID and password to access specific information systems.

As you are aware, VA IT security policy and oversight responsibilities have been centralized under VA's Chief Information Officer; the VA Office of Cyber and Information Security now has Department-wide responsibility for all IT security. Subject to the supervision of VA's OCIS, NCA implements its IT security policy and procedures for field activities by means of a three-layer organizational assignment of responsibilities. Cemetery Directors are responsible for the execution and oversight of IT security policy and procedures. Memorial Service Network (MSN) Offices provide oversight of cemetery

compliance with IT security policies and procedures. The NCA Data Center provides the technological support that implements IT security. All NCA Data Center employees and NCA Headquarters IT staff were detailed to the VA Office of Information and Technology on May 1, 2006, as part of the implementation of the VA IT Federated Model. They will be permanently assigned to that office on October 1, 2006.

Staff at NCA's Data Center centrally control the standard configuration of servers and NCA desktop and laptop computers. They deploy updates automatically -- including security patches and virus protection updates -- to maintain quality assurance and security. Before a server or workstation is connected to the NCA network, the device is loaded with a standard operating system and security software package, and the registry is locked to prevent any unauthorized modifications.

NCA provides data to numerous VA elements. For example, it provides "first notice of death" information to VBA. With respect to such intra-VA requests for data from NCA information systems, NCA has in place a formal process for accepting and reviewing requests for data extracts from NCA information systems. The information request must be cleared by the Deputy Chief Information Officer and presented to the Director of NCA's Data Center where it is documented and approved in NCA's helpdesk tracking system. In very limited and unusual circumstances, NCA also provides information to elements outside

of the VA, usually in response to Freedom of Information Act requests for non-sensitive information.

NCA also has a secure technology solution in place for individuals, *e.g.*, State Cemetery employees, requiring access to NCA systems from outside of VA. That solution requires external users to access NCA systems through the One-VA Virtual Private Network (VPN). The VPN allows remote users to access VA systems in a secure environment. NCA systems limit access from the VPN to NCA applications only. That is, "outside" users allowed access to the VPN by NCA cannot "roam" within VA's VPN.

All users authorized to access VA systems are required to sign approved rules of behavior. These rules of behavior bar the misuse of government systems, the mishandling of sensitive data, and unauthorized disclosure of sensitive information. They also specify, in the case of Federal employee access, that disciplinary action up to and including termination of employment can result from rules of behavior violations.

NCA completed the Federally-mandated certification and accreditation (C&A) of its IT system applications in October 2004. A second independent C&A of our systems will be conducted in FY 2007.

TECHNICAL AND POLICY CHANGES MADE, AND ANTICIPATED, SINCE DATA LOSS INCIDENT

I want to assure you and our Nation's veterans that the recent data breach did not include any NCA records, nor were burial and memorial services for our veterans and their families disrupted. To ensure that our systems will not be compromised, we have undertaken a number of actions based on a thorough review of our current information security processes. This review, which was equivalent to a DOD safety review stand down, dictated the following courses of action:

Actions Completed

- I have disseminated a memorandum to all NCA employees reiterating NCA's privacy and security policies and practices.

- NCA took measures to assure that all employees complete annual refresher training on both Privacy and Cyber Security Compliance by the end of this week.

- We have completed an NCA-wide accounting of employees accessing sensitive information via automated systems.

- NCA has reviewed the formerly-existing roster of persons having VPN remote access. Based on this review, a number of accounts have been deactivated or deleted.

- I established a new requirement that Privacy Coordinators be appointed at every NCA facility that is physically separate from NCA Headquarters to assure that all employees, volunteers, and contractors are aware of their respective roles in safeguarding privacy information.

- We have reviewed and reissued NCA's comprehensive Automated Information Systems Security Directive and Handbook to ensure that NCA information security policies and guidance are current.

Actions Under Way

- NCA is strengthening its Organizational Assessment and Improvement self-assessment guide to ensure more thorough and probing Security and Privacy Reviews are conducted at each cemetery.

- NCA is reviewing the need for the storage of paper records at its cemeteries. I anticipate that we will refine policies and enforcement mechanisms for sensitive document storage.

- NCA is currently reviewing its practices with respect to non-NCA access to NCA systems via the VPN network to ensure that only persons with a "need to know" gain access and to ensure that such persons comply with VA rules of behavior.

- All NCA facilities are currently participating in the Department's IT Privacy and Security Awareness Week.

- NCA is developing a Policy Directive stating requirements for collecting and retaining sensitive data, to include prohibitions on sharing data with third parties.

Future Actions

- NCA will develop a Policy Directive to define sensitivity level designations for all NCA positions.

- NCA will order appropriate background investigations for employees having access to sensitive information.

- Consistent with Department policy, NCA will develop a specific Telework Policy and require NCA workers to agree to VA Telework Rules of Behavior.

- NCA has inventoried, and will recall, all NCA-owned laptops to install the latest software updates including new VPN software, virus patches, and encryption software once it receives direction to do so.

- NCA will re-evaluate the need for external customers' access to our systems and strengthen controls for those customers who require access.

- NCA will develop a Policy Directive to require that new cemeteries implement individual Facility Security Handbooks prior to opening.

CONCLUSION

Our objective is to conduct day-to-day operations and accomplish our mission using security controls that are commensurate with risk, and to maintain a culture where our employees consistently and thoroughly safeguard VA data. NCA officials must assure that management, operational and technical safeguards are in place and are implemented to protect the confidentiality, integrity and availability of systems and data. They will do so. They must also assure that the systems and data are properly controlled and protected to prevent the real harms that can result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. They will do so. As Under Secretary for Memorial Affairs, I will see to that. I accept ultimate responsibility for assuring that these responsibilities are met throughout the National Cemetery Administration.

NCA people have always purposely pursued strategies necessary to safeguard information that is entrusted to them. They are dedicated to the mission of ensuring that the burial needs of veterans and eligible family members are met. Through continued review and diligence, they will ensure and I will ensure that the privacy of our veterans and their loved ones is preserved.

We welcome any guidance and assistance to improve NCA's security posture. We will continue to pursue best practices and we will work with you and

our VA colleagues to ensure that sensitive information entrusted to NCA custody is secure and safeguarded.

Thank you for the opportunity to appear before you today. I would be pleased to respond to any questions that you may have.