Requirements for Drug-Free Workplace (Grants)'' and the related section of the certification form prescribed above applies;

(3) *Anti-lobbying.* Persons (as defined at 15 CFR Part 28, Section 105) are subject to the lobbying provisions of 31 U.S.C. 1352, ''Limitation on use of appropriated funds to influence certain Federal contracting and financial transactions,'' and the lobbying section of the certification form prescribed above applies to applications/bids for grants, cooperative agreements, and contracts for more than $100,000, and loans and loan guarantees for more than $150,000, or the single family maximum mortgage limit for affected programs, whichever is greater; and

(4) *Anti-lobbying Disclosures.* Any applicant that has paid or will pay for lobbying using any funds must submit an SF–LLL, ''Disclosure of Lobbying Activities,'' as required under 15 CFR Part 28, Appendix B.

(h) Lower Tier Certifications. Recipients shall require applicants/bidders for subgrants, contracts, subcontracts, or other lower tier covered transactions at any tier under the award to submit, if applicable, a completed Form CD–512, ''Certifications Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transactions and Lobbying'' and disclosure form, SF–LLL, ''Disclosure of Lobbying Activities.'' Form CD–512 is intended for the use of recipients and should not be transmitted to NIST. SF–LLL submitted by any tier recipient or sub-recipient should be submitted to NIST in accordance with the instructions contained in the award document.

(i) False Statements. A false statement on an application is grounds for denial or termination of funds and grounds for possible punishment by a fine or imprisonment as provided in 18 U.S.C. 1001

(j) American-made Equipment and Products. Applicants are hereby notified that they are encouraged, to the greatest extent practicable, to purchase American-made equipment and products with the funding provided under this program in accordance with Congressional intent.

(k) North American Free Trade Agreement Patent Notification Procedures. Pursuant to Executive Order 12889, the Department of Commerce (DoC) is required to notify the owner of any valid patent covering technology whenever the DoC or its financial assistance recipient, without making a patent search, knows (or has demonstrable reasonable grounds to know) that technology covered by a valid United States patent has been or will be used without a license from the owner. Applicants selected for awards under this program are required to comply with this executive order.

(l) Intergovernmental Review. Applications under this program are not subject to the requirements of Executive Order 12372, ''Intergovernmental Review of Federal Programs''.

(m) Paperwork Reduction Act. This notice contains collection of information requirements subject to the Paperwork Reduction Act which have been approved by the Office of Management and Budget (OMB Control Number 0693–0005, 0348–0043 and 0348–0044).

Program Execution

(a) Cooperative Agreement. The formal agreement between NIST and the applicant will be in the form of a cooperative agreement. Under this agreement, the NIST MEP will have substantial interactions with the applicant in planning and executing this project. This may include the following:

—Assisting in developing required plans
—Providing access to standard manufacturing extension and related tools
—Facilitating partnering with appropriate organizations both within and outside of the MEP
—Defining measures for evaluation of performance
—Direct involvement in helping to understand, define, and resolve problems in the center's operations

(b) Operating Plan. All recipients of awards are required to submit an Operating Plan within ninety (90) days of the project start date. The Operating Plan is a more detailed statement of work based on project objectives and activities the applicant will undertake to achieve the objectives and incorporates recommendations provided by the evaluation panel and the NIST Program Officer. The Operating Plan must be reviewed and approved by NIST and will be incorporated into the cooperative agreement by amendment. Operating Plan guidelines will be distributed to award recipients.

(c) Project Reporting. Quarterly reports will be submitted to the NIST Program Officer no later than thirty (30) days after the end of each quarter of the award year. The information provided is used to characterize the projects, develop detailed case studies, and evaluate individual examples of outcomes. Quarterly reporting instructions will be distributed to award recipients.

Dated: May 31, 1995.

Samuel Kramer,

Associate Director.

[FR Doc. 95–13764 Filed 6–5–95; 8:45 am]

BILLING CODE 3510–13–M

[Docket No. 950420110–5110–01]

RIN 0693–XX06

Proposed Federal Information Processing Standard (FIPS) for Public Key Cryptographic Entity Authentication Mechanisms

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; request for comments.

SUMMARY: NIST is proposing a FIPS for Public Key Cryptographic Entity Authentication Mechanisms, which will specify two challenge-response mechanisms by which entities in a computer system may authenticate their identities to one another. This standard defines protocols which are derived from an international standard for entity authentication based on public key cryptography using digital signatures and random number challenges.

Public key based authentication is advantageous because no secret information has to be shared by the entities involved in the exchange. In the authentication process, a user employs a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

Prior to the submission of this proposed FIPS to the Secretary of Commerce for review and approval, it is essential to assure that consideration is given to the needs and views of manufacturers, the public, and State and local governments. The purpose of this notice is to solicit such views.

The proposed FIPS contains two sections: (1) An announcement section, which provides information concerning the applicability, implementation, and maintenance of the standard; and (2) a specifications section which deal with the technical aspects of the standard. Only the announcement section of the standard is provided in this notice. Interested parties may obtain copies of the specifications section from the Standards Processing Coordinator, National Institute of Standards and Technology, Technology Building, Room B–64, Gaithersburg, MD 20899, telephone (301) 975–2816.

DATES: Comments on this proposed FIPS must be received on or before September 5, 1995.

ADDRESSES: Written comments concerning the proposed FIPS should be sent to: Director, Computer Systems Laboratory, ATTN: Proposed FIPS for Public Key Authentication, Technology Building, Room B–154, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Written comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Reference and Records Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW., Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Mr. James Foti, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone (301) 975–5237.

Dated: May 31, 1995.

Samuel Kramer,

Associate Director.

Federal Information Processing Standards Publication JJJ

Draft 1995—March 13 Draft

Announcing the Draft Standard for Public Key Cryptographic Entity Authentication Mechanisms

Federal Information Processing Standards (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100–235.

1. Name of Standard. Standard for Public Key Cryptographic Entity Authentication Mechanisms (FIPS PUB JJJ).

2. Category of Standard. Computer Security, Subcategory Access Control.

3. Explanation. This standard specifies two challenge-response mechanisms by which entities in a computer system may authenticate their identities to one another. These mechanisms are used during session initiation, and at any other time that entity authentication is necessary. Depending on which protocol is implemented, either one or both entities involved may be authenticated. The defined protocols are derived from an international standard for entity authentication based on public key cryptography using digital signatures and random number challenges.

Public key based authentication has an advantage over many other authentication schemes because no secret information has to be shared by the entities involved in the exchange. A user (claimant) attempting to authenticate oneself must use a private key to digitally sign a random number challenge issued by the verifying entity. This random number is a time variant parameter which is unique to the authentication exchange. If the verifier can successfully verify the signed response using the claimant's public key, then the claimant has been successfully authenticated.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

6. Cross Index.

a. FIPS PUB 140–1, Security Requirements for Cryptographic Modules.

b. FIPS PUB 171, Key Management Using ANSI X9.17.

c. FIPS PUB 180, Secure Hash Standard.

d. FIPS PUB 186, Digital Signature Standard.

e. FIPS PUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives.

f. ISO/IEC 9798–1:1991, Information technology—Security techniques—Entity authentication mechanisms—Part 1: General model.

g. ISO/IEC 9798–3:1993, Information technology—Security techniques—Entity authentication mechanisms—Part 3: Entity authentication using a public key algorithm.

Other NIST publications may be applicable to the implementation and use of this standard. A list (NIST Publications List 91) of currently available computer security publications, including ordering information, can be obtained from NIST.

7. Applicability. This standard is applicable to all Federal departments and agencies that use public key based authentication systems to protect unclassified information within computer and digital telecommunications systems that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. This standard shall be used by all Federal departments and agencies in designing, acquiring and implementing public key based, challenge-response authentication systems at the application layer within computer and digital telecommunications systems. This includes all systems that Federal departments and agencies operate or that are operated for them under contract. In addition, this standard may be used at other layers within computer and digital telecommunications systems.

This standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it is either cost effective or provides interoperability for commercial and private organizations.

8. Applications. Numerous applications can benefit from the incorporation of public key authentication. Networking applications that require remote login will be able to authenticate clients who have not previously registered with the host, since secret material (e.g., a password) does not have to be exchanged beforehand. Also, point-to-point authentication can take place between users who are unknown to one another. The authentication mechanisms in this standard may be used in conjunction with other public key based systems (e.g., a public key infrastructure that uses public key certificates) to enhance the security of a computer system.

9. Specifications. Federal Information Processing Standard (FIPS) JJJ, *Standard for Public Key Cryptographic Entity Authentication Mechanisms* (affixed).

10. Implementations. The authentication mechanisms described in this standard may be implemented in software, firmware, hardware, or any combination thereof.

11. Export Control. Implementations of this standard are subject to Federal Government export controls as specified in Title 15, Code of Federal Regulations, Parts 768 through 799. Exporters are advised to contact the Department of Commerce, Bureau of Export Administration, for more information.

12. Implementation Schedule. This standard becomes effective (insert six months after approval by the Secretary of Commerce).

13. Qualifications. The authentication technology described in this standard is based upon information provided by sources within the Federal Government and private industry. Authentication systems are designed to protect against adversaries mounting cost-effective attacks on unclassified government or commercial data (e.g., hackers, organized crime, economic competitors). The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff.

14. Waivers. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information

Processing Standards (FIPS). The head of such agency may re-delegate 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:

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

b. 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 classified portions clearly identified, shall be sent to: National Institute of Standards and Technology, ATTN: FIPS Waiver Decisions, Technology Building, Room B–154, 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 such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and 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.

[FR Doc. 95–13765 Filed 6–5–95; 8:45 am]

BILLING CODE 3510–CN–M

[Docket No. 950411101–5101–01]

RIN 0693–XX07

Proposed Federal Information Processing Standard (FIPS) for Standard for the Exchange of Product Model Data (STEP)

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; request for comments.

SUMMARY: NIST is proposing a FIPS for STEP that will adopt the voluntary industry specification, International Organization for Standardization (ISO) Product Data Representation and Exchange, ISO 10303:1994.

STEP defines and describes all product data used during the manufacturing life-cycle of a product, the production steps needed to make a product and the order in which they occur. STEP provides a representation of product information along with the necessary mechanisms and definitions to enable product data to be archived, exchanged, or shared among data bases. The STEP specifications are organized as a series of parts, each published separately. Support for specific applications is provided through application protocols (AP). An AP specifies the information requirements for data exchange, the data representation, and the conformance requirements to support the application.

This proposed FIPS contains two sections: (1) An announcement section, which provides information concerning the applicability, implementation, and maintenance of the standard; and (2) a specification section. Only the announcement section of the standard is provided in this notice. Interested parties may obtain copies of the ISO 10303:1994 from the National Computer Graphics Association, 2722 Merrilee Drive, Suite 200, Fairfax, VA 22031, telephone: (703) 698–9600.

DATES: Comments on this proposed standard must be received on or before September 5, 1995.

ADDRESSES: Written comments concerning the adoption of this proposed standard should be sent to: Director, Computer Systems Laboratory, ATTN: Proposed FIPS for STEP, Technology Building, Room B154, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Written comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Reference and Records Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues NW., Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Ms. Lynne Rosenthal, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone: (301) 975–3353.

Dated: May 31, 1995.

Samuel Kramer,

Associate Director.

Proposed Federal Information Processing Standards Publication

_____

(Date)

Announcing the Standard for Product Data Representation and Exchange (STEP)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administration Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100–235.

1. Name of Standard. Product Data Representation and Exchange, commonly known as the Standard for the Exchange of Product model data (STEP) (FIPS PUB _____).

2. Category of Standard. Software standard; Product data representation and exchange; industrial automation systems and integration.

3. Explanation. This publication adopts the International Organization for Standardization (ISO) 10303: 1994, Product Data Representation and Exchange standard as a Federal Information Processing Standard (FIPS). ISO 10303, more commonly known as STEP, Standard for the Exchange of Product model data, defines a neutral computer-interpretable representation for describing product data in a manner that is independent from any particular system. ISO 10303 specifies the necessary mechanisms and definitions to enable product data throughout the life cycle of a product, to be exchange, archived, or shared among product databases.

The purpose of the FIPS for STEP is to enable the compatible exchange and sharing of product definition data used by a wide range of dissimilar computer-aided design (CAD), engineering, manufacturing and product support applications. The specification provides a neutral format for the exchange and sharing of digital three-dimensional (3D) vector and solid representations for a stated application context. Two-dimensional (2D) vector representation