GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285184

May 4, 2000

The Honorable Stephen Horn
Chairman, Subcommittee on Government Management,
Information and Technology
Committee on Government Reform
House of Representatives

Subject: Information Security: Controls Over Software Changes at Federal Agencies

Dear Mr. Chairman:

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 opportunity to compromise systems, and unauthorized actions may not be detected.

This letter responds to your November 4, 1999, request for information regarding software change controls at federal agencies. In subsequent discussions with your office, we agreed to determine whether key controls as described in documented policies and procedures regarding software change authorization, testing, and approval comply with federal guidance. In addition, we agreed to determine the extent to which agencies contracted for Year 2000 remediation of mission-critical systems and the extent to which foreign nationals were involved in these efforts. The results of our work are detailed on the enclosed materials, which were discussed at our April 6, 2000, briefing.

To meet these objectives, we interviewed headquarters officials at 16 of the largest federal agencies and officials at 128 of 211 major components of these agencies. We also obtained pertinent written policies and procedures and compared them to federal guidance issued by in the Office of Management and Budget and the National Institute of Standards and Technology. We did not observe agency practices or test agencies' compliance with their policies and procedures. We performed our work from January

through March 2000, in accordance with generally accepted government auditing standards.

Overall, we concluded that controls over changes to software for federal information systems as described in agency policies and procedures were inadequate. Specifically, we identified deficiencies in three control areas: formal policies and procedures, contract oversight, and background screening of personnel.

- Formally documented policies and procedures did not exist or did not meet the requirements of federal criteria. For example, 8 of 16 agencies had not established formal, agencywide policies for software change management, and 50 of 128 agency components had not established formal procedures or adopted agency-level guidance.

- Based on our interviews at the 16 agencies and the 128 components, oversight of contractors was inadequate, especially when software change functions were completely contracted out. This is of potential concern because 1,980 (41 percent) of 4,785 mission-critical federal systems covered by our study involved the use of contractors for Year 2000 remediation. Of particular concern, code or data associated with 319 of these systems were sent to contractor facilities, but agency officials could not readily determine how such code and data were protected during and after transit.

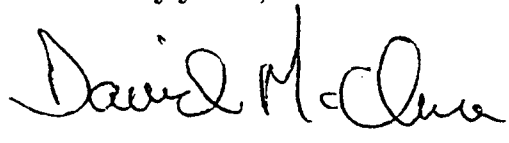
- Based on our interviews with agency officials and review of documented security policies and procedures, background screenings of personnel involved in the software change process were not a routine security control. Of the 128 components we reviewed, 42 did not require routine background screening of foreign national personnel involved in making changes to software. Further, agency officials told us that 24 of 579 contracts for remediation services did not include provisions for background checks of contractor staff. Finally, complete data on use of foreign nationals in the software change process were not readily available.

OMB is in the process of revising its Circular A-130, *Management of Federal Information Resources*, which contains OMB's primary guidance to agencies on protecting federal automated information resources. The proposed revisions do not include any additions or modifications to agency guidance regarding software change controls or related controls pertaining to personnel and contract oversight practices. Because our work identified governmentwide weaknesses in these areas, we plan to recommend, as part of a broader set of comments on the proposed A-130 revisions, that OMB clarify its guidance to agencies. We will send you a copy of these comments when they are provided to OMB.

We are sending copies of this letter to the Honorable Jim Turner, Ranking Minority Member, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform; the Honorable Dan Burton, Chairman and the Honorable Henry Waxman, Ranking Minority Member, House Committee on Government Reform; the Honorable Fred Thompson, Chairman and the Honorable Joseph Lieberman, Ranking Minority Member, Senate Committee on Governmental Affairs; the Honorable Jacob Lew, Director, Office of Management and Budget; and other interested parties. Copies will also be made available to others upon request.

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

Software Change Controls at Federal Agencies

Briefing to the Subcommittee on Government Management, Information and Technology, House Committee on Government Reform

April 6, 2000

Briefing Overview

- Objectives, Scope, Methodology, and Criteria Applied
- Observations
  - Formal Policies and Procedures
  - Controls Over Contract Support
  - Controls Over Personnel and Use of Foreign Nationals

Objectives

The Subcommittee asked us to gather information regarding

- agency controls to ensure that software changes were properly authorized, tested, and approved prior to implementation;
- the extent to which federal agencies contracted out Year 2000 remediation services; and
- the extent to which foreign nationals were involved in Year 2000 remediation.

Scope and Methodology

- We included 16 major federal agencies in our study.
- We interviewed the following officials at 128 of 211 agency components with mission-critical systems remediated for Year 2000:
  - Year 2000 program officials,
  - chief information office technical staff, and
  - contracting officers.
- We performed work in accordance with generally accepted government auditing standards from January through March 2000.

Scope and Methodology (con't)

- We compared formally documented agency and component policies and procedures for software change control and personnel security to criteria.
- We analyzed readily available information on use of contractors and foreign nationals.

Criteria

- The Privacy Act, the Paperwork Reduction Act, and the Computer Security Act require agencies to protect sensitive information.

- The Office of Management and Budget (OMB) Circular A-130, Appendix III, requires key controls for automated systems including background screening of key staff.

- The National Institute of Standards and Technology Special Publications 800-12 and 800-18 require management of software configuration throughout its life cycle.

- GAO's *Federal Information System Controls Audit Manual* provides criteria for assessment of critical software management elements.

Observations

- Formal software change management policies and procedures were lacking or inadequate.

- Remediation activities were contracted out for 41 percent of mission-critical systems included in our study, and controls over contract support were weak.

- Data on the involvement of foreign nationals in Year 2000 remediation efforts were not readily available. However, agency officials told us that foreign nationals were involved in at least 85 of 579 contracts. In addition, background screening policies were inadequate for all personnel involved in software change management.

Formal Policies and Procedures Are Lacking or Inadequate

- Eight of 16 agencies had not established a formal agencywide policy or methodology for software change management.

- Fourteen of 16 agencies delegated software management responsibility to agency components that may further delegate to system owners.

Formal Policies and Procedures Are Lacking or Inadequate (con't)

- Fifty of 128 components had not established formal procedures or adopted agency-level guidance.
- Components that had formal procedures did not always follow agency guidance provided.
- Twenty of 128 components followed different, less-controlled processes for Year 2000 remediation than for routine software management.
- Controls over access to code were weak.

Formal Policies and Procedures Are Lacking or Inadequate (con't)

- The following key controls were frequently not addressed:
  - Documentation, approval, and testing of changes.
  - Maintenance and protection of source code libraries.
  - Separation of duties to prevent unauthorized changes.
  - Labeling and inventory of software programs.
  - Monitoring and addressing unusual change activity.
  - Managing changes to both system software and application software.

Weaknesses in Controls Over Contract Support

- There was limited federal oversight at agencies or components where software change functions were completely contracted out.
- Agencies did not have focal points with knowledge of the extent to which sensitive systems were exposed to contractors or foreign nationals.
- Agencies sent code or data associated with 319 systems to contractor facilities, but officials could not readily determine how such code and data were protected during and after transit.
- Agencies did not include security provisions in 24 of 579 contracts for remediation services.
- Agencies did not have the ability to control remediation of proprietary commercial off-the-shelf software products.

Weaknesses in Controls Over Contract Support

Systems Affected by Contracted Remediation*

	Number of systems	
Mission-critical systems included in component sample	4,785	
Systems contracted out for Year 2000 remediation	1,980	(41%)
Source code sent to external facility:		
Contractor facility (U.S.)	221	(5%)
Contractor facility (Non-U.S.)	98	(2%)
Another federal facility	233	(5%)

* Results are based on unaudited information provided by agency officials.

Weaknesses in Controls Over Contract Support

Data on 579 Contracts Used for Remediation*

	Number of contracts
Existing contracts used for remediation services	394
New contracts awarded for remediation services	101
Contracts with foreign ownership or foreign controlling interest	8
Contracts with foreign nationals on staff	85

* Results are based on unaudited information provided by agency officials.

Personnel Controls and Use of Foreign Nationals

- Forty-two of 128 components did not require performance of routine background screening of foreign nationals or personnel involved in software change management, as required by OMB A-130.

- Information on foreign national staff and related personnel security controls followed was not readily available.

(511685)