

# **VA'S INFORMATION TECHNOLOGY SECURITY PROGRAM**

## **TESTIMONY OF THE HONORABLE RICHARD J. GRIFFIN INSPECTOR GENERAL OFFICE OF INSPECTOR GENERAL DEPARTMENT OF VETERANS AFFAIRS**

### **HOUSE COMMITTEE ON VETERANS' AFFAIRS SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS**

September 26, 2002

Mr. Chairman and Members of the Subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs' (VA) Information Technology (IT) security program. Our work continues to identify serious Department-wide vulnerabilities in IT security. As a result, we concluded from our audit results that the Department must continue to designate information security as a material weakness area under the Federal Manager's Financial Integrity Act (FMFIA).

Since our March 13, 2002 testimony to this Subcommittee, we completed a second national audit of VA's IT security program. A draft report has been provided to the Department for review and comment. The audit found that the Department has a number of initiatives in process that will provide the opportunity to improve VA's information security posture.

Key Department actions include:

- Establishment of a VA-wide security plan; and the required policies, procedures, and guidelines mandated by the Government Information Security Reform Act (GISRA).
- Implementation of VA-wide anti-virus protection.
- Staffing information security officer positions.
- Prioritization of Department-wide security remediation efforts.
- Centralization of the Department's IT security program under the Office of the Chief Information Officer (CIO).

While progress has been made, much work remains to implement key IT security initiatives, establish a comprehensive integrated VA-wide security program, and fully comply with GISRA. Our audit work continues to identify significant security vulnerabilities that represent an unacceptable level of risk to VA operations and its mission of providing healthcare and delivering benefits to the Nation's veterans.

Significant information security vulnerabilities continue to place the Department at risk of:

- Denial of service attacks on mission critical systems.
- Disruption of mission critical systems.
- Unauthorized access to and improper disclosure of data subject to Privacy Act protection and sensitive financial data.
- Fraudulent payment of benefits.

### **Penetration Tests Showed That VA Systems Need To Be Better Protected**

Penetration testing completed during the past 2 years verified that VA's automated systems could be exploited to gain access to sensitive veteran healthcare and benefit information. In response to last year's testing, the Department strengthened security controls at the facilities where we conducted our testing. During this year's follow up testing at these sites, the security control measures established prevented our external penetration attempts (access to systems from outside of VA's network.). VA must implement external automated system protection measures Department-wide to adequately protect its systems and sensitive data.

Continuing automated system control vulnerabilities allowed our internal penetration testing (access to systems from inside of VA's network) to gain access to sensitive veterans' benefit and healthcare information.

The vulnerabilities exploited during this year's testing were present during our previous testing a year ago. The Department has not taken appropriate corrective action to eliminate these vulnerabilities in response to our initial findings. The nature and number of vulnerabilities found warrant immediate attention to reduce the significant exposure and high risk of an internal attack.

Industry experience shows that the risk of inappropriate access by employees/contractors is highest inside of the network. We have again provided the Department with the details of this year's penetration testing results and recommendations on how the vulnerabilities could be corrected.

### **VA's CIO Needed Expanded Authority Over Security Remediation Efforts**

This year's security audit has shown that VA needs to take additional actions to correct information security vulnerabilities. VA's overall weak cyber security posture continues to be unacceptable and is reported as a Department material weakness. In our view, VA's overall security posture is one of the results of a lack of a unified or "One-VA" approach to information security that has lead to an ineffective approach to the implementation of necessary security improvements across the Department.

The Department's Administrations and staff offices have individually managed and controlled their information security program activities. Our security assessment results show that this decentralized management approach has not worked, with a continuing unacceptable security posture for the Department as a whole. Many security vulnerabilities identified in last year's audit remain unresolved, and additional security vulnerabilities were identified. With the exception of certain information technology acquisitions, the Department CIO did not have the authority to assure that the Department's security remediation efforts are completed. The decentralized management approach to information security management impeded the Department's ability to successfully strengthen its overall security posture.

We met with the Department CIO on July 22, 2002 and advised that we would be recommending that the Department centralize authority for the implementation of security remediation efforts to his office. This centralization of authority would include management and decision authority on all Department security remediation efforts. We had previously recommended centralized oversight in our prior year audit. On August 6, 2002 the Secretary of Veterans Affairs issued a memorandum centralizing the Department's IT security program, including authority, personnel, and funding in the Office of the Department CIO, effective October 1, 2002.

We believe that the Secretary's action will provide the opportunity to implement a "One-VA" approach to information security with implementation of necessary security improvements across the Department.

### **Department CIO Needs To Take Corrective Action In Several Key Areas**

Based on the results of our second annual audit of VA's IT security program, we recommended that the Department CIO take the following actions:

- Complete priority security remediation efforts in the next 12 months for the following areas: (1) install intrusion detection systems nationwide; (2) complete infrastructure protection actions; (3) complete data center contingency planning; (4) complete certification and accreditation of VA systems; (5) upgrade/terminate external connections; (6) improve configuration management of VA systems; (7) move the location of the VA Central Office (VACO) data center; (8) eliminate vulnerabilities in the application program/operating system change controls; and, (9) control physical access to computer rooms. Budgetary resources necessary to accomplish the priority security remediation efforts should be requested.
- Require the Administrations to: (1) correct identified security vulnerabilities at their facilities and data centers; (2) improve security awareness at the operating levels; and, (3) highlight the need to assure compliance with existing VA information security policy, procedures, and controls.

- Require the Administrations to certify completion of the remediation of information security vulnerabilities identified by the audit and provide annual facility certification of compliance with VA security policy, procedures, and controls.
- Establish skill levels and training requirements for Department information security staff to assure that they are capable of effectively performing their assigned duties.
- Implement VA-wide policy for effective monitoring of network operations to include use of electronic scanning and penetration testing techniques.
- Establish a national clearinghouse in the Office of Cyber Security for identifying and distributing information on security patch upgrades/fixes that need to be implemented.
- Assure that the GISRA reporting database accurately reflects the status of completed Department security remediation actions.
- Address the areas of non-compliance with GISRA, Office of Management and Budget (OMB) Circular A-130, Appendix III, and Presidential Executive Order 13231 on critical infrastructure protection requirements.

## **Conclusion**

VA needs to take additional actions to establish necessary security controls to proactively identify and prevent information security related risks and implement corrective action. As reported in our Fiscal Year (FY) 2001 information security audit and based on the work completed during the FY 2002 audit, VA still has not effectively implemented all planned security measures and has not assured compliance with established security policies, procedures, and controls requirements.

This concludes my testimony. I would be pleased to answer any questions that you and the members of the subcommittee may have.