determination made by the Deputy Minister of National Revenue, Customs, Excise and Taxation respecting Fresh, Whole, Delicious; Red Delicious and Golden Delicious apples, originating in or exported from the United States of America. The Binational Panel Review is terminated. (Secretariat File No. CDA–95–1904–02).

SUMMARY: On February 14, 1995, the Northwest Horticultural Council (NHC) filed a Request for panel review in the above referenced matter with the Canadian Section of the NAFTA Secretariat. On March 17, 1995, the NHC filed a Notice of Motion requesting termination of this panel review. No other interested person filed a request for Panel Review of this final determination. As of March 17, 1995, no Complaint nor Notice of Appearance had been filed by any interested person. Therefore, pursuant to subrules 71(2) and 78(a) of the NAFTA Article 1904 Panel Rules, this Notice of Completion of Panel Review was effective on March 17, 1995.

FOR FURTHER INFORMATION CONTACT: James R. Holbein, United States Secretary, NAFTA Secretariat, Suite 2061, 14th and Constitution Avenue, Washington, D.C. 20230, (202) 482–5438.

Dated: April 7, 1995.

Caratina L. Alston,

Deputy U.S. Secretary, NAFTA Binational Secretariat.

[FR Doc. 95–9408 Filed 4–14–95; 8:45 am]

BILLING CODE 3510–GT–M

National Institute of Standards and Technology

[Docket No. 950215050–5050–01]

RIN 0693–AB33

Approval of Federal Information Processing Standards Publication 180–1, Secure Hash Standard (SHS)

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

ACTION: The purpose of this notice is to announce that the Secretary of Commerce has approved a new standard, which will be published as FIPS Publication 180–1, Secure Hash Standard (SHS).

SUMMARY: On July 11, 1994 (59 FR 35317–35319), and August 5, 1994 (59 FR 40084) notices were published in the **Federal Register** that a revision of Federal Information Processing Standards Publication FIPS PUB 180, Secure Hash Standard (SHS), was being proposed for Federal use.

The written comments submitted by interested parties and other material available to the Department relevant to this revised standard were reviewed by NIST. On the basis of this review, NIST recommended that the Secretary approve the revised standard as Federal Information Processing Standards Publication (FIPS PUB) 180–1, and prepare a detailed justification document for the Secretary's review in support of that recommendation.

The detailed justification document which was presented to the Secretary is part of the public record and is available for inspection and copying in the Department's Central Reference and Records Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW., Washington, DC 20230.

This 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 deals with the technical requirements of the standard. Only the announcement section of the standard is provided in this notice.

EFFECTIVE DATES: This revised standard is effective October 2, 1995.

ADDRESSES: Interested parties may purchase copies of this standard, including the technical specifications section, from the National Technical Information Service (NTIS). Specific ordering information from NTIS for this standard is set out in the Where to Obtain Copies Section of the announcement section of the standard.

FOR FURTHER INFORMATION CONTACT: Mr. Miles Smid, telephone (301) 975–2938, National Institute of Standards and Technology, Gaithersburg, MD 20899.

SUPPLEMENTARY INFORMATION: NIST has been notified that Department of Defense authorities have approved the use of the SHS with the DSS to sign unclassified data processed by ''Warner Amendment'' systems (10 U.S.C. 2315 and 44 U.S.C. 3502(2)) as well as classified data in selected applications.

Dated: April 11, 1995.

Samuel Kramer,

Associate Director.

Federal Information Processing Standards Publication 180–1

(Date)

Announcing the Secure Hash Standard

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 Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100–235.

Name of Standard: Secure Hash Standard.

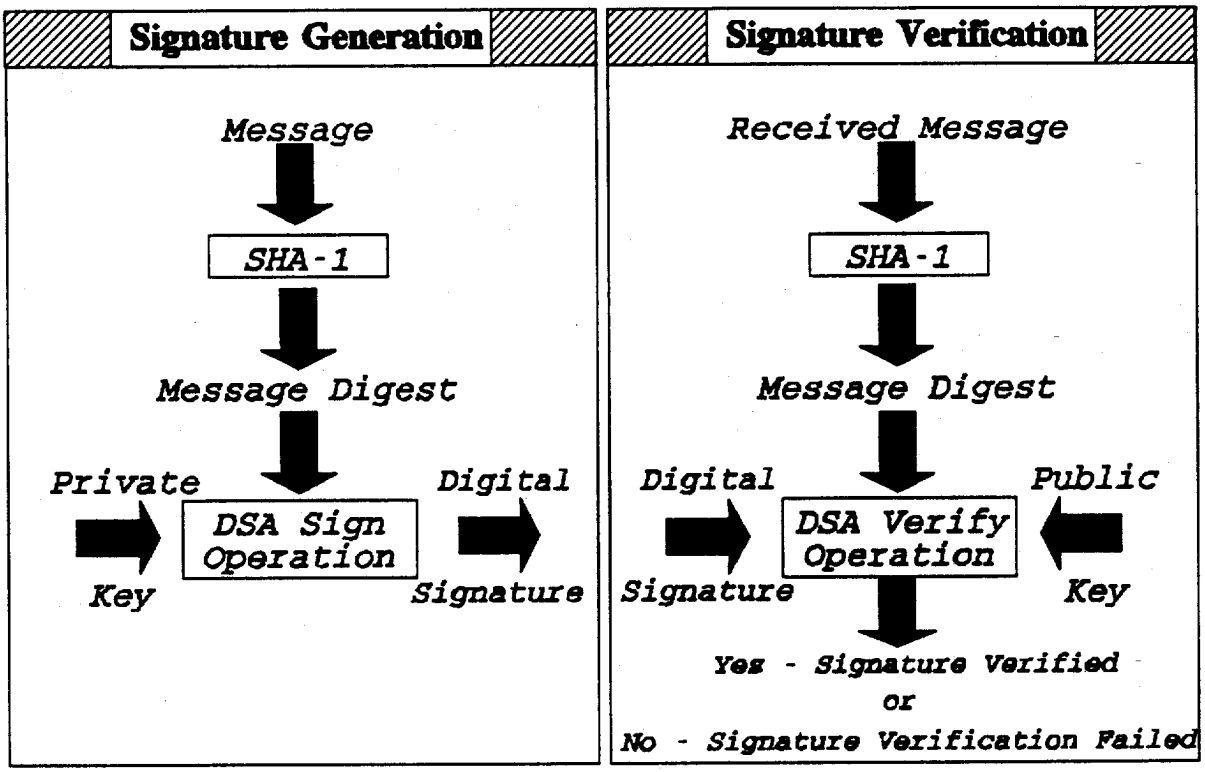
Category of Standard: Computer Security.

Explanation: This Standard specifies a secure hash algorithm, SHA–1, for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA–1 produces a 160–bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message (see Figure 1). Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

The SHA–1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA–1 is a technical revision of SHA (FIPS 180). A circular left shift operation has been added to the specifications in section 7, line b, page 9 of FIPS 180 and its equivalent in section 8, line c, page 10 of FIPS 180. This revision improves the security provided by this standard. The SHA–1 is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm,[1] and is closely modelled after that algorithm.

BILLING CODE 3510–CN–M

[1] ''The MD4 Message Digest Algorithm,'' Advances in Cryptology-CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 303–311.



BILLING CODE 3510–CN–C

Figure 1: Using the SHA–1 With the DSA

Approving Authority: Secretary of Commerce.

Maintenance Agency: U.S. Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

Applicability: This standard is applicable to all Federal departments and agencies for the protection of unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard is required for use with the Digital Signature Algorithm (DSA) as specified in the Digital Signature Standard (DSS) and whenever a secure hash algorithm is required for Federal applications. Private and commercial organizations are encouraged to adopt and use this standard.

Applications: The SHA–1 may be used with the DSA in electronic mail, electronic funds transfer, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication. The SHA–1 may also be used whenever it is necessary to generate a condensed version of a message.

Implementations: The SHA–1 may be implemented in software, firmware, hardware, or any combination thereof. Only implementations of the SHA–1 that are validated by NIST will be considered as complying with this standard. Information about the requirements for validating implementations of this standard can be obtained from the National Institute of Standards and Technology, Computer Systems Laboratory, Attn: SHS Validation, Gaithersburg, MD 20899.

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.

Patents: Implementations of the SHA–1 in this standard may be covered by U.S. and foreign patents.

Implementation Schedule: This standard becomes effective October 2, 1995.

Specifications: Federal Information Processing Standard (FIPS) 180–1, Secure Hash Standard (affixed).

Cross Index

a. FIPS PUB 46–2, Data Encryption Standard.

b. FIPS PUB 73, Guidelines for Security of Computer Applications.

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

d. FIPS PUB 186, Digital Signature Standard.

e. Federal Information Resources Management Regulations (FIRMR) subpart 201.20.303, Standards, and subpart 201.39.1002, Federal Standards.

Objectives: The objectives of this standard are to:

a. Specify the secure hash algorithm required for use with the Digital Signature Standard (FIPS 186) in the generation and verification of digital signatures:

b. Specify the secure hash algorithm to be used whenever a secure hash algorithm is required for Federal applications; and

c. Encourage the adoption and use of the specified secure hash algorithm to private and commercial organizations.

Qualifications: While it is the intent of this standard to specify a secure hash algorithm, conformance to this standard does not assure that a particular

implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security. This standard will be reviewed every five years in order to assess its adequacy.

Waiver Procedure: 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 redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Waiver will 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. Compliance with a standard 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 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 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 accompanying documents, with such deletion as the agency is authorized and decides to make under 5 United States Code Section 552(b), shall be part of the procurement documentation and retained by the agency.

Where to Obtain Copies of the Standard: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 180–1 (FIPSPUB180–1), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

[FR Doc. 95–9386 Filed 4–14–95; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF DEFENSE

Public Information Collection Requirement Submitted to the Office of Management and Budget (OMB) for Review

ACTION: Notice.

The Department of Defense has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Title and Applicable Form: Industrial Capabilities Questionnaire; DD Form X277.

Type of Request: Expedited Processing—Approval date requested: 30 days following publication in the **Federal Register**.

Number of Respondents: 7,500.

Responses per Respondent: 1.

Annual Responses: 7,500.

Average Burden per Response: 27 hours and 27 minutes.

Annual Burden Hours: 205,900.

Needs and Uses: The information collected hereby, will be used by the Department of Defense to perform industrial assessments required as part of its responsibility to encourage the maintenance of a diverse, healthy, and competitive industrial base capable of meeting Departmental needs. The proposed collection consolidates several information collections, including the attendant instruments of collection; i.e., OMB Control Numbers 0702–0037, ''Industrial Base Program Production Capacity, Crisis Production, and Industrial Facility Survey,'' which includes DD Forms 2575, 2575–1, and 2575–2; 0704–0352, ''Industrial Base Assessment Baseline and Update Questionnaires,'' which includes DD Forms 2649 and 2650; 0701–0115, ''Armament Sector Analysis of Precision Guided Munitions Questionnaire;'' and 0703–0033, ''Manufacturing Lead Time Production Solicitation and Occupational Survey.''

Affected Public: Businesses or other for-profit; Federal agencies or employees; and Small Businesses or Organizations.

Frequency: One time and On occasion.

Respondent's Obligation: Voluntary.

OMB Desk Officer: Mr. Peter N. Weiss.

Written comments and recommendations on the proposed information collection should be sent to Mr. Weiss at the Office of Management and Budget, Desk Officer for DoD, Room 10236, New Executive Office Building, Washington, DC 20503.

DOD Clearance Officer: Mr. William Pearce. Written requests for copies of the information collection proposal should be sent to Mr. Pearce, WHS/DIOR, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302.

Dated: April 10, 1995.

Patricia L. Toppings,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

BILLING CODE 5000–04–M