



United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285554

June 30, 2000

Mr. John Dyer
Chief Information Officer
Social Security Administration

Subject: Information Security: Software Change Controls at the Social Security Administration

Dear Mr. Dyer:

This letter summarizes the results of our recent review of software change controls at the Social Security Administration (SSA). 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.

SSA 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 SSA segment of our analysis, we contacted officials responsible for SSA's Year 2000 remediation who told us that background screenings of personnel are a routine security control and that no contracts or foreign nationals were used for remediation of 308 SSA mission-critical systems for the Year 2000. We also reviewed a November 1998 SSA Office of the Inspector General's report that detailed weaknesses in SSA's software control policies

and procedures.¹ This report concluded that discipline and consistency in SSA's systems maintenance process have deteriorated because the Software Engineering Technology Manual was difficult to use. In addition, the report stated that SSA needed to establish an organizational commitment to restoring consistency and discipline in its present process while it plans for the future. We performed our work from January through March 2000 in accordance with generally accepted government auditing standards. At the end of our fieldwork, SSA officials reviewed a draft of this letter, orally concurred with our findings, and provided no substantive comments.

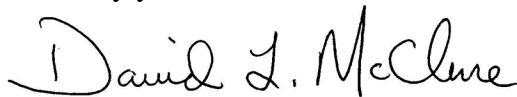
In January 1998, GAO reported² that SSA had established a goal to achieve a level 2, or repeatable, software process maturity based on the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software³ as part of its initiative to improve software processes. SSA's software process improvement initiatives include several activities related to improving software change controls.

- The software maintenance activity process will be improved.
- A process for assessment and implementation of software tools to manage software through its life cycle and control movement of program code will be established.
- A Configuration Control Board process and procedures will be developed.

We suggest that you continue these initiatives to improve software change policies and procedures at SSA. 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 SSA's participation in this study and the cooperation we received from officials at your office. 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

(511989)

¹ *Social Security Administration, Office of Inspector General: Semiannual Report to the Congress*, October 1, 1998, through March 31, 1999.

² *Social Security Administration: Software Development Process Improvements Started But Work Remains* (GAO/AIMD-98-39, January 1998).

³ The Capability Maturity Model is organized into five levels, ranging from *initial* (level 1) to *optimizing* (level 5), to characterize an organization's software process maturity. Level 2 is described as the *repeatable* level, in which basic project management processes are established to track cost, schedule, and functionality.