John W. Lainhart IV
Inspector General

Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990

MEMORANDUM

TO: James M. Eagen III
Chief Administrative Officer

FROM: John W. Lainhart IV
Inspector General

DATE: May 26, 1998

SUBJECT: Management Advisory Report – ACF2 Controls Implemented And Planned Increase House Mainframe Security (Report No. 98-CAO-06)

This is our final management advisory report on the ACF2 software security system. The objective of our review was to determine whether ACF2 and the operating system have been adequately installed and protected. We found that House Information Resources (HIR) has made substantial progress to reasonably ensure the security and integrity of ACF2 and the operating system. However, further actions are still required by HIR. Specifically, HIR needs to develop formal ACF2 standards and procedures, transfer ownership of ACF2 to the Security Office, and define the ACF2 administrator's roles, responsibilities and authority. In addition, HIR needs to reduce the number of special privilege attributes, rewrite key access rules, and review and update ACF2 installation option settings accordingly.

In response to our January 21, 1998 draft report, your office concurred with our findings and recommendations. Your formal written response, dated February 26, 1998, is incorporated in this final report and included in its entirety as an appendix. The corrective actions taken, in process, and planned by your office are appropriate and, when fully implemented, should adequately respond to the recommendations contained in this report and other long-standing recommendations contained in prior OIG reports. Furthermore, we consider the milestone dates provided for implementing the corrective actions reasonable.

We appreciate the courtesy and cooperation extended to us by your staff. If you have any questions or require additional information regarding this report, please call me or Robert B. Frey III at (202) 226-1250.

Attachment

cc: Speaker of the House
Majority Leader of the House
Minority Leader of the House
Chairman, Committee on House Oversight
Ranking Minority Member, Committee on House Oversight
Members, Committee on House Oversight

ACF2 Controls Implemented and Planned Increase House Mainframe Security

Report No. 98-CAO-06
May 26, 1998

RESULTS IN BRIEF

CONCLUSIONS

The Chief Administrative Officer (CAO) has significantly enhanced mainframe security by establishing an Access Control Facility 2 (ACF2) system administrator function within the House Information Resource's (HIR) Security Office and by developing a security policy. HIR has made substantial progress in limiting access to ACF2 and the operating system. Furthermore, the installation of ACF2 system-wide option settings were generally adequate and within accepted parameters to protect the mainframe resources.

However, HIR needs to complete the establishment of the ACF2 administrative function by developing formal ACF2 standards and procedures, transferring ownership of ACF2 to the Security Office, and defining the ACF2 administrator's roles, responsibilities and authority. In addition, the number of special privilege attributes remaining during our review were still too high, requiring further reduction; a rewrite of key access rules to limit access to system resources was needed; and four ACF2 installation option settings need to be reviewed and changed accordingly to strengthen mainframe security.

During the review, management took or agreed to take actions to correct the deficiencies noted. As a result of these actions, the Security Office will be able to reasonably ensure the security and integrity of ACF2 and the operating system. Reducing the number of users who have access through privileges and rules, reduces the risk of compromising ACF2 and the operating system. Furthermore, actions taken to adjust ACF2 system option settings also contributed to minimizing the risk of potential unauthorized activity with respect to the mainframe.

RECOMMENDATIONS

We recommended that the Chief Administrative Officer: (1) establish formal ACF2 security access standards and procedures in support of the security policy; (2) transfer ownership of ACF2 from the Enterprise Computing Group to the Security Office; (3) formally define the roles, responsibilities and authority of the ACF2 administrator; (4) provide ACF2 training to the Security Office personnel; (5) transfer the ACF2 backup function from the Enterprise Computing Group to the Security Office; (6) eliminate logon

IDs[1] from the Computer Center Systems Management (CCSM) Group as appropriate and/or subdivide them into smaller functional groups; (7) research the four questionable ACF2 system-wide option settings and make changes, as appropriate; and (8) establish a baseline for ACF2 system option settings, and periodically reconcile this baseline against new ACF2 releases and/or the current processing environment

MANAGEMENT RESPONSE

On February 26, 1998, the CAO formally concurred with the findings and recommendations in this report. In addition to the actions already taken during the review, the CAO agreed to (1) establish written standards and procedures implementing effective recurring controls; (2) transfer ACF2 ownership from the Enterprise Computing Group to the Security Office; (3) train Security staff personnel to backup the ACF2 administrator; (4) formally transfer the ACF2 backup function from the Enterprise Computing Group to the Security Office; (5) conduct a review of the Computer Center Systems Management Group ID's and eliminate or group logon ID's to reflect job responsibilities; (6) conduct a review of the remaining four questionable settings and make changes or provide justifications for current settings; and (7) review the ACF2 system installation settings against established parameters on an annual basis or after modifications and/or upgrades to the ACF2 system.

OFFICE OF INSPECTOR GENERAL COMMENTS

The CAO's current and planned actions are responsive to the issues we identified, and when fully implemented, should satisfy the intent of our recommendations.

[1] Logon ID identifies each user to ACF2 and corresponding privileges by specifying values that enable ACF2 to identify and validate each user request on an individual basis.