



G A O

Accountability * Integrity * Reliability

**United States General Accounting Office
Washington, DC 20548**

**Accounting and Information
Management Division**

B-285551

June 30, 2000

Ms. Gloria R. Parker
Chief Information Officer
Department of Housing and Urban Development

Subject: Information Security: Software Change Controls at the Department of Housing and Urban Development

Dear Ms. Parker:

This letter summarizes the results of our recent review of software change controls at the Department of Housing and Urban Development (HUD). 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.

HUD 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 in *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 HUD segment of our review, we interviewed officials in HUD's Chief Information Office and Year 2000 project staff at HUD headquarters responsible for remediation of software for HUD's 57 mission-critical systems. We also obtained pertinent written policies

and procedures and compared them to federal guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology. We did not observe practices or test compliance with policies and procedures. We performed our work from January through March 2000 in accordance with generally accepted government auditing standards.

We determined that HUD had established formal departmentwide policies and procedures that adequately addressed major aspects of their centralized software change control function. In fact, the formally documented policy established a goal for the department to maintain a level 2, or repeatable,¹ process maturity based on the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. However, we identified concerns in two related areas: contract oversight and background checks of personnel involved in software change activities.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. For example, contract information on procurement method, inclusion of contract provisions for background checks of employees, and protection of code transmissions and code located at contractor facilities was not readily available. This is of potential concern because all 57 of HUD's mission-critical federal systems involved the use of contractors for Year 2000 remediation. In addition, HUD officials told us that all 10 contracts for remediation services employed foreign nationals. Further, HUD sent code associated with one mission-critical system to a contractor facility, but agency officials could not readily determine how the code was protected during and after transit to the contractor facility, when the code was out of the agency's direct control.
- Although HUD officials told us that all contracts for remediation services included provisions for background checks of contractor staff, background screenings were not a routine security control at HUD for noncontract personnel involved in making changes to software. This is of concern because OMB and NIST criteria require background screening of key staff involved with automated systems.

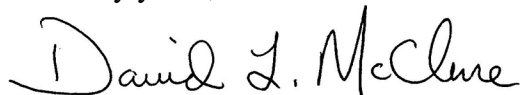
We requested comments on a draft of this letter from your office. You provided us with written comments that are included in the enclosure. In your comments, you stated that you have established a Personnel Security Working Group to address the policies for contract oversight and related personnel practices. You identified contractor practices for background checks of personnel as one of several steps to improve overall computer security that will be implemented by September 30, 2000. We encourage you to continue these efforts to improve HUD's policies and procedures for computer security.

¹ The Capability Maturity Model is organized into five levels that characterize an organization's software process maturity. These levels range from *initial* (level 1), characterized by ad hoc and chaotic processes, to *optimizing* (level 5), characterized by continuous process improvement based upon analysis and quantitative data. Level 2 is described as the *repeatable* level, in which basic project management processes are established to track cost, schedule, and functionality.

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

We appreciate HUD's participation in this study and the cooperation we received from officials at your office. 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



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000

OFFICE OF THE CHIEF INFORMATION OFFICER

JUN 7 2000

David L. McClure
Associate Director, Governmentwide
and Defense Information Systems
U. S. General Accounting Office
441 G Street, N. W. #4075
Washington, DC 20548

Dear Mr. McClure

Thank you for the opportunity to review and comment on your draft letter, "Information Security: Software Change Controls at the Department of Housing and Urban Development". The feedback you have provided will help the Department in strengthening its change control processes. While we do not have any recommendations for substantive changes in the draft, I would like to take this opportunity to highlight some of the Department's actions which address those areas of concern cited in your letter, that is, contract oversight and background checks of personnel involved in software change activities.

In response to identified problems and concerns about computer security, background checks and software change control issues the Department has established a Personnel Security Working Group consisting of staff from the following organizations:

- Chief Information Officer (CIO)
- Chief Financial Officer (CFO)
- Office of Administration (ADMIN)
- Office of Information Technology (OIT)
- Office of Human Resources (OHR)
- FHA Comptroller

The working group has already identified a number of steps that will improve the Department's computer security, including:

- Updating the Departmental Computer Security handbook, and other applicable procedures;
- Clarifying roles and responsibilities;
- Streamlining the process and improving the methodology used to track computer system access requests;
- Improving the information sharing and coordination between

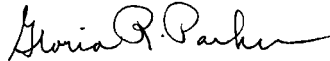
organizations on security issues;

- Reviewing the current inventory of systems to update the Department's "mission critical" list;
- Requiring contractors to document that their employees have relatively recent government security clearances or background checks by approved third parties; and,
- Improving the training and accountability for Government Technical Representatives, Security Administrators and managers.

These recommendations will be implemented by September 30, 2000. Moreover, I have recently hired a Critical Infrastructure Assurance Officer, John R. Haines, who will be responsible for ensuring that the Department has clear and effective policies and procedures governing computer security.

I can assure you that the Department takes its computer security responsibilities very seriously. We are committed to doing whatever is necessary to meet the requirements. Please contact me on 202.708.2050, if you need additional information.

Sincerely



Gloria R. Parker,
Chief Information Officer

(511986)