

statements previously submitted to the Department. Toro and Guacatay submitted copies of their income tax returns; however, they failed to reconcile them with their unaudited financial statements. The remaining respondent, Aguaje, claimed it could not substantiate or reconcile the cost data contained in its unaudited financial statement because it had not filed its income tax returns for the POR, as required by the Mexican government. Although Aguaje claimed that it had not filed its returns, it provided no evidence to demonstrate that it was exempt from filing.

The Department relies on the accounting system used in the preparation of the audited financial statements to ensure that a company's submitted sales and cost data are credible. An "in-house" system which has not been audited, and is not used for tax purposes or for any purpose other than internal deliberations of the company, does not assure the Department that costs have been stated in accordance with generally accepted accounting principles, or that all sales and costs have been appropriately captured by the "in-house" system. (See Final Determination at Less Than Fair Value: Certain Hot-Rolled Carbon Steel Flat Products and Certain Cut-To-Length Carbon Steel Plate from Korea, 58 FR 37186 (July 9, 1993).)

For prior review periods, respondents were not required under Mexican law to maintain audited financial statements or file tax returns. We accepted respondents' unaudited "in-house" statements in prior reviews because they did not have, and therefore could not submit, official corroboration of their internal records. (See Notice of Final Results of Antidumping Duty Administrative Review; Certain Fresh Cut Flowers from Mexico, 56 FR 29621, 59622-23 (June 28, 1991).) However, Mexican law governing income tax reporting changed in 1991, and the respondents were required to have filed tax returns covering the POR. Because respondents made inconsistent statements regarding their obligation to file taxes, and further, failed to reconcile their financial statements to their tax records as requested by the Department, we rejected respondents' data in their entirety.

For the reasons stated above, the Department determines that Aguaje, Guacatay, and Toro are uncooperative respondents. As a result, in accordance with section 776(c) of the Act, we have determined that the use of BIA is appropriate. Whenever, as here, a company refuses to cooperate with the Department, or otherwise significantly

impedes an antidumping proceeding, we use as BIA the higher of (1) the highest of the rates found for any firm for the same class or kind of merchandise in the same country of origin in the less-than-fair-value (LTFV) investigation or in prior administrative reviews; or (2) the highest rate found in this review for any firm for the same class or kind of merchandise. (See Antifriction Bearings from France, et al.; Final Results of Review, 58 FR 39729 (July 26, 1993).) As BIA, we assigned the rate of 39.95 percent, which is the second highest rate found for any Mexican flower producer from both the prior reviews and the LTFV investigation. We have selected this rate because the highest rate found for any Mexican flower producer in prior reviews and the LTFV investigation, 264.43 percent, is an aberrational rate not representative of the market. This rate was due to a company's extraordinarily high business expenses during the review period resulting from investment activities which were uncharacteristic of the other reviewed companies. Therefore, we found it inappropriate to use this rate as BIA, both in the prior review and in this review. (See Notice of Final Results of Antidumping Duty Administrative Review; Certain Fresh Cut Flowers from Mexico, 56 FR 29621, 29623 (June 28, 1991).) We preliminarily determine that the following dumping margins exist for the period April 1, 1991, through March 31, 1992:

Manufacturer/Exporter	Margin (percent)
Ranch el Aguaje	39.95
Rancho Guacatay	39.95
Rancho el Toro	39.95
Visaflor	¹ 0

¹ No shipments during the POR. Rate is from the last review in which Visaflor had shipments.

Any interested party may request a hearing within 10 days of publication of this notice. Any hearing will be held 44 days after the date of publication of this notice, or the first workday thereafter. Interested parties may submit case briefs within 30 days of the publication date of this notice. Rebuttal briefs, limited to issues raised in the case briefs, may be filed not later than 37 days after the date of publication of this notice. The Department will publish a notice of the final results of this administrative review, which will include the result of its analysis of issues raised in any such case briefs.

The following deposit requirements shall be effective for all shipments of the

subject merchandise that are entered, or withdrawn from warehouse for consumption, on or after the publication date of the final results of this administrative review, as provided by section 751(a)(1) of the Act: (1) The cash deposit rates for the reviewed companies shall be those rates established in the final results of this review; (2) for previously reviewed or investigated companies not listed above, the cash deposit rate will continue to be the company-specific rate published for the most recent period; (3) if the exporter is not a firm covered in this review, a prior review, or the original LTFV investigation, but the manufacturer is, the cash deposit rate shall be the rate established for the most recent period for the manufacturer of the merchandise; and (4) if neither the exporter nor the manufacturer is a firm covered in this or any previous review, the cash deposit rate will be 18.28 percent, the all others rate established in the LTFV investigation.

These deposit requirements, when imposed, shall remain in effect until publication of the final results of the next administrative review.

This notice serves as a preliminary reminder to importers of their responsibility under 19 CFR 353.26 to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in the Secretary's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

This administrative review and notice are in accordance with section 751(a)(1) of the Act (19 U.S.C. 1675(a)(1)) and section 353.22 of the Department's regulations.

Dated: April 7, 1995.

Susan G. Esserman,
Assistant Secretary for Import Administration.

[FR Doc. 95-9407 Filed 4-14-95; 8:45 am]
BILLING CODE 3510-DS-P

North American Free Trade Agreement (NAFTA), Article 1904 Binational Panel Reviews: Notice of Completion of Panel Review

AGENCY: North American Free Trade Agreement, NAFTA Secretariat, United States Section, International Trade Administration, Department of Commerce.

ACTION: Notice of Completion of Panel Review of the final dumping

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.