



United States General Accounting Office  
Washington, DC 20548

Accounting and Information  
Management Division

B-285544

June 30, 2000

Mr. Daryl W. White  
Chief Information Officer  
Department of the Interior

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

Dear Mr. White:

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

DOI 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 DOI segment of our review, we interviewed officials from DOI's Office of Information Resources Management and Year 2000 program management officials at 12 DOI components responsible for remediation of mission-critical systems for the Year 2000. These 12 components, listed in the enclosure, remediated 87 of DOI's 90 mission-critical systems. We also obtained pertinent written policies and procedures from the Bureau of Land Management (BLM), Office of Surface Mining (OSM), Bureau of Indian Affairs (BIA), the

National Business Center in the District of Columbia (NBC-DC), and the Bureau of Reclamation (BOR) 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, DOI officials reviewed a draft of this letter and concurred with our findings. Their oral comments have been incorporated where appropriate.

We identified weaknesses in DOI's formal policies and procedures, contract oversight, and background screening of personnel.

- According to DOI officials, DOI had no formal departmentwide software change control policy. Instead, each component developed its own change control policy. Of the five component policies we reviewed, only BLM and OSM had formally documented change control policies. BIA, NBC-DC, and BOR had policies to control Year 2000 remediation changes, but they had no formally documented process for change control during routine operations. Specifically, the five policies we reviewed either did not address, or did not adequately address key internal controls for
  - testing and approving all new and revised software (NBC-DC),
  - controlling program changes as changes progress from testing to final approval (BIA),
  - authorizing and/or documenting program modifications (NBC-DC and BIA),
  - monitoring access to and use of operating system software (NBC-DC, BIA, OSM, BLM and BOR),
  - controlling application software libraries, including labeling and/or maintaining an inventory of programs (NBC-DC, BOR, BIA, BLM and OSM),
  - limiting access to operating system software (NBC-DC, BOR and BIA), and
  - controlling changes to the operating system software (NBC-DC, BIA, BLM, and OSM).
- We found that agency officials were not familiar with contractor practices for software management. This is of particular concern because DOI contracted for Year 2000 software change activities for 41 (47 percent) of 87 DOI mission-critical federal systems requiring Year 2000 remediation. For example, BOR sent code associated with a mission-critical system to a contractor's facility, and the BOR official did not have information available on how the code was to be protected during and after transit to the contractor facility, when the code was out of the agency's direct control.
- We found, based on our interviews and review of documented security policies and procedures, that background screenings of personnel involved in the software change process were not a routine security control. Of the 12 DOI components we reviewed, only the Minerals Management Service (MMS) and the U.S. Geological Survey required routine background screening of foreign national personnel involved in making changes to software. Further, officials at BOR, the National Business Center in Reston, National

Park Service (NPS), and OSM told us that 6 of 7 contracts for remediation services at these components did not include provisions for background checks of contractor staff.

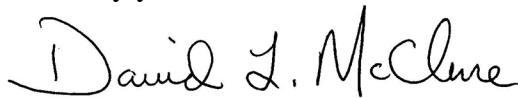
- An MMS official told us that one contractor MMS used for Year 2000 remediation employed foreign nationals. In addition, DOI's Office of Special Trustee and NPS each had a mission-critical system developed, remediated, and maintained at the contractors' facilities, and agency officials did not know whether the contractors employed foreign nationals to work on the code.

In comments on a draft of this letter, DOI stated that it is taking steps to resolve issues noted in this letter and in lessons learned collected during DOI's Year 2000 remediation. Specifically, officials in your office told us that DOI is drafting a permanent policy to significantly improve software change control processes throughout DOI. This policy will be based on the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. To further improve DOI's software change controls, we suggest that you continue this effort and that you review DOI's related contract 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 DOI's participation in this study and the cooperation we received from officials at your office and at the DOI 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](mailto: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](mailto:boltzj.aimd@gao.gov).

Sincerely yours,



David L. McClure  
Associate Director, Governmentwide  
and Defense Information Systems

Enclosure

Enclosure

**Department of Interior Components Included in Study**

1. Bureau of Indian Affairs
2. Bureau of Land Management
3. Bureau of Reclamation
4. Minerals Management Service
5. National Park Service
6. Office of Fish and Wildlife Service
7. Office of the Secretary/National Business Center-Denver
8. Office of the Secretary/National Business Center-District of Columbia
9. Office of the Secretary/National Business Center-Reston
10. Office of Special Trustee
11. Office of Surface Mining
12. U. S. Geological Survey

(511981)