GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285541

June 30, 2000

Mr. Roger W. Baker
Chief Information Officer
Department of Commerce

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

Dear Mr. Baker:

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

DOC 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 DOC segment of our review, we interviewed officials in DOC's Chief Information Office and Year 2000 project staff at headquarters and at 12 of 13 DOC components responsible for remediation of software for Year 2000. These 12 components, listed in the enclosure, remediated 470 of DOC's 473 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 (NIST). 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, DOC officials reviewed a draft of this letter and concurred with our findings. Their oral comments have been incorporated where appropriate.

At DOC, we identified concerns in three control areas: formal policies and procedures, contract oversight, and background screening of personnel.

- Departmentwide guidance and formally documented component procedures were inadequate, and not all components had formally documented controls. Although DOC had established department-level guidance for software management, implementation was delegated to DOC components, which did not consistently apply or adopt the requirements. Four of the 12 components covered by our review had adopted formal procedures for software change control (the Bureau of Economic Analysis [BEA], NIST, the National Oceanographic and Atmospheric Administration [NOAA], and the Patent and Trademark Office [PTO]). Only NOAA officials told us that they had formally adopted the department-level guidance. Also, we found that the department-level guidance, which was followed by NOAA, and related procedures for BEA, NIST, and PTO did not address key controls. Specific key controls not addressed by the department-level guidance and the component procedures were (1) operating system software changes, monitoring, and access, and (2) 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 89 (19 percent) of 470 DOC mission-critical federal systems covered by our study involved the use of contractors for Year 2000 remediation. At the Minority Business Development Agency (MBDA), DOC officials directed us to interview contractor staff. In addition, DOC officials at the following seven components could not readily provide information on software control requirements included in contracts or on related contractor practices.
  - Bureau of the Census (Census)
  - Economics and Statistics Administration (ESA)
  - MBDA
  - Office of the Secretary (OS)
  - NOAA
  - National Telecommunications and Information Administration (NTIA)
  - PTO

  Also of concern is that BEA, Census, NOAA, and PTO sent code or data associated with 30 mission-critical systems to contractor facilities. 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 and review of documented security policies and procedures, background screenings of personnel involved in the software change process were not a

routine security control. Of the 12 DOC components we reviewed, ESA and the National Technical Information Service did not require routine background screening of personnel involved in making changes to software or include security provisions in contracts.

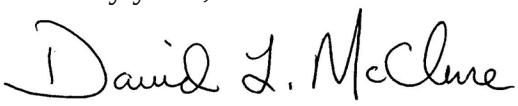
- According to agency officials, foreign nationals were involved in remediation activities on 10 contracts at Census, EDA, MBDA, NTIA, and PTO. At headquarters, Census, the Economic Development Administration, ESA, OS, and PTO, complete data on the involvement of foreign nationals in software change process activities were not readily available.

According to a DOC official, efforts are underway to update the departmentwide software change management process. As part of this effort, DOC officials plan to consider incorporating best practices provided by the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software.

We suggest that you continue your initiative to update DOC's software change policies and procedures. 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 DOC's participation in this study and the cooperation we received from officials at your office and at the DOC 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

Enclosure

Enclosure

U.S. Department of Commerce Components Included in Study

1. Bureau of Economic Analysis
2. Bureau of the Census
3. Economic Development Administration
4. Economics and Statistics Administration
5. International Trade Administration
6. Minority Business Development Agency
7. National Institute of Standards and Technology
8. National Oceanographic and Atmospheric Administration
9. National Telecommunications and Information Administration
10. National Technical Information Service
11. Office of the Secretary
12. Patent and Trademark Office

(511978)