DEPARTMENT OF VETERANS AFFAIRS

Memorandum

Date: May 6, 1999

From: Director, Financial Management Audit Division (52CF)

Subj: Management Letter - ADP Security at Hines Benefits Delivery Center (Report No. 9AF-G10-098)

To: Director, Benefits Delivery Center (20SD1)

1. Purpose and Scope

In accordance with the Chief Financial Officers Act, the Office of Inspector General (OIG) audits VA's Consolidated Financial Statements (CFS) annually. As part of our audit of Department of Veterans Affairs (VA) Fiscal Year (FY) 1998 CFS, we observed and tested selected Automated Data Processing (ADP) general controls at VA's Benefits Delivery Center (BDC) located at Hines, Illinois, during December 1998.

Our testing at Hines was limited to follow-up on issues in our FY 1997 CFS report[1] specifically concerning the Hines BDC. To evaluate corrective actions at the Hines BDC, we tested selected ADP general controls and selected security parameters of the IBM mainframe. We also interviewed BDC security staff regarding security controls and the status of corrective actions on the previously reported security control weaknesses.

2. Results

Management at the Hines BDC had initiated steps to improve their information security program. Management contracted with an independent firm to conduct a risk assessment, began updating policies and procedures, and was in the initial stages of implementing intrusion detection software. However, management had not taken sufficient action to reduce risk in the following four areas that we evaluated.

[1] Report of Audit of the Department of Veterans Affairs Consolidated Financial Statements for Fiscal Years 1997 and 1996, Report Number 8AF-G10-103, issued May 18, 1998.

a. Computer Duties Were Not Properly Segregated

General ADP security practices prescribe that the same individuals should not have both computer security and operations duties to reduce the risk that errors or fraud will occur and go undetected. Our review found proper segregation of duties did not exist at the Hines BDC. The operations staff continued performing security functions with access to the security and security backup files during FY 1998. For example, one report showed the operations staff was not only assigned the use of the IBM master security account, but was using this account more frequently than the security staff used their security accounts. The master account assigned to operations staff had been used 4,768 times to administer security. In contrast, the security accounts assigned to the Information Security Officers (ISOs) had been used no more than 56 times in the same time period. Risk was increased because ISOs were not reviewing the activities of the master security account.

b. Security Oversight Needed Improvement

General ADP security practices prescribe that staff overseeing security are technically knowledgeable, that computer configurations are documented and approved, and that reviews are conducted to verify the need for and use of powerful operating system privileges. The risks created by the absence of segregation of duties were increased because oversight did not incorporate these practices. For example,

- The ISOs lacked the technical knowledge to provide effective oversight to the operations staff.

- An approved system design was not yet documented.

- Reviews of security profiles and sensitive user privileges were not conducted during FY 1998. In one case, the Top Secret report *Cross-Reference of Privileges and Attributes* was not being used.

c. Access Controls Needed Improvement

Generally accepted access controls require changing passwords periodically, preventing the use of common words, and limiting the number of invalid password attempts. In addition, general practices require periodic reviews of user accounts to remove unneeded accounts or change access permissions. Our review found current access controls did not meet these standards. For example,

- The password parameter on the IBM mainframe had not been changed to prevent the use of English passwords by the user. In addition, reviews were not being conducted to assess the content of passwords.

- Entering an unlimited number of incorrect passwords continued to be allowed without suspending the master security account. This practice of allowing unlimited password attempts to this account increases the risk of unauthorized access to powerful privileges.

- Inactive user accounts had not been fully reviewed. The ISOs had started reviewing inactive user accounts during FY 1998, but this review was terminated due to resistance received from Regional Office managers.

d. Monitoring of security activities was not adequate

The risks associated with the access controls were increased because adequate monitoring was not conducted. General practice is to routinely monitor the access activities of users, especially those possessing powerful operating system privileges and access. This monitoring of access activities can help identify significant problems and deter users from inappropriate and unauthorized activities. Without properly monitoring the system and user access activity, the Hines BDC has little assurance that unauthorized attempts to access sensitive information would be detected. Our review found the following:

- Monitoring user activities on the mainframe and the network had not been implemented during FY 1998.

- The Hines BDC lacked substantive logging procedures for monitoring the use of privileged attributes and user utilities. Our review found no logging had been implemented during FY 1998.

During our discussions with management, they informed us that significant changes in the security program were not likely to take place until after their Year 2000 (Y2K) effort is complete. Further, management stated that the Hines ISO cannot adequately satisfy security oversight for all of the various hardware and software platforms without additional experienced and technically trained employees or contractor support.

3. Conclusion

These control weaknesses should be addressed by the Hines BDC as soon as practical. We encourage management to implement appropriate security changes during their Y2K effort. Steps need to be taken to ensure that actions already initiated to improve the BDC information security program are completed. Additionally, actions need to be taken to ensure computer duties are properly segregated, and that security oversight, access controls, and monitoring are improved. These controls will help reduce internal vulnerabilities.

Until a strong security program is implemented, sensitive veteran information will remain at risk of undetected disclosure, destruction, and alteration. A strong security program includes periodically assessing risks, implementing effective controls for restricting access based on job requirements, proactively reviewing access activities, monitoring and evaluating the effectiveness of controls and policies to ensure that they remain effective, and, perhaps most important, properly segregating security and operations duties.

4. Management Comments

When we brought these issues to the attention of Hines BDC management, they acknowledged the need for improvement in several areas. They had begun taking actions and investigating alternatives to address and correct the control weaknesses and reduce the risks on the IBM as well as other significant technologies that they manage. These actions included transferring more of the security administration functions away from operations staff to the ISOs, changing the master security account password often, and having warning messages generated every time an incorrect password is used for the master security account. While these controls do reduce risk, they do not reduce risk to an adequate level. Until experienced and technically knowledgeable ISOs are used, sufficient segregation of duties cannot be achieved and access control vulnerabilities are likely to remain or recur.

5. Reporting

Audit results from Hines BDC will be incorporated into our report to VA's Chief Financial Officer. This report, which will be available publicly, is typically of a general nature. However, we may site specific concerns identified during our audits of VA facilities. In these instances, we are careful not to associate particular weaknesses with specific facilities.

If you have any questions, please contact Jeff Shearer at (202) 565-7894.

(Original signed by)

JOHN E. JONSON

cc: Acting Assistant Secretary for Information Technology (005)
Veterans Benefits Administration, Chief Information Officer (20S)