G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285543

June 30, 2000

Mr. John M. Gilligan
Chief Information Officer
Department of Energy

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

Dear Mr. Gilligan:

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

DOE 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 DOE segment of our review, we interviewed officials in DOE's Office of the Chief Information Officer (OCIO) and Year 2000 project staff at headquarters and at 20 of 34 DOE components responsible for remediation of software for Year 2000. These 20 components, listed in enclosure I, remediated 352 of DOE's 417 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 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 DOE, we identified concerns in three control areas: formal policies and procedures, contract oversight, and background screening of personnel.

- We found that 3 of 20 components—Nevada Operations Office (NOO), Ohio Field Office (OFO), and Western Area Power Administration (WAPA)—had no formally documented process for routine software change control.

- Departmentwide guidance and formal procedures at 17 of the 20 components included in our review were inadequate. Of these 17 components, only headquarters offices had formally adopted the department-level guidance in documented procedures. DOE had established department-level guidance for software engineering that adopted the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. However, the guidance was not mandatory, was adopted by only headquarters offices, and did not address key controls. Specifically, procedures in

  - four components did not address testing of routine software changes;
  - eight components did not address, and nine did not adequately address, controls over application software libraries including access to code, movement of software programs, and inventories of software;
  - sixteen components did not address operating system software access;
  - fifteen components did not address operating system monitoring; and
  - thirteen components did not address operating system software changes.

  Enclosure II identifies the specific weaknesses we identified in each of the 16 components with documented procedures.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because 324 (92 percent) of 352 DOE mission-critical systems covered by our study involved the use of contractors for Year 2000 remediation. For example, AlliedSignal/Kansas City (AlliedSignal), Grand Junction Project Office, Idaho National Engineering Laboratory (INEL), and Oak Ridge Operations Office (OROO) sent code or data associated with five mission-critical systems to contractor facilities, including one offshore foreign-owned company. 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. Also, officials at nine DOE components were unfamiliar with daily contractor practices and either directed us to interview contractor staff to obtain this information or relied on contractor personnel in our interview. These nine components are listed below.

  - AlliedSignal
  - Ames Laboratory (Ames)
  - INEL
  - NOO
  - OROO
  - Office of Civilian Radioactive Waste Management (OCRWM)
  - PANTEX
  - Sandia National Laboratories
  - Savannah River Operations Office

- 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 at all components. For example, officials at Ames, OCRWM, and WAPA told us that four contracts for remediation services did not include provisions for background checks of contractor staff.

- Agency officials at Ames, headquarters, and NREL told us that foreign nationals were employed on three contracts for remediation services. Further, officials at Ames, headquarters, and WAPA did not require routine background screening of foreign national personnel involved in making changes to software. At Ames and headquarters, complete data on the involvement of foreign nationals in software change process activities were not readily available.

In light of these weaknesses, we suggest that you review DOE software change and 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 requested comments on a draft of this letter from the OCIO. We received oral comments from OCIO and from two of DOE's components, BPA and WAPA. OCIO and WAPA concurred with our findings. BPA provided new information showing that it had a formally documented process in place. We have made revisions to this letter to reflect our analysis of this new information. In addition, the BPA official told us that the *Configuration Management Authority* established in April 2000 corrects the software change control weaknesses at BPA that we identify in enclosure II. The WAPA official commented that initiatives are underway to improve software change controls including a dedicated software configuration management staff, a pilot program to assess and enhance process elements, and development of improved administrationwide procedures to be drafted by September 30, 2000. In addition, a Change Control/Configuration Management Group is planned for long-term monitoring of process effectiveness.

We encourage DOE and its components to continue efforts to improve controls over software. We appreciate DOE's participation in this study and the cooperation we received from officials at your office and at the DOE 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

Enclosures

Department of Energy Components Included in Study

1. Albuquerque Operations Office
2. AlliedSignal (Kansas City)
3. Ames Laboratory
4. Bonneville Power Administration
5. Brookhaven National Laboratory
6. Grand Junction Project Office
7. Headquarters, Department of Energy
8. Idaho National Engineering Laboratory
9. National Renewable Energy Laboratory
10. Nevada Operations Office
11. Oak Ridge Operations Office
12. Office of Civilian Radioactive Waste Management
13. Office of Naval Reactors
14. Office of Scientific and Technical Information
15. Ohio Field Office
16. PANTEX
17. Richland Operations Office
18. Sandia National Laboratories
19. Savannah River Operations Office
20. Western Area Power Administration

Weaknesses in DOE Component Software Change Policies and Procedures

Component name	Change Control Areas ("X" = Not Addressed, "NI" = Addressed but Needs Improvement)					
	Changes to application software	Testing	Application software libraries	Access to operating system software	Monitoring and use of operating system software utilities	Operating system software changes
Albuquerque Operations Office			NI	X	X	X
AlliedSignal (Kansas City)		X	NI	X		X
Ames Laboratory		X	NI	X	X	X
Bonneville Power Administration			NI	X	X	NI
Brookhaven National Laboratory			X	X	X	
Grand Junction Project Office			NI	X	X	X
Headquarters Department of Energy			X	X	X	X
Idaho National Engineering Laboratory			X	X	X	X
National Renewable Energy Laboratory		X	X	X	X	
Oak Ridge Operations Office		NI	X	X	X	X
Office of Civilian Radioactive Waste Management			X	X	X	X
Office of Naval Reactors			NI	Incomplete documentation provided	Incomplete documentation provided	Incomplete documentation provided
Office of Scientific and Technical Information			NI	X	X	X
PANTEX			NI	X	X	X
Richland Operations Office	X	NI	X	X	X	X
Sandia National Laboratories		X	X	X	X	X
Savannah River Operations Office			NI	X	X	X

(511980)