



United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285557

June 30, 2000

Mr. Robert P. Bubniak
Acting Principal Deputy Assistant Secretary
for Information and Technology
Department of Veterans Affairs

Subject: Information Security: Software Change Controls at the Department of Veterans Affairs

Dear Mr. Bubniak:

This letter summarizes the results of our recent review of software change controls at the Department of Veterans Affairs (VA). Controls over access to and modification of software are essential in providing reasonable assurance that system-based security controls are not compromised. Without proper software change controls, there are risks that security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. If related personnel policies for background checks and system access controls are not adequate, there is a risk that untrustworthy and untrained individuals may have unrestricted access to software code, terminated employees may have the opportunity to compromise systems, and unauthorized actions may not be detected.

VA was 1 of 16 agencies included in a broader review of federal software change controls that we conducted in response to a request by Representative Stephen Horn, Chairman, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform. The objectives of this broader review were to determine (1) whether key controls as described in agency policies and procedures regarding software change authorization, testing, and approval complied with federal guidance and (2) the extent to which agencies contracted for Year 2000 remediation of mission-critical systems and involved foreign nationals in these efforts. The aggregate results of our work were reported *Information Security: Controls Over Software Changes at Federal Agencies* (GAO/AIMD-00-151R, May 4, 2000), which we are sending with this letter.

For the VA segment of our review, we interviewed officials in VA's Office of Information and Technology and Year 2000 project staff at two of the four VA components responsible for remediation of mission-critical systems for the Year 2000. These VA components, the Veterans Benefits Administration (VBA) and the Veterans Health Administration (VHA),

remediated 305 of VA's 316 mission-critical systems. We also obtained pertinent written policies and procedures from these components and compared them to federal guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). We did not observe the components' practices or test their compliance with their policies and procedures. We performed our work from January through March 2000 in accordance with generally accepted government auditing standards.

Overall, we identified weaknesses in three areas: formally documented policies and procedures, contract oversight, and background screening practices.

- The component-level policies and procedures used by VA components were adequate except that VBA did not address controlling installation of operating system software. However, departmental guidance for software change control was limited to restricting access to operating system software and investigating unusual change activity. The department-level policies did not address the following key controls.
 - Documenting, approving, and testing software changes.
 - Controlling application software libraries.
 - Monitoring changes, access to, and use of operating system software.
- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of some concern because VA used contract services for 40 (13 percent) of VA's 305 mission-critical systems included in our review. For example, VBA sent code for two mission-critical systems to a contractor's facility, but agency officials did not tell us how the code was protected after transit to the contractor facility, when the code was out of the agency's direct control. In your comments on a draft of this letter, you stated that the code was fully protected. However, you did not describe the protective controls in place to prevent unauthorized disclosure of code or unauthorized access to code. Therefore, we cannot evaluate the adequacy of these controls. According to your comments, VA did not use the renovated code for these two mission-critical systems because the contractors had not completed the task. Nevertheless, as a general practice, controls over code are important during the transmission of code to a contractor facility and while at the contractor facility to prevent disclosure of code for intelligence gathering by malicious individuals.
- VA officials told us that the nine contracts for Year 2000 remediation services did not include provisions for background screening of personnel. This is of potential concern because one contract for remediation of source code for a VHA project management system involved a foreign national. Also, OMB and NIST criteria require background screening of key staff involved with automated systems.

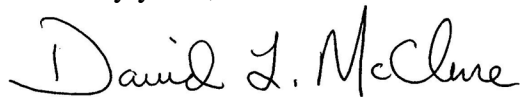
We requested comments on a draft of this letter from your office. You provided us with written comments that are included in the enclosure. In your comments, you mentioned VA's planned implementation of a formal certification and accreditation process that you said would assure the effectiveness of security measures. As part of this improvement effort, we suggest that you review VA's software change control policies and procedures and consider adopting industry best practices, such as the Carnegie Mellon University Software

Engineering Institute's Capability Maturity Model for Software. In addition, in light of the weaknesses we found, we also suggest that you review related contractor oversight and personnel policies and procedures and make any changes you deem necessary.

We have identified software control weaknesses at other agencies covered by our review; therefore, we have recommended that OMB clarify its guidance to agencies regarding software change controls as part of broader revisions that OMB is currently making to Circular A-130, *Management of Federal Information Resources*.

We appreciate VA's participation in this study and the cooperation we received from officials at your office and at the VA components covered by our review. If you have any questions, please contact me at (202) 512-6240 or by e-mail at mcclured.aimd@gao.gov, or you may contact Jean Boltz, Assistant Director, at (202) 512-5247 or by e-mail at boltzj.aimd@gao.gov.

Sincerely yours,

A handwritten signature in black ink that reads "David L. McClure". The signature is written in a cursive style with a large initial "D".

David L. McClure
Associate Director, Governmentwide
and Defense Information Systems

Enclosure

**Department of
Veterans Affairs**

Memorandum

Date: JUN 5 2000
From: Acting Principal Deputy Assistant Secretary for Information and Technology (005)
Subj: General Accounting Office (GAO) Correspondence, GAO File #3060D EDMS #93562
To: Deputy Assistant Secretary for Congressional Operations (60)

1. This office has reviewed GAO's draft correspondence, *Information Security: Software Change Controls at the Department of Veterans Affairs* (GAO/AIMD-00-201R), and offer the following comments:

Contractor Practices for Software Management

In reference to GAO's example that the Veterans Benefits Administration (VBA) sent code for two mission-critical systems to a contractor's facility, we find that the VBA code was fully protected. VBA did not use the renovated code because of the contractor's failure to complete the task. The contractor code was not re-installed on VBA systems.

VA Information Security

The most recent annual Consolidated Financial Statement (CFS) audit performed by VA's Office of Inspector General reaffirmed a recommendation made in two earlier CFS audits that is directly related to software change control, as defined by GAO report B-285184 (May 4, 2000). The recommendation was that VA enhance information security by "strengthening information systems controls that limit and monitor access to operating system and application software as well as data

VA is aware that an underlying cause of poor Federal information security is that agencies have not instituted a framework for proactively managing risk. Instead, there is a tendency to react to individual audit findings, with little ongoing attention to systemic causes of control weaknesses. Since VA's Chief Information Officer (CIO) strengthened central security management in early 1999, improvements have been and will continue to be pursued within a risk management framework. A variety of initiatives are underway in risk management and needs determination, policy development, controls implementation, awareness programs, and program evaluation. Efforts are pursued from a Department-wide perspective, concentrating on areas where consistency and balance across the Department are desirable.

The CIO's Information Security Program believes its principal contribution to improving the security of software change control across VA will be through its implementation of a formal system certification and accreditation (C&A) program. Certification and accreditation policies and procedures are a significant aspect of any Federal agency information security program. VA's C&A program will assure that effective security

Page 2.

Deputy Assistant Secretary for Congressional Operations (60)

measures are developed, implemented, and maintained throughout a system's life cycle, beginning with early planning phases. Certification will assure that the effectiveness of security measures (including those related to software change control) is formally assessed, and meaningful advice is presented to responsible officials regarding their decision to accredit for processing.

During FY 2000, the CIO's Information Security Program intends to launch a major contractor-assisted effort to promulgate its C&A program. The contractor will help VA determine the program's concept of operation. This will include recommending an appropriate C&A process model, outlining the resources needed to implement the model at three levels of effort, and providing a framework to categorize information to ensure VA invests in controls requisite to the value of the information asset.

The contractor will also provide guides for certifying and accrediting information systems. These guides will be largely specific to a particular technical setting. The initial investment will be for general support system (GSS) environments that support mission-critical programs. This priority scheme is consistent with GAO's position that application controls may be "rendered ineffective by circumvention or modification" of GSS controls. Additional guides for other categories of GSS environments and specific categories of application environments will be acquired later as the C&A program advances.

2. If you have any questions, please call me at 273-8842, or have a member of your staff contact Ms. Cynthia Krohmal, Director, IRM Planning and Acquisitions Service (045A1), at 273-8125.



Robert P. Bubniak

(511993)