

## SUPPLEMENTAL INFORMATION ON VA's INFORMATION TECHNOLOGY

This enclosure presents your questions and our responses, to supplement information provided in our testimony before the Subcommittee on April 4, 2001.

### Post-Hearing Questions from Mr. Buyer:

1. Was computer security vulnerability an issue in regard to the recent indictment of a VBA employee at the Houston Resident Office?

The indicted employee was able to take advantage of a Regional Office (RO) violation of information security procedures. The RO believes that she established the false veteran during a brief six-week trial/experiment period, from August - September 1997. During this time, Veteran Service Officers were permitted to have two passwords to speed up the processing of veterans claims. Specifically, this was the "entry of data" password and the "authorization" password. This allowed the employee to establish, adjudicate, and authorize benefit payments. Once this account was established, adjustments could be made without oversight from a supervisor.

The other genuine account the employee accessed in late 1999 and 2000 was simply an entry that "recouped" funds for final payment to an authorized payee after a veteran is deceased. These funds would go to heirs or "other designated payee." Apparently there is no way to find this illegal action in the system, especially if the paid amounts are less than \$10,000.

2. Your information security survey identified significant security weaknesses. In your opinion, which of these should the Secretary address immediately, and, in the next six months?

The following issues should be addressed immediately:

- Appointment and confirmation of a Chief Information Officer for VA.
- Empowerment of the VA Cyber Security Officer to enforce standards already issued by the Assistant Secretary for Information and Technology.
- Centralize the management of the VACO network.
- Staffing effective Information Security Officer (ISO) positions to provide adequate oversight and implementation of necessary security control measures at the local facility level.
- Evaluation and correction of the potential vulnerabilities identified in our probes of VACO networks, data center networks, and selected field stations.
- Correction of the physical security weaknesses identified at the VACO data center and the Austin Automation Center.

The following issues should be addressed within the next six months:

- Implementing department-wide intrusion detection to reduce VA's vulnerability to inappropriate and undetected access to its systems and data.
- Deploying department-wide antivirus regime to better prevent/contain virus outbreaks that continue to occur in VA and cause disruption of services, adversely affect staff productivity, and divert technical staff efforts.
- Upgrading to VA-standard external electronic connections to reduce the vulnerability of VA's systems to penetration because of weaknesses in its external connections.
- Upgrading of all VA Desktop computers used in VA's automated systems to meet minimum acceptable security standards.

3. What computer security weaknesses have your Combined Assessment Programs Reviews identified in the VA?

The following is a list of the issues the CAP reviews have identified:

- A full-time ISO position had not been established.
- Strong password controls had not been implemented to reduce the risk of unauthorized access to VA systems.
- User access levels needed to be promptly updated to reflect current access requirements.
- Physical security of computer room and equipment needed to be strengthened.
- Annual AIS security awareness training had not been provided.
- Facility information system risk assessment and contingency plans needed to be developed to help ensure continuity of operations.

Some of these are repeated in our National Audit. However, I believe that the identification of these weaknesses at repeated sites is indicative of the systemic nature of the problems.

#### Post-Hearing Questions from Dr. Snyder

1. Is the VBA too overwhelmed by reform and redesign efforts that it cannot manage to resolve the system penetration threat at this time? Can VBA address the security issue in a series of steps that will not undermine the rest of its agenda? Could you propose steps to do so?

VBA has been reforming and redesigning its benefits delivery system for more than 10 years. The current task, VETSNET, is only the most recent of a series of projects. I do not believe that VBA is 'overwhelmed' with the task. The application of security should be a part of the process not another task. The

'retrofitting' of security to existing applications is one of the main reasons that VBA is in the state it is in regarding security.

Steps that should be taken to address the security vulnerabilities include:

- Each VBA facility should have an Information Security Officer (ISO). Information security should be the primary, if not exclusive, assignment for this person. Implementation of information security should be a critical factor in evaluations for the ISO.
- Each VBA facility director Performance Standards should include Information Security.
- Empowerment of an Information Security Officer at the Central Office level to enforce standards already issued by VA security offices and VBA security offices.
- Upgrading of all equipment to support a more stringent standard of security than is currently possible with Windows 95/98 machines currently in use.