GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285556

June 30, 2000

Mr. Jim Flyzik
Chief Information Officer
Department of the Treasury

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

Dear Mr. Flyzik:

This letter summarizes the results of our recent review of software change controls at the Department of the Treasury. 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.

Treasury 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 Treasury segment of our review, we interviewed staff from the Chief Information Office, Year 2000 project office, and procurement officials. In addition, we interviewed officials from all 14 Treasury components, listed in the enclosure, which remediated 310 mission-critical systems for Year 2000. 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 Treasury officials, departmental components routinely performed background screenings of federal and contractor personnel involved in software changes, and all 12 components that contracted for Year 2000 remediation services included security provisions in contracts requiring background screenings of personnel. However, we identified weaknesses related to formal policies and procedures and contract oversight.

- Treasury's departmentwide guidance does not detail required software change control processes. However, Treasury's Information System Life Cycle Manual, currently under revision, lists some activities that Treasury's components may implement, including change control.

- Seven of the 14 components covered by our review had formally documented procedures. However, our review of procedures for 6 of these components found that they did not adequately address key controls, such as documentation, approval, and testing of changes; controls over application software libraries; operating system software access, monitoring, and changes; and personnel controls. Financial Management Service (FMS) officials stated that a formally documented process was in place. However, FMS officials did not provide any documentation for our review. Prior GAO reports have shown that FMS software management had been delegated to FMS data center sites and, of those sites visited, most either had not established policies and procedures, had adopted inadequate policies and procedures, or were not following the policies and procedures in place.[1]

- We found that the remaining 7 of 14 components did not have a formally documented process for software change control.
  - Bureau of Engraving and Printing
  - Chief Information Office (CIO)
  - Federal Law Enforcement Training Center
  - Financial Crimes Enforcement Network (FinCEN)
  - Office of Comptroller of the Currency (OCC)
  - U.S. Secret Service
  - U.S. Customs Service

- Based on our interviews, agency officials were not familiar with contractor practices for software management. This is of potential concern because 259 (84 percent) of 310 Treasury mission-critical systems covered by our study involved the use of contractors for Year 2000 remediation. For example, OCC sent code for three systems to contractor facilities, and 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.

[1] *Financial Management Service: Significant Weaknesses in Computer Controls* (GAO/AIMD-00-4, October 4, 1999) and *Financial Management Service: Areas for Improvement in Computer Controls* (GAO/AIMD-99-10, October 20, 1998).

- Six contracts at the CIO, U.S. Mint, Office of Thrift Supervision (OTS), and Internal Revenue Service, involved hiring of foreign nationals. For example, at OTS, remediation of all 15 mission-critical systems involved foreign nationals. Also, according to an agency official, FinCEN contractors were not required to disclose the country of their citizenship. At CIO, FinCEN, IRS, and Customs, complete data on the involvement of foreign nationals in software change process activities were not readily available.

In light of these weaknesses and to further improve Treasury's controls over software changes, we suggest that you review your software change control policies and procedures and consider adopting industry best practices, such as the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software. In addition, we suggest that you review related contract oversight 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 Treasury's Year 2000 Program Project Coordinator. We received oral comments from the Year 2000 Program Project Coordinator, which have been incorporated into this letter where appropriate. The responding official took issue with identifying CIO as a component of Treasury. We acknowledge that CIO is actually an office within Treasury's Departmental Offices (DO) major component. We identify CIO as a component because, for the purposes of this review, CIO had responsibility for remediation of mission-critical systems for Year 2000 separate from those for which DO was responsible.

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

Enclosure

Enclosure

U.S. Department of the Treasury Components Included in Study

1. Alcohol, Tobacco, and Firearms
2. Bureau of the Public Debt
3. Bureau of Engraving and Printing
4. Chief Information Office
5. Departmental Offices
6. Federal Law Enforcement Training Center
7. Financial Crimes Enforcement Network
8. Financial Management Service
9. Internal Revenue Service
10. Office of Comptroller of the Currency
11. Office of Thrift Supervision
12. U.S. Customs Service
13. U.S. Mint
14. U.S. Secret Service

(511991)