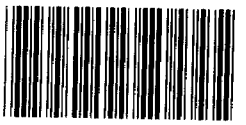
149131

GAO

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

Accounting and Financial
Management Division

B-253174



May 4, 1993

Mr. Charles E. Tompkins, III
Deputy Program Manager
Reserve Component Automation System
Department of the Army

Dear Mr. Tompkins:

This letter responds to your March 5, 1993, request that we sanction the electronic authentication system used in the Reserve Component Automation System (RCAS) for financial applications. RCAS processes unclassified and classified data. Based on the material provided with your letter and discussions with your staff, we have concluded that the electronic signatures generated by this system do not provide the same quality of evidence as the handwritten signatures they are designed to replace. We are unable to sanction your electronic authentication system for financial and contractual purposes because it does not provide reasonable assurance that the signatures generated will meet the criteria outlined in 71 Comp. Gen. 109 (1991). Specifically, we note that your system uses cryptographic algorithms and techniques which have not been approved by either the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA). We do not sanction systems whose algorithms and techniques have not been approved by the appropriate agency.

The Computer Security Act assigns to NIST the authority and the responsibility to establish standards for federal computer systems that process sensitive but unclassified information after coordination with NSA. These standards include acceptable methods to ensure the security and privacy of information in those systems. In addition, NSA establishes polices and procedures that must be used for the protection of classified material. Both NIST and NSA have established procedures for the evaluation and approval of cryptographic algorithms for use by the federal government.

Although the RCAS contractor's conceptual approach of condensing the data to be signed and then encrypting the condensed value can produce acceptable electronic signatures, the techniques adopted do not follow federal government standards and practices which have been approved by NIST and NSA. Our concerns include the use of (1) proprietary cryptographic and hash algorithms which have not been approved by either NIST or NSA and (2) a cryptographic process that primarily depends on the

protection and secrecy of the cryptographic and hash algorithms. We believe that several options are available to address our concerns.

CRYPTOGRAPHIC AND HASH ALGORITHMS

It is our understanding that the cryptographic and hash algorithms used in your system were developed by your contractor and have not been approved by either NIST or NSA. Since these agencies are recognized experts on cryptographic algorithms, systems, and techniques for unclassified and classified applications, respectively, we defer to them for ensuring that the methodology selected is appropriate. The hash algorithm appears to be critical to your signature generation process because it represents a condensed version of the data which is used in that process. Therefore, the hash algorithm needs to be designed so that it is computationally infeasible to (1) find a message which corresponds to a given message digest or (2) find two different messages which will produce the same message digest. As in the case of cryptographic algorithms, very few hash algorithms have maintained their integrity over time.

SECRECY OF CRYPTOGRAPHIC AND HASH ALGORITHMS

As discussed in the material provided, the cryptographic and hash algorithms appear to construct the keys used in their processes from the data being signed. Since the algorithms are able to generate and derive the critical keying material, any individual who has access to the algorithm can derive the key. Once the key is known, the data can be changed and a forged signature generated. When these altered data are validated later, the forged signature will validate the changed data. We are concerned about this approach because relying primarily on an algorithm's secrecy for its security increases the risk of accepting an improper signature as valid. According to a NIST official, good cryptographic systems do not depend entirely on the secrecy of the algorithm. Instead, they depend on (1) using good key generation methods and (2) keeping the critical keying material from unauthorized disclosure.

The unauthorized disclosure of your cryptographic algorithm would be catastrophic to your electronic signature system. All data would become suspect, and the electronic signature system would have to be reengineered. During this reengineering process, other methods, probably costly manual paper and handwritten signatures, would need to be employed. We recognize that in good cryptographic systems the unauthorized disclosure of critical keying material can also cause significant problems and may cause the existing data to become suspect. However, the primary advantage of using sound cryptographic techniques is that the system itself can still be used with new keying material.

Furthermore, the risk of unauthorized disclosure is increased in your system because the electronic signature system is software-based and is maintained in the RCAS system where access is more readily available than if it resided in secure hardware-based cryptographic modules. For example, one possible source of unauthorized disclosure would appear to include the programmers working on the electronic signature generation and validation modules.

AVAILABLE OPTIONS

Adopting and properly implementing government approved standards and techniques would address our concerns. For example, proper implementation of the proposed Digital Signature Standard (DSS) would be acceptable for your unclassified data, and NSA has agreed to accept it on a case-by-case basis for classified applications. Therefore, NSA may also approve its use in your system. Since your system processes classified data, we would also accept a statement from NSA that your system has adequate controls to ensure that the GAO criteria have been met. Specifically, the signatures generated are to be (1) unique to the signer, (2) under the signer's sole control, and (3) capable of being verified. The signatures must also be generated in a manner that links the data to the signature. Therefore, should the underlying data change, the signature would be invalidated during the signature verification process. We recognize that other alternatives may also address our concerns.

- - - - -

We appreciate the opportunity to comment on your proposed electronic signature approach and the challenges that your agency faces in undertaking a major system development such as RCAS. We hope that our comments will assist your efforts. Should you have any questions, please contact Chris Martin, Assistant Director, at (202) 512-9481.

Sincerely yours,

Donald H. Chapin
Assistant Comptroller General

(901633)