GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285549

June 30, 2000

Mr. George R. Molaski
Chief Information Officer
Department of Transportation

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

Dear Mr. Molaski:

This letter summarizes the results of our recent review of software change controls at the Department of Transportation (DOT). 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.

DOT 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 DOT segment of our review, we interviewed officials in DOT's Chief Information Office and Year 2000 project staff at DOT headquarters and at 12 of 14 major DOT components responsible for remediation of software for Year 2000. These 12 components,

listed in the enclosure, remediated 185 of DOT's 609 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 include the Federal Aviation Administration in our study because we recently completed similar work[1] at this component. Also, 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, DOT officials reviewed a draft of this letter, orally concurred with our findings, and provided no substantive comments.

At DOT we identified concerns in three control areas: formal policies and procedures, contract oversight, and awareness of contractor and foreign national personnel involvement in software change activities.

- Although DOT had established departmentwide guidance for software management, implementation was delegated to DOT components, which did not consistently apply or adopt the requirements. For example, 9 of 12 components (all except the Federal Highway Administration (FHWA), the Office of the Secretary of Transportation (OST), and the Transportation Administrative Service Center (TASC)) had no formal procedures for software change control. Only OST had formally adopted the department-level guidance in documented procedures. Also, we found that the department-level guidance followed by OST and related procedures for FHWA and TASC did not address key controls. Specific key controls not addressed were operating system software changes, monitoring, and access and controls over application software libraries including access to code, movement of software programs, and inventories of software.

- We found that agency officials were not familiar with contractor practices for software management. At the Bureau of Transportation Statistics (BTS), OST, and U.S. Coast Guard (USCG), data on contracts used for remediation were not readily available. This is of potential concern because 171 of DOT's mission-critical federal systems covered by our study involved the use of contractors for Year 2000 remediation. For example, BTS, the Federal Railroad Administration, the Maritime Administration, OST, and USCG sent code associated with 28 mission-critical systems to external contractor facilities. We could not readily determine how the code was protected during and after transmission to the contractor facilities, when it was out of the agency's direct control.

- We determined that background screenings 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. However, officials at BTS, FHWA, National Highway Traffic Safety Administration (NHTSA), and the Research and Special Programs Administration told us that their 13 contracts for remediation services of 64 mission-critical systems did not include provisions for background checks of contractor staff.

[1] *Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software, (*GAO/AIMD-00-55, December 23, 1999).

- Officials at FHWA, FRA, NHTSA, OST, TASC, and USCG told us that foreign nationals were employed on 12 of 41 contracts for remediation services. Complete data on the involvement of foreign nationals in software change process activities at DOT headquarters, FHWA, OST, STB, and the USCG were not readily available.

In light of these weaknesses and to further improve DOT controls over software changes, we suggest that you review DOT 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, throughout the department. In addition, we suggest that you review related personnel and contract oversight 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 DOT's participation in this study and the cooperation we received from officials at your office and at the DOT 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 Transportation Components Included in Study

1. Bureau of Transportation Statistics
2. Federal Highway Administration
3. Federal Railroad Administration
4. Maritime Administration
5. National Highway Traffic Safety Administration
6. Office of the Inspector General
7. Office of the Secretary of Transportation
8. Research and Special Programs Administration
9. Saint Lawrence Seaway Development Corporation
10. Surface Transportation Board
11. Transportation Administrative Service Center
12. U.S. Coast Guard

(511984)