



United States
General Accounting Office
Washington, D.C. 20548

151523

Accounting and Information
Management Division

B-256463

April 25, 1994

Mr. E. T. Bender
Project Manager
Workload Control System
Naval Aviation Depot
Department of the Navy
PSC Box 8021
Cherry Point, N.C. 28533

Dear Mr. Bender:

Your November 12, 1993, letter asked us to review and approve the development of your prototype electronic signature module of your time and attendance (T&A) system for compliance with Title 6, "Pay, Leave, and Allowances," of GAO's Policy and Procedures Manual for Guidance of Federal Agencies. That module is to replace the manual certification of T&A data. As we understand it, your office located at the Naval Aviation Depot (NAD) at Cherry Point, North Carolina is developing a prototype electronic signature module that would be available for use in all NADs after it is fully developed and implemented.

As discussed with your staff, we no longer review and approve complete or partial accounting system designs. The approval function required by law (31 U.S.C. 3512(e)(2)) is conducted under one stage, approval of the operating accounting system. Standards for developing T&A systems, or portions of T&A systems, with advanced technologies, such as full automation, are already permitted by Title 6. The criteria for using electronic signatures for certifications are contained in Title 7, "Fiscal Procedures," of the same manual.

However, we do review and as warranted sanction electronic signature modules. As we explained to your staff, a GAO sanction would mean that the proposed electronic signature module, based on a limited review of selected aspects of the design, would generate signatures with attributes of

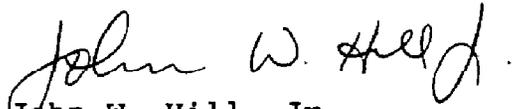
B-256463

valid signatures as outlined in the 1991 Comptroller General decision 71 Comp. Gen. 109.

As discussed with Ms. Jamison of your staff, we will provide our views when necessary on the design and test results of the electronic signature certification module of the T&A system, and provide explanations and interpretations of the requirements in Title 6 and Title 7, as needed. The information needed to assess the design and implementation of the electronic signature module as well as the general internal controls necessary for receiving the sanction are contained in the enclosure to this letter. We look forward to receiving the information referred to in the enclosure and to working with you on this matter.

Should you have any questions, please contact Bruce Michelson, Assistant Director, of my staff, at (202) 512-9366.

Sincerely yours,



John W. Hill, Jr.
Director, Audit Support and
Analysis Group

Enclosure

GAO REVIEW AND SANCTION OF
AN ELECTRONIC SIGNATURE MODULE
OF A TIME AND ATTENDANCE SYSTEM

TYPES OF INFORMATION NEEDED

For purposes of providing a sanction, our review of the design and implementation of an electronic signature module of a T&A system is, by necessity, an iterative process. As the systems are being designed, agencies make choices regarding which procedures, controls, or electronic methods and devices to select to achieve a specific control objective. Consequently, the detailed information necessary to allow GAO to review the module is also derived as the design progresses.

Certain information of a general nature can be initially provided while more detailed information will be specified during meetings or contacts with agency officials as the system design and testing progresses. For example, the first step is the preparation of a detailed conceptual design of the T&A system. This design must describe the T&A data and the related internal controls intended to assure data integrity. This description should include, but is not limited to:

1. A general description of the inherent risk¹ and control risk² involved in the electronic signature process.
2. A functional description of T&A data being originated, entered into automated systems, approved, certified, and recorded in the official agency records.
3. The control objectives intended to be achieved during each of the functional processes and the techniques to be applied in achieving each of the objectives.

¹Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related internal controls.

²Control risk is the risk that a material misstatement that could occur in an assertion will not be prevented or detected and corrected on a timely basis by the entity's internal controls. Internal controls consist of (1) the control environment, (2) the accounting system, and (3) control techniques.

REQUIRED INTERNAL CONTROLS
FOR AN ELECTRONIC SIGNATURE
MODULE OF A T&A SYSTEM

The control objectives of an electronic signature function must ensure that the signatures are (1) unique to the individual, (2) capable of verification, and (3) under the sole control of the individual. In addition, in order for the signature to provide evidence that the signer attests to the accuracy of the T&A data, the signature must be linked to that data in such a manner that if the data is changed, the signature is invalidated. A discussion of these three control objectives is contained in 71 Comp. Gen. 109 (1991).

Depending upon the automated specifications adopted to achieve these overall control objectives, other requirements, such as those issued by the National Institute of Standards and Technology, may also need to be followed. For example, Federal Information Processing Standard (FIPS) 113 provides one method for generating electronic signatures and FIPS 46-2 provides a means for achieving data confidentiality.

(922206)