or through the email hotline – *vietnam–texapp-monitor–hotline@mail.doc.gov*.

PRODUCT COVERAGE: The Department intends to monitor five product groups – trousers, shirts, underwear, swimwear and sweaters. However, the Department recognizes that these five product groups are too broad for effective monitoring. Within these five groups, the Department intends to focus on those traditional three–digit textile and apparel categories of greatest significance based on trade trends, composition of the U.S. industry and input from parties, as appropriate. In addition to gathering aggregate value data for each of the monitored three–digit categories, the Department intends to gather volume, value and average unit value data for selected products within those categories that will be collected and examined on a 10–digit Harmonized Tariff System (HTS) code basis. All data will be updated monthly and made available to the public on the Import Administration's Office of Textile and Apparel website – *http://www.otexa.ita.doc.gov/*.

Product coverage is not intended by the Department necessarily to be static. Changes in product coverage may occur in response to input received from interested parties, changes in the trade, or as the Department broadens its understanding of the composition and structure of the domestic textile and apparel industry. Further, as the Department's extends its knowledge of the domestic industry and the products it produces, as part of its monitoring, biannual evaluation and like product analysis, it intends to continue its interaction with stakeholders to allow for full comment and input. As part of this process, products may be added or removed from monitoring, as appropriate.

PRODUCTION TEMPLATES: Production templates will be developed on an as–needed basis, as merited by the Department's analysis of the monitored imports, and their impact on, and relation to, the domestic industry. In developing these templates, the Department intends to gather input from parties knowledgeable about the production process. Proxy countries, appropriate for the product being examined, will not be selected until that time.

BIANNUAL EVALUATION: The Department intends to conduct its formal evaluation of the information gathered under the monitoring program on a biannual basis. Interim reviews are not expected to be conducted unless warranted by unforeseen developments.

As explained above, public import data gathered by the Department as part of its monitoring program will be posted on the Import Administration website and updated monthly. Data will be reviewed at the 10–digit HTS level and shifts in product mix and seasonality will be considered when evaluating price and volume trends, as appropriate. In addition to analyzing import data as part of this review process, the Department will consider domestic industry information including production, employment and other indicators of industry health, to the extent relevant to the biannual evaluation process.

SELF–INITIATION: Any self–initiation of an antidumping investigation arising from this program will be fully consistent with U.S. law as set forth in the statute and the Department's regulations, and with the applicable WTO rules.

CRITICAL CIRCUMSTANCES: Any application of critical circumstances in the context of a self–initiated investigation will be fully consistent with U.S. law, and with the applicable WTO rules. Should the Department find critical circumstances, suspension of liquidation would apply to unliquidated entries of merchandise entered, or withdrawn from warehouse, for consumption on or after the later of: 1) 90 days before the date on which suspension of liquidation is first ordered; or 2) the date on which notice of the initiation of the investigation is published in the **Federal Register** (section 733(e)(2) of the Tariff Act of 1930, as amended).

NEW REPORTING REQUIREMENTS: There are no new paperwork or reporting requirements as a result of the Department's monitoring program. Furthermore, all responses to the Department's **Federal Register** notice requests for information, including this request, are strictly voluntary.

Dated: January 17, 2007.

David M. Spooner,

Assistant Secretary for Import Administration.

[FR Doc. E7–928 Filed 1–22–07; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 061213336–6336–01]

Announcing the Development of New Hash Algorithm(s) for the Revision of Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and request for comments.

SUMMARY: A process to develop and standardize one or more new hash algorithms to augment and revise FIPS 180–2, Secure Hash Standard, is being initiated by the National Institute of Standards and Technology (NIST). As a first step in this process, NIST is publishing draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms to solicit public comment. It is intended that the revised hash function standard will specify one or more additional unclassified, publicly disclosed hash algorithms that are available royalty-free worldwide, and are capable of protecting sensitive government information well into the foreseeable future.

The purpose of this notice is to solicit comments on the draft minimum acceptability requirements, submission requirements, and evaluation criteria of candidate algorithms from the public, the cryptographic community, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations so that their needs can be considered in the process of developing the augmented and revised hash function standard.

DATES: Comments must be received on or before April 27, 2007.

ADDRESSES: Written comments should be sent to Mr. William Burr, Attn: Hash Algorithm Requirements and Evaluation Criteria, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930.

Electronic comments should be sent to *hash-function@nist.gov* with a subject line of ''Hash Algorithm Requirements and Evaluation Criteria''.

Comments received in response to this notice will be made part of the public record and will be available for inspection on the Web site: *http://www.nist.gov/hash-function.*

[1] In this announcement, the term ''has function'' and ''hash algorithm'' are used interchangeably.

FOR FURTHER INFORMATION CONTACT: For general information, contact: Shu-jen Chang, National Institute of Standards and Technology, Stop 8930, Gaithersburg, MD 20899–8930; telephone 301–975–2940 or via fax at 301–975–8670.

Technical inquiries regarding the proposed draft acceptability requirements, submission requirements, and evaluation criteria should be sent electronically to *hash-function@nist.gov,* or addressed to William Burr, National Institute of Standards and Technology, Stop 8930, Gaithersburg, MD 20899–8930; telephone 301–975–2914 or via fax at 301–975–8670 (Attn: Hash Algorithm Requirements and Evaluation Criteria). Answers to germane questions will be posted at *http://www.nist.gov/hash-function.* Questions and answers that are not pertinent to this announcement may not be posted.

NIST will endeavor to answer all questions in a timely manner.

SUPPLEMENTARY INFORMATION: A hash function takes binary data, called the message, and produces a condensed representation, called the message digest. A cryptographic hash function is a hash function that is designed to achieve certain security properties. The Federal Information Processing Standard 180–2, Secure Hash Standard specifies algorithms for computing four cryptographic hash functions—SHA–1, SHA–256, SHA–384, and SHA–512. FIPS 180–2 was issued in August, 2002, superseding FIPS 180–1.

In recent years, several of the non-NIST approved cryptographic hash functions have been successfully attacked, and serious attacks have been published against SHA–1. In response, NIST held two public workshops on cryptographic hash functions, on Oct. 31–Nov. 1, 2005 and Aug. 24–25, 2006, to assess the status of its approved hash functions and to solicit public input on its cryptographic hash function policy and standard. As a result of these workshops, NIST has decided to develop one or more additional hash functions through a public competition, similar to the development process for the Advanced Encryption Standard (AES).

To begin the competition process, NIST has drafted the following minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. NIST seeks comments on these draft minimum acceptability requirements, submission requirements, and evaluation criteria, as well as suggestions for other criteria and for the relative importance of each individual criterion in the evaluation process. Since neither the submission requirements nor the evaluation criteria have been finalized, and may evolve over time as a result of the public comments that NIST receives, candidate algorithms should NOT be submitted at this time.

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107–347.

A. Proposed Draft Minimum Acceptability Requirements for Candidate Algorithms

The draft minimum acceptability requirements for candidate hash algorithms are:

A.1 The algorithm must be publicly disclosed and available on a worldwide, non-exclusive, royalty-free basis.

A.2 The algorithm must be implementable in a wide range of hardware and software platforms.

A.3 The algorithm must support 224, 256, 384, and 512-bit message digests, and must support a maximum message length of at least 264 bits.

B. Proposed Draft Submission Requirements

In order to provide for an orderly, fair, and timely evaluation of candidate algorithms, submission requirements will specify the procedures and supporting documentation necessary to submit a candidate algorithm. The submission package must include the following:

B.1 A complete written specification of the algorithm, including any applicable mathematical equations, tables, and parameters that are needed to implement the algorithm. The documentation must include design rationale; an explanation for all the important design decisions; any security argument that is applicable, such as a security reduction proof; and a preliminary analysis, such as possible attack scenarios for collision-finding, second-preimage-finding, or any cryptographic attacks that have been considered and their results.

In addition, the documentation should suggest one or more parameters of the algorithm that can be modified, or suggest other modification techniques, to enhance the security of the design. A supporting rationale should also be provided. For example, for SHA–1 the number of rounds is a natural parameter to modify to increase the security of the design.

B.2 An ANSI C source language reference implementation and an optimized implementation. The optimized code will be used to compare software performance and memory requirements to the implementations of other submitted algorithms.

B.3 A statement of the estimated computational efficiency and memory requirements in hardware and software across a variety of platforms, including 8-, 32-, and 64-bit platforms.

B.4 A hashing example that maps a specified message into its message digest.

B.5 A statement of issued or pending patents that the submitter believes may be infringed by implementations of this algorithm.

B.6 A statement of advantages and limitations of the submitted algorithm. If the submitter believes that the algorithm has certain advantageous features, then these should be listed and described, along with supporting rationale.

Should NIST later decide to add such features to the evaluation criteria, submitters of candidate algorithms may be asked to provide additional information with respect to these new criteria.

(End of draft submission requirements)

C. Proposed Draft Evaluation Criteria of Candidate Algorithms

Candidate algorithms that meet the minimum acceptability requirements and the submission requirements will be compared, based on the following factors:

- Security,
- Computational efficiency,
- Memory requirements,
- Hardware and software suitability,
- Simplicity,
- Flexibility, and
- Licensing requirements.

With the exception of self-explanatory items in the above list, these evaluation criteria are described below.

C.1 Security

Algorithms will be judged on the following factors:

- The actual security provided by the algorithm as compared to other submitted algorithms (of the same hash length), including (but not limited to) first and second preimage resistance, collision resistance, and resistance to generic attacks (e.g., length extension).
- The extent to which the algorithm output is indistinguishable from a random oracle.
- The soundness of the mathematical basis for the algorithm's security.
- Other security factors raised by the public during the evaluation process, including any attacks which demonstrate that the actual security of the algorithm is less than the strength claimed by the submitter.

Correction for the Federal Register Notice: A.3 of the Proposed Draft Minimum Acceptability Requirements for Candidate Algorithms (Section A) should have stated:

"A.3 The algorithm must support 224, 256, 384, and 512-bit message digests, and must support a maximum message length of at least 264 bits."

Claimed attacks will be evaluated for practicality.

C.2 Cost

C.2.1 Computational efficiency: The evaluation of computational efficiency will be applicable to both hardware and software implementations.

Computational efficiency essentially refers to the throughput of an implementation. NIST will use the optimized software of each submission (discussed in B.2 above) on a variety of platforms and analyze their computation efficiency for a variety of message lengths. The data in the submission packages and any public comments on computational efficiency will also be taken into consideration.

C.2.2 Memory requirements: The memory required for hardware and software implementations of the candidate algorithm will be considered during the evaluation process.

Memory requirements will include such factors as gate counts for hardware implementations, and code size and RAM requirements for software implementations.

NIST will use the optimized software of each submission (discussed in B.2 above) on a variety of platforms and test their memory requirements for a variety of message lengths. The data in the submission packages and any public comments on memory requirements will also be taken into consideration.

C.3 Algorithm and Implementation Characteristics

C.3.1 Flexibility: Candidate algorithms with greater flexibility that meet the needs of more users are preferable. Some examples of ''flexibility'' include (but are not limited to) the following:

i. The algorithm is parameterizable, e.g. can accommodate additional rounds.

ii. Implementations of the algorithm can be parallelized to achieve higher performance efficiency.

iii. The algorithm can be implemented securely and efficiently in a wide variety of platforms, including constrained environments such as smart cards.

C.3.2 Simplicity: A candidate algorithm will be judged according to relative simplicity of design.

Dated: January 16, 2007.

James E. Hill,

Acting Deputy Director.

[FR Doc. E7–927 Filed 1–22–07; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[Docket No. 070108002–7002–01; I.D. 122706A]

Listing Endangered and Threatened Species and Designating Critical Habitat: Petition to List Copper and Quillback Rockfishes in Puget Sound (Washington) as Threatened Species under the Endangered Species Act

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of finding.

SUMMARY: We, NMFS, have received a petition to list copper rockfish (*Sebastes caurinus*) and quillback rockfish (*S. maliger*) in Puget Sound (Washington) as threatened or endangered species under the Endangered Species Act (ESA). We find that the petition does not present substantial scientific or commercial information indicating that the petitioned actions may be warranted.

ADDRESSES: Copies of the petition and related materials are available on the Internet at *http://www.nwr.noaa.gov/Other-Marine-Species/PS-Marine-Fishes.cfm*, or upon request from the Chief, Protected Resources Division, NMFS, 1201 NE Lloyd Boulevard, Suite 1100, Portland, OR 97232.

FOR FURTHER INFORMATION CONTACT: Dr. Scott Rumsey, NMFS, Northwest Region, (503) 872–2791; or Marta Nammack, NMFS, Office of Protected Resources, (301) 713–1401.

SUPPLEMENTARY INFORMATION:

Background

On September 18, 2006, we received a petition from Mr. Sam Wright (Olympia, Washington) to list the Puget Sound Distinct Population Segments (DPSs) of copper and quillback rockfish as endangered or threatened species under the ESA. Copies of this petition are available from NMFS (see **ADDRESSES**, above).

ESA Statutory and Policy Provisions

Section 4(b)(3) of the ESA contains provisions concerning petitions from interested persons requesting the Secretary of Commerce (Secretary) to list species under the ESA (16 U.S.C. 1533(b)(3)(A)). Section 4(b)(3)(A) requires that, to the maximum extent practicable, within 90 days after receiving such a petition, the Secretary make a finding whether the petition presents substantial scientific or commercial information indicating that the petitioned action may be warranted. Our ESA implementing regulations define Asubstantial information@ as the amount of information that would lead a reasonable person to believe that the measure proposed in the petition may be warranted. In evaluating a petitioned action, the Secretary considers whether the petition contains a detailed narrative justification for the recommended measure, including: past and present numbers and distribution of the species involved, and any threats faced by the species (50 CFR 424.14(b)(2)(ii)); and information regarding the status of the species throughout all or a significant portion of its range (50 CFR 424.14(b)(2)(iii)).

Under the ESA, a listing determination may address a species, subspecies, or a DPS of any vertebrate species which interbreeds when mature (16 U.S.C. 1532(15)). On February 7, 1996, we and the U.S. Fish and Wildlife Service (USFWS) adopted a policy to clarify the agencies' interpretation of the phrase ''Distinct population segment of any species of vertebrate fish or wildlife'' (ESA section 3(15)) for the purposes of listing, delisting, and reclassifying a species under the ESA (51 FR 4722). The joint DPS policy established two criteria that must be met for a population or group of populations to be considered a DPS: (1) The population segment must be discrete in relation to the remainder of the species (or subspecies) to which it belongs; and (2) the population segment must be significant to the remainder of the species (or subspecies) to which it belongs.

A species, subspecies, or DPS is ''endangered'' if it is in danger of extinction throughout all or a significant portion of its range, and ''threatened'' if it is likely to become endangered within the foreseeable future throughout all or a significant portion of its range (ESA Sections 3(6) and 3(19), respectively).

Life History of Copper and Quillback Rockfish

Copper Rockfish - Copper rockfish are found from the Gulf of Alaska southward to central Baja California (Eschmeyer *et al.*, 1983; Stein and Hassler, 1989; Matthews, 1990a; Love, 1991), including in Puget Sound (Buckley and Hueckel, 1985; Quinnel and Schmitt, 1991). Adult copper rockfish are found in nearshore waters from the surface to 183 m deep (Eschmeyer *et al.*, 1983; Stein and Hassler, 1989). Larval and small juvenile copper rockfish are pelagic for several months and are frequently found