April 1991

CSL Bulletin

Advising users on computer systems technology

FIPS 140 - A STANDARD IN TRANSITION

The Computer Systems Laboratory (CSL) of the National Institute of Standards and Technology (NIST) receives many inquiries regarding the implementation of Federal Information Processing Standard (FIPS) 140, *General Security Requirements for Equipment Using the Data Encryption Standard*. Since FIPS 140 is currently being revised and will be reissued as FIPS 140-1, many agency officials ask if the provisions of FIPS 140 still apply. This *CSL Bulletin* addresses these issues and provides guidance to agencies on FIPS waiver procedures. The bulletin does not establish new policy or modify the status of existing FIPS; rather, it summarizes and clarifies existing policy.

Background

FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard,* establishes the physical and logical security requirements for the design and manufacture of Data Encryption Standard (DES) equipment. Previously issued by the General Services Administration as *Federal Standard 1027,* the standard was brought under CSL's responsibility as a result of legislative changes in 1988 and redesignated as FIPS 140. CSL initiated the revision of FIPS 140 to allow agencies to use the latest technologies for the protection of information.

Revision of FIPS 140

The proposed FIPS 140-1 defines four security levels for cryptographic modules:

Level 1 provides a **basic** level of security and is appropriate for implementation in applications having minimum risk and personalized systems such as smart cards. Level 1 products must meet basic security requirements, excluding physical security mechanisms.

Level 2 augments the security of Level 1 by adding requirements for **tamper evident** protection such as coatings or seals.

continued on page 2.

NOTE:

Effective February 10, 1991, a reorganization of the National Institute of Standards and Technology resulted in our name change to the Computer Systems Laboratory (CSL).

CSL Bulletins are published by the Computer Systems Laboratory (CSL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from CSL Publications, National Institute of Standards and Technology, B151, Technology Building, Gaithersburg, MD 20899, telephone (301) 975-2821 or FTS 879-2821. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

The following bulletins are available:

Data Encryption Standard, June 1990

Guidance to Federal Agencies on the Use of Trusted Systems Technology, July 1990

Computer Virus Attacks, August 1990

Bibliography of Computer Security Glossaries, September 1990

Review of Federal Agency Computer Security and Privacy Plans (CSPP): A Summary Report, October 1990

Computer Security Roles of NIST and NSA, February 1991

Level 3 further enhances physical security through the use of **tamper prevention** mechanisms (e.g., if the module's cover is removed, the cryptographic keys are adjusted to zero value.) Additionally, Level 3 provides a significantly higher level of software and firmware assurance and allows software cryptography in multi-user systems at the B2 level of trust.

Level 4 provides specifications for **enhanced tamper prevention** which are particularly useful for operation of devices in a physically unprotected environment. Level 4 also provides for physically (rather than logically) separated plaintext, ciphertext, and key entry paths.

Who we are

CSL is one of nine major science and engineering research components of the National Institute of Standards and Technology (NIST) of the Department of Commerce. We develop standards and test methods, conduct research on computer and related telecommunications systems, and provide technical assistance to government and industry. We seek to overcome barriers to the efficient use of computer systems, to the cost-effective exchange of information, and to the protection of valuable information resources in computer systems.

James H. Burrows, Director

The cryptographic modules applicable to FIPS 140-1 incorporate cryptographic algorithms and functions specified in related FIPS. In this sense, draft FIPS 140-1 is an umbrella standard which provides a framework under which all NIST cryptographic standards are to be implemented in products. This framework will include the Data Encryption Standard (FIPS 46-1), DES Modes of Operation (FIPS 81), Computer Data Authentication (FIPS 113), and anticipated new standards.

All technical provisions of the original standard are being readdressed in the revision process. NIST is also examining various methods for conducting tests for conformance to the requirements of FIPS 140-1.

A draft of FIPS 140-1 is available to interested individuals and organizations as part of the normal standards review process. To request a copy, please contact:

Standards Processing Coordinator (ADP)
National Institute of Standards and Technology
Technology Building, Room B64
Gaithersburg, MD 20899
Telephone: (301) 975-2816

Applicability of FIPS 140

The use of encryption products which conform to FIPS 140 is mandatory for all federal agencies, including defense agencies, for the protection of sensitive unclassified information when the agency determines that cryptographic protection is required. Note that information covered by 10 U.S.C. 2315, commonly referred to as the "Warner Amendment," is excluded from this requirement.

Waiving Provisions of FIPS 140

NIST recognizes that FIPS 140 is in transition and, therefore, waiving its provisions is reasonable under certain circumstances. Heads of federal departments have already been notified that they may wish to consider waiving FIPS 140 in order to buy equipment which is cost-effective and meets their needs, but which may not meet all provisions of the current standard. **Waiving the applicable provisions of FIPS 140 is reasonable when an agency wishes to begin the transition to FIPS 140-1 products.**

Agencies wishing to obtain commercially available security products which meet agency needs but are not in conformance with FIPS 140 are encouraged to review the draft of FIPS 140-1. Given the pending issuance of the revised standard, NIST believes it is reasonable for agencies to begin the transition toward utilization of those types of products which are in concert with the anticipated provisions of FIPS 140-1. The following procedures have been extracted from an attachment to a memorandum from the Secretary of Commerce to the heads of executive departments and agencies, dated November 14, 1988.

Waiver Procedures

"Under certain exceptional circumstances, the heads of federal departments or agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when:

• Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or

• Compliance would cause a major adverse financial impact on the operator which is not offset by Governmentwide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to:

National Institute of Standards and Technology
ATTN: FIPS Waiver Decisions
Technology Building, Room B154
Gaithersburg, MD 20899

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the *Federal Register*.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the *Commerce Business Daily* as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to the notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting or accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency."

Endorsement of DES Products

Agencies frequently ask whether the procurement of NSA-endorsed encryption products for unclassified use is required. Since NSA terminated its Federal Standard 1027 endorsement program of DES encryption devices in 1987, developers of new DES devices cannot obtain this endorsement. Federal agencies may therefore purchase FIPS 140 products that have not been endorsed under the NSA endorsement program without processing a waiver to FIPS 140. To do so, agencies must require written affirmation from vendors that their products are in conformance with the provisions of the current standard. A copy of the vendor's statement of conformance should be sent to NIST.

General Applicability of FIPS

Federal Information Processing Standards, including FIPS 140, do not apply to classified systems or those unclassified defense or intelligence systems which fall under 10 U.S.C. Section 2315. This section of the U.S.C. excludes those Department of Defense systems the function, operation, or use of which:

• involves intelligence activities;

• involves cryptologic activities related to national security;

• involves the direct command and control of military forces;

• involves equipment which is an integral part of a weapon or weapon systems; or

• is critical to the direct fulfillment of a military or intelligence mission.

Agencies should be aware that the National Security Agency (NSA) of the U.S. Department of Defense develops and promulgates requirements for telecommunications and automated information systems operated by the U.S. government, its contractors, or agents, that contain classified national security information or those covered by 10 U.S.C. Section 2315.

Note that the term unclassified information as used in this document **excludes** information covered by 10 U.S.C. 2315.

Additional Information Regarding Cryptographic Standards

NIST recognizes the need to develop FIPS for key generation, key distribution, public key cryptography, and public key certificate distribution. In addition, NIST is actively developing a public key-based digital signature standard.

For additional information regarding DES and associated standards, see the June 1990 issue of the *CSL Bulletin,* which also contains a listing of reference documents.

NIST's Computer Security Program

For information regarding other aspects of NIST's computer security program, please contact:

Computer Security Division
Computer Systems Laboratory
National Institute of Standards and Technology
Technology Building, Room A216
Gaithersburg, MD 20899
Telephone: (301) 975-2934

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology
Bldg. 225/B151
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NO G195