GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285542

June 30, 2000

The Honorable Arthur L. Money
Chief Information Officer
Department of Defense

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

Dear Mr. Money:

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

DOD 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 DOD segment of our review, we interviewed officials in DOD's Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. We also interviewed Year 2000 project staff at DOD headquarters and at 9 of 23 major DOD components responsible for remediation of software for Year 2000. These nine components, which are listed below, remediated 1,618 of DOD's 2,101 mission-critical systems.

- Defense Finance and Accounting Service (DFAS)
- Defense Information Systems Agency (DISA)
- Defense Intelligence Agency (DIA)
- Defense Logistics Agency (DLA)
- Department of the Army
- Department of the Navy (Navy)
- United States Air Force (Air Force)
- United States Marine Corps (USMC)
- Washington Headquarters Services (WHS)

We also obtained pertinent written policies and procedures from DFAS, DISA, and DLA 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, DOD officials reviewed a draft of this letter and concurred with our findings. Their oral comments have been incorporated where appropriate.

We found 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. Further, officials told us that all 57 contracts for remediation services of 253 mission-critical systems included provisions for background checks of contractor staff. This is important because we found that foreign nationals were involved in two contracts with the Navy. One contract involved Year 2000 changes to the source code for seven Navy logistics systems. The other contract involved independent validation and verification of source code changes for Navy and USMC personnel systems.

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

- Departmentwide guidance did not exist and development and implementation of software change policies had been delegated to DOD components. We identified several deficiencies in these component-level procedures. Specifically, WHS had no formal procedures for software change controls. Procedures for the three components reviewed did not address operating system software changes, monitoring, and access or 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 headquarters and at six of the components (all except DIA, DLA, and WHS), complete data on contracts used in software change process activities were not readily available. This is of potential concern because 253 of DOD's mission-critical systems covered by our study involved the use of contractors for Year 2000 remediation. For example, six components (DFAS, DIA, DLA, Air Force, Navy, and USMC) sent code or data associated with 79 mission-critical systems to contractor facilities, including code

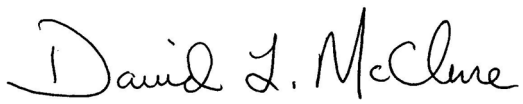
associated with 36 Navy systems and 5 modules of a USMC personnel system sent to a foreign-owned contractor facility. However, agency officials could not readily determine how the code and data were protected during and after transit to the contractor facility when the code was out of the agency's direct control.

In your comments on a draft of this letter, you stated that your office is addressing issues in software change policies as part of an overall improvement of software management practices within DOD. You stated that the Software Management Division established in March 2000 would analyze software best practices, including the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software, for development of a departmentwide software methodology. In addition, you stated that new security policies addressing the use of foreign nationals for work on software modification will be included in the next revision to a pertinent DOD regulation.

In conjunction with these efforts, we suggest that you review related 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 DOD's participation in this study and the cooperation we received from officials at your office and at the DOD 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

(511979)