GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285558

June 30, 2000

Mr. Joseph Leo
Chief Information Officer
Department of Agriculture

Subject: Information Security: Software Change Controls at the Department of Agriculture

Dear Mr. Leo:

This letter summarizes the results of our recent review of software change controls at the Department of Agriculture. 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.

The Department of Agriculture 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 Agriculture segment of our review, we interviewed officials in the Office of the Chief Information Officer, who provided information pertaining to 6 of Agriculture's 22 components responsible for remediating 229 of Agriculture's 343 mission-critical systems. These 6 components were the Animal and Plant Health Inspection Service (APHIS), the Farm Service Agency (FSA), the Food and Nutrition Service, the Forest Service (FS), the Natural

Resources Conservation Service (NRCS), and Rural Development (RD). 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, Agriculture officials reviewed a draft of this letter, orally concurred with our findings, and provided no substantive comments.

At the Department of Agriculture, we identified weaknesses regarding formal policies and procedures, contract oversight, and background screening of personnel involved in software change control activities.

- Departmentwide guidance did not exist and formally documented component procedures were inadequate. Although several components had informal controls in place, most were not documented. We found that APHIS and FSA did not have formally documented processes for software change control. In addition, the procedures for the remaining four components covered by our review did not adequately address key controls, including operating system software changes, monitoring, and access; nor controls over application software libraries including access to code, movement of software programs, and inventories of software.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because 74 (32 percent) of Agriculture's 229 mission-critical federal systems covered by our study involved the use of contractors for Year 2000 remediation. For example, five components (all except for the NRCS) sent code associated with 69 mission-critical systems to contractor facilities for remediation, including code for 40 systems sent to non-U.S. contractor facilities in England, India, and Canada. 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.

- Based on our interviews, background screenings of personnel involved in the software change process were not a routine security control. Of 43 contracts issued for remediation services by the six components, 14 contracts (all issued by FS) did not include contract provisions for background checks of contractor staff. In addition, five components (all except RD) did not require routine background screening of foreign national personnel involved in making changes to software.

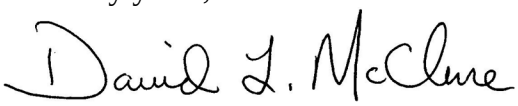
- Complete data on the involvement of foreign nationals in software change process activities were not readily available from agency officials interviewed. However, officials told us that all six components included in our study involved foreign nationals on 11 contracts for remediation services.

In light of these weaknesses, and to further improve controls over software changes, we suggest that you review Agriculture's software change control policies and procedures and

consider adopting industry best practices, such as the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. In addition, we suggest that you review related contract 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 Agriculture's participation in this study and the cooperation we received from officials at your office and at the Agriculture 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
Associate Director, Governmentwide
and Defense Information Systems

(511992)