GAO
Accountability * Integrity * Reliability

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

**Accounting and Information**
**Management Division**

B-285550

June 30, 2000

The Honorable John J. Callahan
Chief Information Officer
Department of Health and Human Services

Subject: Information Security: Software Change Controls at the Department of Health and Human Services

Dear Mr. Callahan:

This letter summarizes the results of our recent review of software change controls at the Department of Health and Human Services (HHS). 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.

HHS 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 HHS segment of our review, we interviewed officials at HHS' Chief Information Office, and Year 2000 project staff at headquarters and at all 11 HHS components, listed in the enclosure, responsible for remediation of HHS' 284 mission-critical systems for the Year 2000. 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. 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. At the end of our fieldwork, HHS officials reviewed a draft of this letter and provided no comments.

At HHS, we identified weaknesses regarding formal policies and procedures, contract oversight, and background screening of personnel.

- Formally documented departmentwide change control policies and procedures did not exist at HHS. In addition, the following eight components had not implemented formally documented procedures for change control.
  - Centers for Disease Control and Prevention (CDC),
  - Food and Drug Administration (FDA),
  - Health Care Financing Administration (HCFA),
  - Health Resources and Services Administration (HRSA),
  - National Institutes of Health (NIH),
  - Office of Inspector General (OIG),
  - Program Support Center (PSC), and
  - Substance Abuse and Mental Health Services Administration (SAMHSA).

- Formally documented component-level policies and procedures at the Administration for Children and Families (ACF), Administration on Aging (AoA), and Indian Health Service (IHS), did not meet federal criteria. Specifically, these components did not address key software change controls as detailed below.
  - ACF's formally documented Change Management Procedure did not address application software libraries, and operating system software access and monitoring.
  - AoA had a formally documented change control procedure, but it was not in place during Year 2000 remediation – it was effective March 2000. This new procedure did not address operating system software access and monitoring.
  - IHS had a formally documented change control process. However, the process did not require documentation of software changes and it did not address access to application program libraries and operating system software, and operating system software monitoring and change control.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because 233 (82 percent) of HHS' 284 mission-critical federal systems covered by our study involved the use of contractors for Year 2000 remediation. For example, HCFA, IHS, OIG, and PSC sent code for 52 mission-critical systems to contractor facilities, including code for 15 systems transmitted by HCFA to a foreign-owned contractor facility. Agency officials could not readily determine how the code and data were protected during and after transit to the contractor facility, when the code was out of the agency's direct control.

- Based on our interviews, ACF, AoA, HCFA, NIH, and PSC did not include background screening provisions in contracts, and ACF, AoA, and NIH did not require routine

background screenings of federal or contract staff performing software change functions. This is of potential concern because three ACF contracts and four NIH contracts involved foreign nationals. For example, three ACF contracts had foreign nationals on staff from India, Pakistan, Singapore, Russia, Ukraine, Taiwan, China, and Guatemala, yet ACF did not include background screening provisions in their contracts. Although IHS required routine screening of all staff, the background screening of a British foreign national was not completed prior to the individual's work on Year 2000 remediation.

According to HHS officials, efforts are underway to develop a departmentwide software change management process based on the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. We suggest that you continue your initiative to review software change policies and procedures at HHS. In light of other weaknesses, we also suggest that you review related contractor oversight and personnel policies and practices and implement any changes that you deem necessary. 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 HHS' participation in this study and the cooperation we received from officials at your office and all HHS 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,

David L. McClure

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

Enclosure

Enclosure

## Department of Health and Human Services' Components Included in Study

1. Administration for Children and Families
2. Administration on Aging
3. Centers for Disease Control and Prevention
4. Food and Drug Administration
5. Health Care Financing Administration
6. Health Resources and Services Administration
7. Indian Health Service
8. National Institutes of Health
9. Office of Inspector General
10. Program Support Center
11. Substance Abuse and Mental Health Services Administration

(511985)