John W. Lainhart IV
Inspector General

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

MEMORANDUM

TO: Scot M. Faulkner
Chief Administrative Officer

FROM: John W. Lainhart IV
Inspector General

DATE: July 31, 1996

SUBJECT: Audit Report - Additional Vendor Guarantees Are Needed To Ensure Integrity Of HIR's Operating System (Report No. 96-CAO-06)

As part of our information systems audit of House Information Resources (HIR) operations, we have reviewed issues associated with computer system integrity. During this information systems audit, my staff identified a system integrity exposure which is described in detail in the restricted attachment.

The weakness identified in the attachment could expose information on House computer systems to unauthorized access, disclosure, modification, or destruction. For example, as part of our normal testing, we identified the existence of a system integrity exposure associated with the use of system software running under the IBM operating system in the HIR central computer facility. While using the software, provided by a commercial vendor, we were able to switch system authorization to supervisor state. By gaining access to change the system authorization, the potential exists to access and execute privileged operating system instructions that are otherwise restricted. Thus, the primary emphasis of the restricted attachment focuses on the issue pertaining to access to House computer systems.

We discussed our observations and recommendations for initial corrective action with HIR staff. Recommendations addressed the issues of:

- Vendor correction of the system integrity exposure;
- Integrity statements for all vendor system software products running on the HIR
- mainframe;
- Integrity statement policies and procedures over new and existing House system software.

We notified the HIR staff of the exposure and potential impact of a knowledgeable user accessing the House computer system. Furthermore, the initial corrective action steps identified

by my staff are being implemented by HIR's Security and Enterprise Computing staff along with additional supplemental actions in order to protect access to the HIR operating system. Specifically, HIR staff immediately contacted the vendor to ensure that needed corrective actions were taken to correct the exposure identified and also contacted Carnegie Mellon University's Computer Emergency Response Team to apprise them of the system integrity exposure.

If you should have any questions regarding the issues identified in this report, you can contact 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