



United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-285552

June 30, 2000

Mr. Lee Holcomb
Chief Information Officer
National Aeronautics and Space Administration

Subject: Information Security: Software Change Controls at the National Aeronautics and Space Administration

Dear Mr. Holcomb:

This letter summarizes the results of our recent review of software change controls at the National Aeronautics and Space Administration (NASA). 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.

NASA 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 NASA segment of our review, we interviewed an official in NASA's Chief Information Office. Based on a list of data items we provided in writing to NASA, this official provided information about software change control policies and procedures at NASA headquarters and its 10 components. These 10 components, which are listed in enclosure I, remediated 156 mission-critical systems. We did not review the components' written change

control policies and procedures, observe the components' practices, or test 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 the information provided to us, all NASA components performed background screenings of federal, contractor, and foreign national personnel involved in making changes to software. However, we identified concerns regarding NASA's formal policies and procedures and contract oversight.

- NASA does not have a formally documented agency-level software change control policy. Development and implementation of software change policies and procedures are the responsibility of each component. According to the NASA official, the components used their routine software change control processes for Year 2000 remediation. However, we were not provided copies of these component policies to make comparisons to federal guidance. Instead, the agency official provided us with a written explanation of software change practices at NASA components.
- Based on our interview, the agency official was not familiar with contractor practices for software management. This is of potential concern because contractors performed remediation of all 156 mission-critical systems. For example, one contract was with a foreign-owned company that also hired foreign nationals. In addition, source code for two systems was transmitted to contractor facilities, one of which was a foreign-owned facility that received source code for administrative systems. The NASA official provided no details regarding protective controls over the source code when the code was out of the agency's direct control.

We were told by the NASA official that the Mission Operations function of the Goddard Space Flight Center component is certified as a Carnegie Mellon University Software Engineering Institute's Capability Maturity Model for Software (SW-CMM) level 3 organization.¹ In comments on a draft of this letter, you stated that as part of broader efforts to improve software change controls, NASA plans to bring the major internal software activities of NASA's 10 components to SW-CMM level 3. We encourage you to proceed on this course.

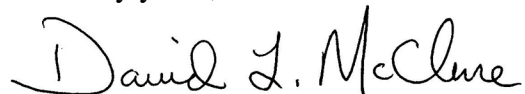
Because we also identified software control weaknesses at other agencies covered by our review, we have recommended that OMB clarify its guidance to agencies regarding software change controls as part of broader revisions that OMB is currently developing to Circular A-130, *Management of Federal Information Resources*.

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.

We requested comments on a draft of this letter from your office. You provided us with written comments which are included in enclosure II. We have incorporated your comments into this letter where appropriate.

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

A handwritten signature in black ink that reads "David L. McClure". The signature is written in a cursive style with a large initial "D".

David L. McClure
Associate Director, Governmentwide
and Defense Information Systems

Enclosures

National Aeronautics and Space Administration Components Included in Study

1. Ames Research Center
2. Dryden Flight Research Center
3. Goddard Space Flight Center
4. Jet Propulsion Lab
5. Johnson Space Center
6. Kennedy Space Center
7. Lewis Research Center
8. Langley Research Center
9. Marshall Space Flight Center
10. Stennis Space Center

National Aeronautics and
Space Administration
Office of the Administrator
Washington, DC 20546-0001



JUN -5 2000

Mr. David L. McClure
Associate Director
Government-wide and Defense Information Systems
United States General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. McClure:

We would like to express our appreciation concerning the effort you and your associates put forth to review the software change processes in use at NASA. We are very aware that effective management and control in this area is critical to assuring the security and integrity of our systems. We, too, are deeply concerned about the three areas reviewed in your report and wish to inform you of the actions we are taking to address them.

The use of foreign nationals for software related work such as Year 2000 remediation can be expected to increase. Congress is currently working on expanding the role of these professionals in the United States due to difficulties in filling software positions. NASA will continue to insist on adequate security evaluations and screening for these individuals, but we expect the situation to continue for some time.

NASA is addressing the lack of a formally documented agency-level software change control process as part of a wider software initiative across the Agency. Part of this initiative will be to establish a NASA-wide set of procedures and guidelines providing detailed guidance for software engineering practice, including software change control. Integral to this document will be the IEEE Standard 12207, Software Lifecycle Processes, which will bring all of NASA into compliance with generally accepted practice.

Increased oversight of contractor software engineering activity will be implemented through more active enforcement of our existing policy directive, NPD 2820.1, NASA Software Policies. This states, in part, that software providers must have "proven organizational capabilities and experience to deliver quality software". The directive also states that acceptable evidence of this is "an independent certification of ISO 9001 compliance as described in ISO 9000-3 or

an independent assessment of a software Capability Maturity Model (CMM) rating of 3 or above". If we assure ourselves that our contractors are operating at this level of capability, we can significantly increase our confidence in their change control processes. It is also worthy of note that another part of our software initiative will be to bring the major internal software activities of our ten components to CMM level 3 as well.

Again, we appreciate all the work your office has done in reviewing our software activities. Please be assured that NASA is addressing your concerns and is moving aggressively to improve our software 'state of the practice'. Secure and reliable software is critical to the Agency's mission and activities. We will provide the resources and take the actions necessary to ensure performance by ourselves and our contractors at an acceptably high level.

Sincerely,



Lee B. Holcomb
Chief Information Officer