G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285545

June 30, 2000

The Honorable Stephen R. Colgate
Chief Information Officer
Department of Justice

Subject: <u>Information Security: Software Change Controls at the Department of Justice</u>

Dear Mr. Colgate:

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

DOJ 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 DOJ segment of our review, we interviewed officials at DOJ's Chief Information Office and Year 2000 project staff at headquarters and at 9 of the 30 DOJ components responsible for remediation of mission-critical systems for the Year 2000. These 9 components, listed in the enclosure, remediated 155 of DOJ's 216 mission-critical systems. We also obtained pertinent written policies and procedures and compared them to federal guidance issued by the Office of Management and Budget (OMB) and the National Institute

of Standards and Technology (NIST). 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.

Based on our interviews and review of documented security policies and procedures, background screenings of personnel involved in the software change process were a routine security control at DOJ. Further, officials told us that all 37 contracts for remediation services of 137 mission-critical systems included provisions for background checks of contractor staff. This is important because we found that although foreign nationals were involved in one DEA contract, officials told us that adequate personnel security controls were practiced. However, we identified several weaknesses related to formal policies and procedures for software change control and contract oversight.

- Formally documented change control policies and procedures did not exist at the department-level, or at the following components.
  - Federal Bureau of Investigation (FBI)
  - INTERPOL
  - Justice Management Division (JMD)
  - U.S. Marshals Service (USMS)

- Formally documented component-level policies and procedures at the Drug Enforcement Administration (DEA), Immigration and Naturalization Service (INS), and Antitrust Division (ATR) did not meet federal criteria. Specifically, the documented procedures at these components did not address key software change controls as detailed below.
  - ATR procedures did not address testing of changes, protection of application software libraries, and restricting and monitoring of access to operating system software.
  - DEA procedures did not adequately address restricting access to program code in application software libraries. In addition, the procedures do not address restricting and monitoring access to operating system software. In comments on a draft of this letter, DEA told us they have undertaken an initiative to improve documentation of their procedures to reflect the Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software (SW-CMM). DEA has set a goal to achieve and maintain a SW-CMM level 3 process.[1]
  - INS procedures did not adequately address control of application software libraries. In addition, the documented procedure does not address restricting and monitoring access to operating system software and controlling changes to operating system software.

- Based on our interviews, DEA and FBI officials were not familiar with contractor practices for software management when source code was out of the agency's direct control. Specifically, the FBI and the DEA electronically transmitted code for six mission-critical systems to contractor facilities for remediation, and agency officials could

---

[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.

not readily determine how the code was protected during and after transit to the contractor facilities.

In light of these weaknesses and to further improve DOJ controls over software changes, we suggest that you review DOJ 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 departmentwide. In addition, we suggest that you review related personnel and 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 DOJ's Year 2000 Program Manager or his designee. We received oral comments from DEA, FBI, and JMD. DEA officials concurred and their comments have been incorporated where appropriate. FBI officials took issue with the need for a formally documented component-level change control process. Although an overall process was not documented, detailed configuration management plans were in place to control changes to specific FBI applications. However, we contend that NIST guidance recommends that all aspects of computer operations should be documented to ensure that not only changes to application configurations are controlled, but also that changes to the operating system software and hardware on which the applications rely are controlled. JMD officials told us that they concur and plan to revise the department-level policy contained in DOJ Order 2640.2c, *Telecommunications and Automated Information Systems Security*, to reflect DOJ's overall process for software change control to be followed by all DOJ components.

We appreciate DOJ's participation in this study and the cooperation we received from officials at your office and at the DOJ 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,
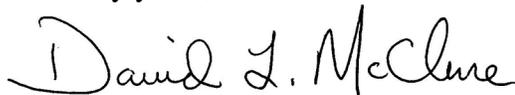
David L. McClure
Associate Director, Governmentwide
  and Defense Information Systems

Enclosure

Enclosure

Department of Justice Components Included in Study

1. Antitrust Division

2. Drug Enforcement Administration

3. Federal Bureau of Investigation

4. Immigration and Naturalization Service

5. INTERPOL

6. Justice Management Division/Finance Staff

7. Justice Management Division/Security & Emergency Planning Staff

8. Justice Management Division/Systems Technology Staff

9. U.S. Marshals Service

(511982)