GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285548

June 30, 2000

Ms. Patricia W. Lattimore
Chief Information Officer
Department of Labor

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

Dear Ms. Lattimore:

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

DOL 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 DOL segment of our review, we interviewed an official at DOL's Year 2000 Program Office and Year 2000 project staff at three of the nine DOL components responsible for remediation of mission-critical systems for Year 2000. These three components, which remediated 44 of DOL's 61 mission-critical systems, were the Bureau of Labor and Statistics (BLS), the Employment and Standards Administration (ESA), and the Mine Safety and Health Administration (MSHA).

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.

Use of personnel security controls, such as background screenings of contract personnel involved in the software change process were important because 38 (86 percent) of 44 DOL mission-critical systems covered by our study involved the use of contractors for Year 2000 remediation and all five ESA contracts involved foreign nationals. Of potential concern is that all components included in our review sent application source code for a total of eight mission-critical systems to contractor facilities for remediation, during which time the code was out of the agency's direct control. As a general practice, controls over code are important during the transmission of code to a contractor facility and while at the contractor facility to prevent access to code by, or disclosure of code to, unauthorized individuals for malicious purposes and intelligence gathering activities.

In our review, we identified weaknesses related to formal policies and procedures for the software change control process. Specifically, formally documented change control policies and procedures did not exist at the department-level; however, agency officials told us that substantial efforts were in process to develop and formalize department-level criteria. Also, we found that formally documented component-level policies and procedures for BLS and ESA needed improvement to reflect controls over mainframe operating system software that officials told us were practiced but not documented. The component-level formally documented process for MSHA did not address documenting and authorizing software changes, controlling application software libraries (which includes access to software source code, labeling and inventory of programs, and movement of software program code), and controlling operating system software (which includes changes, access, and monitoring and use of operating system software, including procedures to investigate unauthorized software change activities).

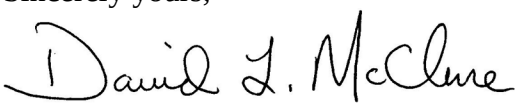
We requested comments on a draft of this letter from your office or your designee. You provided us with written comments that are included in the enclosure. In addition, we have made revisions to this letter to reflect new information provided by BLS and ESA subsequent to our fieldwork, in response to the draft. In your comments, you stated that in May 2000 you issued the *Computer Security Handbook*, which provides guidance for limiting and monitoring access to, and use of, operating system software. You also stated that the *Systems Development and Life Cycle Methodology Manual* has been drafted and is scheduled for final approval in July 2000. You stated that the manual reflects the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software, and addresses change management and control procedures, including the need to document and authorize program modifications and control of application software libraries. We encourage these efforts to improve software change controls.

To further improve DOL controls over software changes, we suggest that you review related contractor oversight and personnel 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 making to Circular A-130, *Management of Federal Information Resources.*

We appreciate DOL's participation in this study and the cooperation we received from officials at your office and at the DOL 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

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

June 7, 2000

Mr. David L. McClure
Associate Director
Governmentwide and
Defense Information Systems
Accounting and Information Management Division
U. S. General Accounting Office
Washington, D.C. 20548

Subject: Draft Letter: *Information Security: Software Change Controls at the Department of Labor*

Dear Mr. McClure:

I appreciate the opportunity to review the draft letter summarizing the results of your recent review of software change controls at the Department of Labor.

Based on the results of our Year 2000 review in January, the Department embarked on a strategy to enhance its change control policies and procedures. The results of this endeavor have been captured in several key guidance documents, including the Department's Computer Security Handbook and Systems Development and Life Cycle Methodology Manual (SDLCM).

The Computer Security Handbook provides guidance for monitoring access to and use of operating system software, and limiting access to operating system software. The Computer Security Handbook was developed based on Office of Management and Budget and NIST guidance, and was issued by the Office of the Chief Information Officer in May 2000.

The Systems Development and Life Cycle Methodology Manual addresses change management and control procedures, including the need to document and authorize program modifications and control of application software libraries. The SDLCM was developed based on IEEE Software and Life Cycle management guidelines (IEEE/EIA Standard 12207.0-1996 and 12207.2-1997) and comports with the Software Engineering Institute's Capability Maturity Model.

The SDLCM, version 2.0 draft was completed on May 31, 2000. The target for final review and approval by the Department's Information Technology (IT) community and IT Capital Planning Investment Review Board is scheduled for July 2000.

GAO's review of federal software change controls was conducted during the period of January through March 2000. Unfortunately, the review activities were broad in nature and did not engage the full participation of a number of key Department personnel, specifically the staff of the Office of the Chief Information Officer. This was an inadvertent and unfortunate oversight that has affected the results of the review. If the Office of the Chief Information Officer had been engaged, the aforementioned progress would have been identified and factored into the review results.

In light of the significant progress the Department has made by proactively identifying and addressing its weaknesses, I request the results of the review be expanded to include the efforts led by the Office of the Chief Information Officer and the development of the Computer Security Handbook and SDLCM guidance documents.

I also have concern that some of the alleged weaknesses are not factually accurate. There are a number of instances where the Department submitted information to GAO in which your letter states this same information was not available or provided.

As there is substantive Departmental information not previously reviewed by GAO -- and an apparent misunderstanding of some important issues -- I request the opportunity for our staffs to meet to discuss these findings before they are issued in final form. I look forward to hearing from you in the near future.

Sincerely,

PATRICIA W. LATTIMORE
Assistant Secretary for
Administration and Management/
Chief Information Officer

(511983)