GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285553

June 30, 2000

Ms. Janet Barnes
Chief Information Officer
Office of Personnel Management

Subject: Information Security: Software Change Controls at the Office of Personnel Management

Dear Ms. Barnes:

This letter summarizes the results of our recent review of software change controls at the Office of Personnel Management (OPM). 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.

OPM 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 OPM segment of our review, we interviewed Year 2000 project staff at the two OPM components—Retirement and Insurance Service Systems (RISS) and the Non Retirement and Insurance Service Systems—responsible for remediation of software for OPM's 107 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.

According to OPM officials, background checks of personnel involved in the software change process were a routine security control for contractor personnel involved in making changes to software. Also, officials told us that all four contracts for remediation services included provisions for background checks of contractor staff. However, we identified weaknesses regarding formal policies and procedures and contract oversight.

- Office-level guidance for routine software change control did not exist, and formally documented component procedures for Year 2000 software changes were inadequate. Procedures developed by both OPM components for Year 2000 remediation of software did not adequately address key controls for operating system software access and monitoring.

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because 65 (61 percent) of OPM's 107 mission-critical federal systems involved the use of contractors for Year 2000 remediation. Also of concern is that RISS sent code associated with 7 mission-critical systems to a contractor facility for remediation, and agency officials could not readily determine how the code was protected after transit to the contractor facility, when the code was out of the agency's direct control.

- OPM officials did not have complete data on the involvement of foreign nationals in software change process activities. However, officials told us that one of two contracts issued by RISS for remediation of 57 mission-critical systems involved foreign nationals.

We requested comments on a draft of this letter from your office. You provided us with written comments that are included in the enclosure. In your comments, you stated that OPM is actively improving system development procedures to reflect the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software (SW-CMM) and that you have set an ultimate goal to achieve a SW-CMM level 3 process.[1] We encourage you to proceed on this course.

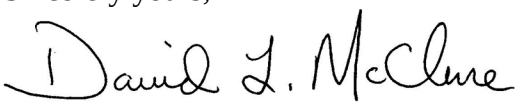
In addition, we suggest that you review related contract oversight and personnel policies and practices and implement any changes that you deem necessary. Because we also identified software control weaknesses at other agencies covered by our review, we have recommended

[1] The Capability Maturity Model is organized into five levels that characterize an organization's software process maturity. These levels range from *initial* (level 1), characterized by ad hoc and chaotic processes, to *optimizing* (level 5), characterized by continuous process improvement based upon analysis and quantitative data. Level 3 is described as the *defined* level, in which the software process for both management and engineering activities is documented, standardized, and integrated.

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

United States
Office of Personnel Management
Washington, DC 20415-0001

JUN 5 2000

In Reply Refer To:

Your Reference:

Mr. David L. McClure
Associate Director, Governmentwide
and Defense Information Systems
United States General Accounting Office
Washington, DC 20548

Dear Mr. McClure:

This is in response to your request for comments on the draft memorandum you recently sent us, Subject: Information Security: Software Change Controls at the Office of Personnel Management. We would like to address a few items that you may have overlooked in your assessment of OPM's software change controls, specifically those addressing office-level guidance for routine software change control and formally documented component procedures for Year 2000 software changes.

While we were preparing for Y2K, Director Lachance issued written policy guidance to institute a moratorium on changes to IT systems. This moratorium on changes to mission-critical systems began on November 1, 1999, and ran through March 1, 2000. During this period, requests for changes required an explicit Y2K impact assessment and personal approval by the responsible program manager. Changes that were made were required to be controlled, documented, and subjected to thorough Y2K testing.

To further implement the Director's guidance, the Retirement and Insurance Service (RIS), the organization that provides technical support for the majority of our mission-critical systems, issued additional guidance. This supplemental guidance provided specific change management procedures for existing systems, new system implementation, new system starts, and emergency changes.

Recognizing that the Year 2000 Project would necessitate extensive changes to application code, RIS implemented comprehensive change control processes and software. The software operates both as a repository for operative code and as a process model for moving code from development, through testing, and into production. With the implementation of this software and related processes, we strictly control application code from beginning to end, with appropriate permissions and acceptance for any changes to the systems.

RIS issued two contracts to support the Y2K remediation effort. The first was for an Inventory/Impact Analysis of mission critical systems. The second, larger contract was for

CON 114-24-3
July 1995

the Renovation, Testing, and Implementation of Y2K compliant code. The second contract was divided into several tasks; one of the first being the development of a comprehensive Software Change Management Plan (SCMP) that described, in detail, what was to be done in the subsequent steps of the Y2K Project. OPM employees participated in the development of the SCMP and were extensively involved in the oversight of the contract to ensure that the plan was executed properly.

A second task of the Renovation contract was to develop and execute a Pilot Project using a representative example of OPM code. The purpose of the Pilot was to test the procedures developed in the SCMP. In addition, as part of the pilot, we did send code to an off-site contractor. We reviewed changes to the code when it came back from the contractor and determined that the renovations were not acceptable. Based on this test, we decided not to use off-site renovation and none of the contractor changes from the off-site facility were used.

As an additional step in our agencywide Y2K effort, we developed a Compliance Verification Program. Compliance Verification provided an added assurance that our mission-critical systems would operate correctly in the Year 2000 and beyond. Under this program, all of our mission-critical systems were subjected to an additional Y2K verification test phase, beyond that performed by our remediation teams during their validation testing. This process included ensuring that our component procedures for change control were documented.

Even though we conducted the Compliance Verification Program and independently verified our systems as Y2K compliant, we recognized that normal system changes could result in the introduction of problems to previously Y2K compliant systems. Therefore, to address this risk, we initiated an additional contractor-assisted Compliance Reverification Program to recheck every mission-critical system. This process did not necessarily require additional Y2K testing, but instead focused on a detailed review of change control documentation and test records.

Although we believe our software change controls procedures are adequate we concur with your recommendations that we adopt industry best practices such as the Carnegie Mellon University Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for software. In fact, we are actively improving our system development procedures. We have developed a system development life cycle (SDLC) model that we call our IT Project Manager. This methodology, when followed, ensures that a system development project will be assessed at SEI CMM Level 2. We feel that by doing this we can incorporate industry best practices into our model at minimal cost while at the same time make strides toward moving OPM to a CMM Level 2 organization. OPM's ultimate goal is to achieve Level 3. By working within this model, the structure for software change control is built into the systems life cycle. We have started the adoption of our IT Project Manager model by phasing it in for individual projects so that we can use the success of these efforts as a springboard to agency-wide implementation.

I hope that this additional information has clarified our past and continued efforts towards adopting industry best practices for software change control. If you have additional questions, please feel free to contact me at 202-606-2150.

Sincerely,

for Janet Barnes
Chief Information Officer

(511988)