GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285555

June 30, 2000

Mr. Fernando Burbano
Chief Information Officer
Department of State

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

Dear Mr. Burbano:

This letter summarizes the results of our recent review of software change controls at the Department of State. 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 State 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 State segment of our review, we interviewed a State official in the Chief Information Office and officials at three of the nine State components responsible for remediation of software for Year 2000—the bureaus of Information Resource Management, Consular Affairs, and Finance Management and Policy. These three components remediated 43 of

State's 59 mission-critical systems. 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, State officials reviewed a draft of this letter and concurred with our findings. Their oral comments have been incorporated where appropriate.

According to State officials, background checks of personnel involved in the software change process were a routine security control for federal, contractor, and foreign national personnel involved in making changes to software. Also, officials told us that all 19 contracts included provisions for background checks of contractor staff. This is important because 4 of these contracts for remediation services involved foreign nationals. In comments on a draft of this letter, State officials told us that in 1999, the Bureau of Diplomatic Security prepared a report entitled "Foreign Contractor Involvement with the Year 2000 Program." This report was a result of the Secretary of State's concern regarding the extent to which foreign nationals were involved in Year 2000 remediation activities.

However, we identified weaknesses regarding formal policies and procedures and contract oversight.

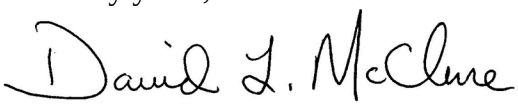
- All three State components told us that they followed State's departmentwide formally documented guidance for software change control, but we found that this guidance did not adequately address key software change controls. Specifically, the guidance did not address (1) operating system software access and monitoring and (2) application software library controls for labeling and inventorying software programs.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because all 43 of State's mission-critical systems involved the use of contractors for Year 2000 remediation. For example, all three State components sent code associated with 18 mission-critical systems to contractor facilities for remediation, and 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 State's direct control.

In light of these weaknesses and to further improve State's controls over software changes, we suggest that you review State'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 the Department of State's participation in this study and the cooperation we received from officials at your office and at the Department of State 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

(511990)