Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: 070911510-7512-01

Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and Request for nominations for candidate hash algorithms.

SUMMARY: This notice solicits nominations from any interested party for candidate algorithms to be considered for SHA-3, and specifies how to submit a nomination package. It presents the nomination requirements and the minimum acceptability requirements of a "complete and proper" candidate algorithm submission. The evaluation criteria that will be used to appraise the candidate algorithms are also described.

DATES: Candidate algorithm nomination packages must be received by **October 31, 2008**. Further details are available in Section 2.

ADDRESSES: Candidate algorithm submission packages should be sent to: Ms. Shu-jen Chang, Information Technology Laboratory, Attention: Hash Algorithm Submissions, 100 Bureau Drive - Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.

FOR FURTHER INFORMATION CONTACT: For general information, send email to hash-function@nist.gov. For questions related to a specific submission package, contact Ms. Shu-jen Chang, National Institute of Standards and Technology, 100 Bureau Drive - Stop 8930, Gaithersburg, MD 20899-8930; telephone: 301-975-2940 or via fax at 301-975-8670, email: shu-jen.chang@nist.gov.

SUPPLEMENTARY INFORMATION: This notice contains the following sections:

3. Minimum Acceptability Requirements
4. Evaluation Criteria
    4.A Security
    4.B Cost
    4.C Algorithm and Implementation Characteristics
5. Initial Planning for the First SHA-3 Candidate Conference
6. Plans for the Candidate Evaluation Process
    6.A Overview
    6.B Round 1 Technical Evaluation
    6.C Round 2 Technical Evaluation
7. Miscellaneous

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.

1. Background

Modern, collision resistant hash functions were designed to create small, fixed size message digests so that a digest could act as a proxy for a possibly very large variable length message in a digital signature algorithm, such as RSA or DSA. These hash functions have since been widely used for many other "ancillary" applications, including hash-based message authentication codes, pseudo random number generators, and key derivation functions.

A series of related hash functions have been developed, such as MD4, MD5, SHA-0, SHA-1 and the SHA-2 family, (which includes 224, 256, 384 and 512-bit variants); all of these follow the Merkle-Damgard construct. NIST began the standardization of the SHA hash functions in 1993, with a specification of SHA-0 in the Federal Information Processing Standards Publication (FIPS PUBS) 180, the Secure Hash Standard; subsequent revisions of the FIPS have replaced SHA-0 with SHA-1 and added the SHA-2 family in FIPS 180-1 and FIPS 180-2, respectively.

Recently, cryptanalysts have found collisions on the MD4, MD5, and SHA-0 algorithms; moreover, a method for finding SHA-1 collisions with less than the expected amount of work has been published, although at this time SHA-1 collisions have not yet been demonstrated. Although there is no specific reason to believe that a practical attack on any of the SHA-2 family of hash functions is imminent, a successful collision attack on an algorithm in the SHA-2 family could have catastrophic effects for digital signatures.

NIST has decided that it is prudent to develop a new hash algorithm to augment and revise FIPS 180-2. The new hash algorithm will be referred to as "SHA-3", and will be developed through a public competition, much like the development of the Advanced Encryption Standard (AES). NIST intends that SHA-3 will specify an unclassified, publicly disclosed algorithm(s), which is available worldwide without royalties or other intellectual property restrictions, and is capable of protecting sensitive information for

decades. Following the close of the submission period, NIST intends to make all "complete and proper" (as defined in Section 3) submissions publicly available for review and comment.

NIST does not currently plan to withdraw SHA-2 or remove it from the revised Secure Hash Standard; however, it is intended that SHA-3 can be directly substituted for SHA-2 in current applications, and will significantly improve the robustness of NIST's overall hash algorithm toolkit. Therefore, the submitted algorithms for SHA-3 must provide message digests of 224, 256, 384 and 512-bits to allow substitution for the SHA-2 family. The 160-bit hash value produced by SHA-1 is becoming too small to use for digital signatures, therefore, a 160-bit replacement hash algorithm is not contemplated.

Many cryptographic applications that are currently specified in FIPS and NIST Special Publications require the use of a NIST-approved hash algorithm. These publications include:

- FIPS 186-2, Digital Signature Standard;
- FIPS 198, The Keyed-Hash Message Authentication Code (HMAC);
- SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; and
- SP 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs).

The SHA-3 algorithm is expected to be suitable for these applications.

Since SHA-3 is expected to provide a simple substitute for the SHA-2 family of hash functions, certain properties of the SHA-2 hash functions must be preserved, including the input parameters; the output sizes; the collision resistance, preimage resistance, and second-preimage resistance properties; and the "one-pass" streaming mode of execution. However, it is also desirable that the selected SHA-3 algorithm offer features or properties that exceed, or improve upon, the SHA-2 hash functions. For example, the selected SHA-3 algorithm may offer efficient integral options, such as randomized hashing, that fundamentally improve security, or it may be parallelizable, more efficient to implement on some platforms, more suitable for certain applications, or may avoid some of the incidental "generic" properties (such as length extension) of the Merkle-Damgard construct that often result in insecure applications.

NIST expects SHA-3 to have a security strength that is at least as good as the hash algorithms currently specified in FIPS 180-2, and that this security strength will be achieved with significantly improved efficiency. NIST also desires that the SHA-3 hash functions will be designed so that a possibly successful attack on the SHA-2 hash functions is unlikely to be applicable to SHA-3. The SHA-3 family should be suitably flexible for a wide variety of implementations, even though it may not operate with optimal efficiency in each and every potential application.

For interoperability, NIST strongly desires a single hash algorithm family (that is, that different size message digests be internally generated in as similar a manner as possible) to be selected for SHA-3. However, if more than one suitable candidate family is identified, and each provides significant advantages, NIST may consider recommending more than one family for inclusion in the revised Secure Hash Standard.

2. Requirements for Candidate Algorithm Submission Packages

Candidate algorithm nomination packages must be received by **October 31, 2008**. Submission packages received before **August 31, 2008** will be reviewed for completeness by NIST; the submitters will be notified of any deficiencies by **September 30, 2008**, allowing time for deficient packages to be amended by the submission deadline. No amendments to packages will be permitted after the submission deadline. Requests for the withdrawal of submission packages will only be honored until the submission deadline.

Due to the specific requirements of the submission package such as Intellectual Property Statements / Agreements / Disclosures as specified in Section 2.D, email submissions will not be accepted for these statements or for the initial submission package. However, email submissions of amendments to the initial submission package will be allowed prior to the submission deadline.

"Complete and proper" submission packages received in response to this notice will be posted at <http://www.nist.gov/hash-competition> for inspection.

To be considered as a "complete" submission package (and continue further in the hash algorithm consideration process), candidate algorithm submission packages must contain the following (as described in detail below):

- Cover Sheet
- Algorithm Specifications and Supporting Documentation
- Optical Media
- Intellectual Property Statements / Agreements / Disclosures
- General Submission Requirements

Each of these items is discussed in detail below.

2.A Cover Sheet

A cover sheet shall contain the following information:

- Name of the submitted algorithm
- Principal submitter's name, e-mail address, telephone, fax, organization, and postal address
- Name(s) of auxiliary submitter(s)

- Name of the algorithm inventor(s)/developer(s)
- Name of the owner, if any, of the algorithm. (normally expected to be the same as the submitter)
- Signature of the submitter
- (optional) Backup point of contact (with telephone, fax, postal address, e-mail address)

2.B Algorithm Specifications and Supporting Documentation

2.B.1 A complete written specification of the algorithm shall be included, consisting of all necessary mathematical operations, equations, tables, diagrams, and parameters that are needed to implement the algorithm. The document shall include design rationale (e.g., the rationale for choosing the specific number of rounds for computing the hashes) and an explanation for all the important design decisions that are made. It should also include 1) any security argument that is applicable, such as a security reduction proof, and 2) a preliminary analysis, such as possible attack scenarios for collision-finding, first-preimage-finding, second-preimage-finding, length-extension attack, multicollision attack, or any cryptographic attacks that have been considered and their results.

In addition, the submitted algorithm may include a tunable security parameter, such as the number of rounds, which would allow the selection of a range of possible security/performance tradeoffs. If such a parameter is provided, the submission document must specify a recommended value for each digest size specified in Section 3, with justification. The submission should also provide any bounds that the designer feels are appropriate for the parameter, including a bound below which the submitter expects cryptanalysis to become practical. The tunable parameter may be used to produce weakened versions of the submitted algorithm for analysis, and permit NIST to select a different security/performance tradeoff than originally specified by the submitter, in light of discovered attacks or other analysis, and in light of the alternative algorithms that are available. NIST will consult with the submitter of the algorithm if it plans to select that algorithm for SHA-3, but with a different parameter value than originally specified by the submitter. Submissions that do not include such a parameter should include a weakened version of the submitted algorithm for analysis, if at all possible.

NIST is open to, and encourages, submissions of hash functions that differ from the traditional Merkle-Damgard model, using other structures, chaining modes, and possibly additional inputs. However, if a submitted algorithm cannot be used directly in current applications of hash functions as specified in FIPS or NIST Special Publications, the submitted algorithm must define a compatibility construct with the same input and output parameters as the SHA hash functions such that it can replace the existing SHA functions in current applications without any loss of security. The replacement of all SHA functions in any standardized application by this compatibility construct shall require no additional modification of the standard application beyond the alteration of any algorithm specific parameters already present in the standard, such as algorithm name and message block length. Submissions may optionally define other variants, constructs, or iterated structures for specific useful applications.

It should be noted that standards which refer to a block length are generally designed with the Merkle-Damgard model in mind, and a number of applications make additional assumptions – for example HMAC implicitly assumes that the message block length is larger than the message digest size. This is not to say that NIST requires the candidate algorithm to satisfy these assumptions, but in cases where the appropriate choice for a parameter such as message block length is not obvious, the submission package must specify a value that will preserve the security properties and functionality of any of the current standard applications.

2.B.2 A statement of the algorithm's estimated computational efficiency and memory requirements in hardware and software across a variety of platforms shall be included. At a minimum, the submitter shall state efficiency estimates for the "NIST SHA-3 Reference Platform" (specified in Section 6.B) and for 8-bit processors. (Efficiency estimates for other platforms may be included at the submitters' discretion.) These estimates shall **each** include the following information, at a minimum:

a. Description of the platform used to generate the estimate, in sufficient detail so that the estimates could be verified in the public evaluation process (e.g., for software running on a PC, include information about the processor, clock speed, memory, operating system, etc.). For hardware estimates, a gate count (or estimated gate count) should be included.

b. Speed estimate for the algorithm on the platform specified in Section 6.B. At a minimum, the number of clock cycles required to:
    1. generate one message digest, and
    2. set up the algorithm (e.g., build internal tables)

   shall be specified for each message digest size required in the Minimum Acceptability Requirements section (Section 3) of this announcement.

c. Any available information on tradeoffs between speed and memory.

2.B.3 A series of Known Answer Tests (KATs) and Monte Carlo Tests (MCTs) shall be included as specified below. All of these KAT and MCT values shall be submitted electronically, in separate files, on a CD-ROM or DVD as described in Section 2.C.3. Each file shall be clearly labeled with header information listing:

1. Algorithm name,
2. Test name,
3. Description of the test, and
4. Message digest size being tested.

All values within the file shall be clearly labeled (e.g., message, message digest, etc.), and shall be in the exact format specified by NIST at <http://www.nist.gov/hash-competition>.

a. All applicable KATs shall be included that can be used to exercise various features of the algorithm. A set of KATs shall be included for each message digest size specified in Section 3. Required KATs include:

   i. If the candidate algorithm calculates intermediate values (e.g., internal rounds) for a message digest computation, then the submitter shall include known answers for those intermediate values for a 1-block and a 2-block message digest computation for each of the required message digest sizes. Examples of providing such intermediate values for the SHA family of hash functions are available at http://www.nist.gov/CryptoToolkitExamples .

   ii. If tables are used in the algorithm, then a set of KAT vectors shall be included to exercise every table entry.

   Note: The submitter is encouraged to include any other KATs that exercise different features of the algorithm (e.g., for permutation tables, etc.). The purposes of these tests shall be clearly described in the file containing the test values.

b. Four MCTs, to be specified at the web site indicated below, shall be included, with message and message digest values, for each of the message digest sizes specified in Section 3.

A link to a description of the required tests will be available at <http://www.nist.gov/hash-competition>. Required submission data for the MCTs will also be found at that location.

2.B.4 A statement of the expected strength (i.e., work factor) of the algorithm shall be included, along with any supporting rationale, for each of the security requirements specified in Sections 4.A.ii and 4.A.iii, and for **each** message digest size specified in Section 3.

2.B.5 An analysis of the algorithm with respect to known attacks (e.g., differential cryptanalysis) and their results shall be included.

To prevent the existence of possible "trap-doors" in an algorithm, the submitter shall explain the provenance of any constants or tables used in the algorithm, with justification of why these were not chosen to make some attack easier.

The submitter shall provide a list of known references to any published materials describing or analyzing the security of the submitted algorithm. The submission of copies of these materials (accompanied by a waiver of copyright or permission from the copyright holder for the SHA-3 public evaluation purposes) is encouraged.

2.B.6 A statement that lists and describes the advantages and limitations of the algorithm shall be included. Such advantages and limitations may address the ability to:

a. implement the algorithm in various environments, including - but not limited to: 8-bit processors (e.g., smartcards), voice applications, satellite applications, or other environments where low power, constrained memory, or limited real-estate are factors. To demonstrate the efficiency of a hardware implementation of the algorithm, the submitter may include a specification of the algorithm in a nonproprietary Hardware Description Language (HDL).

b. use the algorithm with message digest sizes other than those specified in Section 3.

If the submitter believes that the algorithm has certain features that are deemed advantageous, then these should be listed and described, along with supporting rationale. Some examples of these features might include, for example: mathematically (rather than empirically) designed tables, statistical basis for inter-round mixing, etc.

2.C Optical Media

All electronic data shall be provided on a single CD-ROM or DVD labeled with the submitter's name, and the algorithm name.

2.C.1 Reference Implementation

A reference implementation shall be submitted in order to promote the understanding of how the candidate algorithm may be implemented. This implementation shall consist of source code written in ANSI C; appropriate comments should be included in the code, and the code should clearly map to the algorithm description included under Section 2.B.1. Since this implementation is intended for reference purposes, clarity in programming is more important than efficiency.

The reference implementation shall be capable of fully demonstrating the operation of the candidate algorithm. The reference implementation shall support all message digest sizes specified in Section 3. Additionally, it must support all other message digest sizes that are claimed to be supported by the algorithm.

NIST will specify a set of cryptographic service calls, namely a cryptographic API, for the ANSI C implementations, which will be made available at <http://www.nist.gov/hash-competition>. All ANSI C submissions shall implement that API so that the NIST test system can be compatible with all the submissions.

Separate source code for implementing the required KATs with the reference implementation shall also be included. This code shall be able to process input specified in the format indicated by NIST (on the web site as referred to under Section 2.B.3) and run the required tests.

The reference implementation shall be provided in a directory labeled: \Reference Implementation.

2.C.2 Optimized Implementations

Two optimized implementations of the candidate algorithm shall be submitted - one implementation that is optimized for a 32-bit platform, and another for a 64-bit platform. The optimized implementations shall be specified in the ANSI C programming language. These implementations will be evaluated on 32- and 64-bit platforms.

General Requirements for Both Optimized Implementations:

- Both of the optimized implementations shall support the message digest sizes specified in Section 3.
- Separate source code for implementing the required KATs and MCTs with the optimized implementations shall also be included. This code shall be able to process the input specified in the format indicated by NIST (on the web site as referred to under Section 2.B.3) and run the required tests.
- The submitter shall provide the optimized implementations in two separate directories labeled:
    - \Optimized_32 bit
    - \Optimized_64 bit

  respectively.
- Additionally, submitters may, at their discretion, submit revised optimized implementations (for both the 32- and 64-bit implementations) for use in the Round 2 evaluation process, allowing additional time for improvements. These must be received prior to the beginning of the Round 2 evaluation; submitters will be notified of the specific deadline, as appropriate. Note that the optimized implementations on file with NIST at the close of the initial submission period will be the ones used by NIST in the Round 1 evaluation.

2.C.3 Test Values - Known Answer Tests and Monte Carlo Tests

The files on the CD-ROM or DVD shall contain all of the test values required under Section 2.B.3 of this announcement. That section includes descriptions of the required tests, as well as a list of the values that must be provided.

The required format for the test vectors will be specified by NIST at <http://www.nist.gov/hash-competition>.

The test values shall be provided in a directory labeled: \KAT_MCT.

2.C.4 Supporting Documentation

To facilitate the electronic distribution of submissions to all interested parties, **copies of all written materials must also be submitted in electronic form in PDF**. Submitters

are encouraged to use the thumbnail and bookmark features, to have a clickable table of contents (if applicable), and to include other links within the PDF as appropriate.

This electronic version of the supporting documentation shall be provided in a directory labeled: \Supporting Documentation.

2.C.5 General Requirements for Optical Media

For the portions of the submissions that may be provided electronically, the information shall be provided on a single CD-ROM or DVD using the ISO 9660 format. This disc shall have the following structure:

- \README
- \Reference Implementation
- \Optimized_32 bit
- \Optimized_64 bit
- \KAT_MCT
- \Supporting Documentation

The "README" file shall list all files that are included on this disc with a brief description of each.

All optical media presented to NIST must be free of viruses or other malicious code. The submitted media will be scanned for the presence of such code. If malicious code is found, NIST will notify the submitter and ask that a clean version of the optical media be re-submitted.

NIST will define a set of cryptographic service calls for the ANSI C implementations. These calls will be used by the NIST test software to make appropriate calls to the optimized and reference implementations, so that the test software does not have to be rewritten for each submitted algorithm. Therefore, **both the optimized and reference implementations are required to conform to these specific calls**. The implementations shall be supplied in source code so that NIST can compile and link them appropriately with the test software. The two selected sets of required calls will be available at the following location: <http://www.nist.gov/hash-competition>. NIST intends to make these available within three months after publication of this notice.

2.D Intellectual Property Statements / Agreements / Disclosures

Each submitted algorithm must be available worldwide on a royalty free basis during the period of the hash function competition. In order to ensure this and minimize any intellectual property issues, the following series of signed statements are required for a submission to be considered complete: Statement by the Submitter, Statement by Patent (and Patent Application) Owner(s) (if applicable), and Statement by Reference/Optimized Implementations' Owner(s). Note for the last two statements, separate statements must be completed if multiple individuals are involved.

2.D.1 Statement by the Submitter

I, _____ (print submitter's full name) _____ do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as ____ (print name of algorithm)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if appropriate)_____ .

I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted algorithm, reference implementation or optimized implementations. **– OR –** *I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or optimized implementations: _____ (describe and enumerate) _____.*

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).

Signed:
Title:
Dated:
Place:

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner of the patent and patent applications above identified.

I, _____ (print full name) _____ , of _____(print full postal address)_____ , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): _____ (enumerate) _____ , and do hereby agree to grant to any interested party if the algorithm known as _____(print name of algorithm) _____ is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.

Signed:
Title:
Dated:
Place:

Note that the U.S. government may conduct research as may be appropriate to verify the availability of the submission on a royalty free basis worldwide.

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, _____ (print full name) _____ , am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.

Signed:
Title:
Dated:
Place:

2.E General Submission Requirements

NIST welcomes both domestic and international submissions; however, in order to facilitate analysis and evaluation, it is required that the submission packages be in English. This requirement includes the cover sheet, algorithm specification and supporting documentation, source code, and intellectual property information. Any required information that is submitted in a language other than English shall render the

submission package "incomplete." Optional supporting materials (e.g., journal articles) in another language may be submitted.

Classified and/or proprietary submissions will not be accepted.

2.F Technical Contacts and Additional Information

For technical inquiries, send email to hash-function@nist.gov, or contact Mr. William Burr, National Institute of Standards and Technology, 100 Bureau Drive - Stop 8930, Gaithersburg, MD 20899-8930; telephone: 301-975-2914 or via fax at 301-975-8670, email: william.burr@nist.gov (Attn: Hash Algorithm Competition Questions).

Answers to germane questions will be posted at <http://www.nist.gov/hash-competition>. 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.

3. Minimum Acceptability Requirements

Those packages that are deemed to be "complete" will be evaluated for the inclusion of a "proper" candidate algorithm. To be considered as a "proper" candidate algorithm submission (and continue further in the SHA-3 Development Process), a candidate hash algorithm shall meet the following minimum acceptability requirements:

1. The algorithm shall be publicly disclosed and available worldwide without royalties or any intellectual property restrictions.

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

3. The candidate algorithm shall be capable of supporting message digest sizes of 224, 256, 384, and 512 bits, and shall support a maximum message length of at least 2^{64}-1 bits. Submitted algorithms may support other message digest sizes and maximum message lengths, and such features will be taken into consideration during the analysis and evaluation period.

(End of minimum acceptability requirements)

A candidate algorithm submission package that is complete (as defined above) and whose algorithm meets the minimum acceptability requirements (as defined immediately above) will be deemed to be a "complete and proper" submission. A submission that is deemed otherwise at the close of the submission period will receive no further consideration. Submissions that are "complete and proper" will be posted at <http://www.nist.gov/hash-competition> for public review.

4. Evaluation Criteria

In order to provide a basis for the analysis and evaluation of hash algorithms submitted to be considered for SHA-3, evaluation criteria will be used to review candidate algorithms. NIST will form an internal selection panel composed of NIST employees to analyze the candidate algorithms; the evaluation process will be discussed in Section 6. All of NIST's analysis results will be made publicly available.

Although NIST will be performing its own analyses of the candidate algorithms, NIST strongly encourages public evaluation and publication of the results, including any complete or partial analysis of a candidate algorithm or component of an algorithm (e.g., the compression function or iterative structure), and whether the result is positive or negative. NIST will take into account its own analysis, as well as the public comments that are received in response to the posting of the "complete and proper" submissions, to make its decision on the selection of SHA-3.

Candidate algorithms with submission packages deemed to be "complete and proper" will be compared, based on the following factors (ranked in the order of relative importance):

4.A Security

The security provided by an algorithm is the most important factor in the evaluation. Algorithms will be judged on the following factors:

i. Applications of the hash functions

   Algorithms having the same hash length will be compared for the security that may be provided in a wide variety of cryptographic applications, including digital signatures (FIPS 186-2), key derivation (NIST Special Publication 800-56A), hash-based message authentication codes (FIPS 198), deterministic random bit generators (SP 800-90), and additional applications that may be brought up by NIST or by the public during the evaluation process. Claimed applications of the hash functions will be evaluated for their practical importance if this evaluation is necessary for comparing the submitted hash algorithms.

ii. Specific requirements when hash functions are used to support HMAC, Pseudo Random Functions (PRFs), and Randomized Hashing:

   NIST requires that the selected SHA-3 support HMAC, PRFs, and randomized hashing. Each candidate algorithm must have at least one construction to support HMAC as a PRF; it may have additional constructions for other, non-HMAC based PRFs, or for use in a randomized hashing scheme. The following criteria will be used to evaluate each candidate algorithm of message digest size n in such constructions.

- When the candidate algorithm is used with HMAC to construct a PRF as specified in the submitted package, that PRF must resist any distinguishing attack that requires much fewer than $2^{n/2}$ queries and significantly less computation than a preimage attack.
- Any additional PRF constructions specified for use with the candidate algorithm must provide the security that is claimed in the submission document.
- If a construct is specified for the use of the candidate algorithm in a randomized hashing scheme, the construct must, with overwhelming probability, provide *n* bits of security against the following attack: The attacker chooses a message, M_1. The specified construct is then used on M_1 with a randomization value r_1 that has been randomly chosen without the attacker's control after the attacker has supplied M_1. Given r_1, the attacker then attempts to find a second message M_2 and randomization value r_2 that yield the same randomized hash value.

iii. Additional security requirements of the hash functions

In addition to the specific requirements mentioned above, NIST expects the SHA-3 algorithm of message digest size *n* to meet the following security requirements at a minimum. These requirements are believed to be satisfiable by fairly standard hash algorithm constructions; any result that shows that the candidate algorithm does not meet these requirements will be considered to be a serious attack.

- Collision resistance of approximately *n*/2 bits,
- Preimage resistance of approximately *n* bits,
- Second-preimage resistance of approximately *n*-*k* bits for any message shorter than 2^k bits,
- Resistance to length-extension attacks, and
- Any *m*-bit hash function specified by taking a fixed subset of the candidate function's output bits is expected to meet the above requirements with *m* replacing *n*. (Note that an attacker can choose the *m*-bit subset specifically to allow a limited number of precomputed message digests to collide, but once the subset has been chosen, finding additional violations of the above properties is expected to be as hard as described above.)

Increasing the second preimage resistance property and resistance against other attacks, such as multicollision attacks, will be viewed positively by NIST; however, this could also have performance implications. Submitters should be prepared to argue for their overall security/performance trade-offs.

iv. Evaluations relating to attack resistance

Hash algorithms will be evaluated against attacks or observations that may threaten existing or proposed applications, or demonstrate some fundamental flaw in the design, such as exhibiting nonrandom behavior and failing statistical tests.

Claimed attacks will be evaluated for their practicality and for their impact on applications. Attacks that violate the security of an existing FIPS or NIST Special Publication's use of a hash function will be given more weight than attacks that violate the security of other applications; and attacks on rare or obscure applications may be given relatively little weight.

Hash algorithms will be evaluated not only for their resistance against previously known attacks, but also for their resistance against attacks discovered during the evaluation process, and for their likelihood of resistance against future attacks.

v. Other consideration factors

In addition to the evaluation factors mentioned above, the quality of the security arguments/proofs, the clarity of the documentation of the algorithm, the quality of the analysis on the algorithm performed by the submitters, the simplicity of the algorithm, and the confidence of NIST and the cryptographic community in the algorithm's long-term security may all be considered.

4.B Cost

As described in Section 2.C.2, submitters of hash algorithms may submit revised optimized implementations for use in the Round 2 evaluation process. In the following discussion, it should be noted that all technical evaluations are performed either on the optimized implementations that are received initially, or on the revised implementations that are received before the beginning of Round 2.

i. *Computational efficiency*: The evaluation of the computational efficiency of the candidate algorithms will be applicable to both hardware and software implementations. The Round 1 analysis by NIST will focus primarily on software implementations; hardware implementations will be addressed more thoroughly during the Round 2 analysis.

Computational efficiency essentially refers to the speed of the algorithm. The computational efficiency will be analyzed using each submission's optimized implementations on a variety of platforms as specified in Section 6.B, and for a variety of input message lengths. The data in the submission packages and public comments on each algorithm's efficiency (particularly for various platforms and applications) will also be taken into consideration by NIST.

ii. *Memory requirements*: The memory required to implement a candidate algorithm - for both hardware and software implementations of the algorithm - will also be considered during the evaluation process. The Round 1 analysis will focus primarily on software implementations; hardware implementations will be addressed more thoroughly during Round 2.

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

Testing will be performed by NIST using the optimized implementations provided by the submitters. Memory requirement estimates (for different platforms and environments) that are included in the submission package or the revised optimization package will also be taken into consideration by NIST. Input from the public evaluations of each algorithm's memory requirements (particularly for various platforms and applications) will also be taken into consideration by NIST.

4.C Algorithm and Implementation Characteristics

i. *Flexibility*: Candidate algorithms with greater flexibility will meet the needs of more users than less flexible algorithms, and therefore, are preferable. However, some extremes of functionality are of little practical use (e.g., extremely short message digest lengths) - for those cases, preference will not be given.

Some examples of "flexibility" may include (but are not limited to) the following:

a. The algorithm has a tunable parameter which allows the selection of a range of possible security/performance tradeoffs.
b. The algorithm can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.
c. Implementations of the algorithm can be parallelized to achieve higher performance efficiency.

ii. *Simplicity*: A candidate algorithm will be judged according to its relative design simplicity.

5. Initial Planning for the First SHA-3 Candidate Conference

An open public conference will be held shortly after the end of the submission period, at which the submitter of each complete and proper submission package will be invited to publicly discuss and explain their candidate algorithm. The documentation for these candidate algorithms will be made available at the Conference. Details of the conference will be posted at <http://www.nist.gov/hash-competition>.

6. Plans for the Candidate Evaluation Process

NIST plans to form an internal selection panel composed of NIST employees for the technical evaluations of the candidate algorithms. This panel will analyze the submitted algorithms, review public comments that are received in response to the posting of the

"complete and proper" submissions, and all presentations, discussions and technical papers presented at the SHA-3 Candidate Conferences, as well as other pertinent papers and presentations made at other cryptographic research conferences and workshops. NIST will issue a report on each SHA-3 Candidate Conference, make a final selection and document the technical rationale for that selection in a final report, as NIST did in the selection of AES. The following is an overview of the envisioned SHA-3 candidate review process.

6.A Overview

Following the close of the call for candidate algorithm submission packages, NIST will review the received packages to determine which are "complete and proper," as described in Sections 2 and 3 of this notice. NIST will post all "complete and proper" submissions at <http://www.nist.gov/hash-competition> for public inspection. To help inform the public, the First SHA-3 Candidate Conference will be held at the start of the public comment process to allow submitters to publicly explain and answer questions regarding their submissions.

Round 1 will consist of a twelve-month public review of the first round candidate algorithms. During the Round 1 public review, NIST intends to evaluate the candidate algorithms as outlined in Section 6.B. NIST will review the public evaluations of the candidate algorithms' cryptographic strengths and weaknesses, and will use these to narrow the candidate pool for more careful study and analysis during Round 2.

Because of limited resources, and also to avoid moving evaluation targets (i.e., modifying the submitted algorithms undergoing public review), NIST will NOT accept modifications to the submitted algorithms during Round 1.

For informational and planning purposes, near the end of the Round 1 public evaluation process, NIST intends to hold the Second SHA-3 Candidate Conference. Its purpose will be to publicly discuss the SHA-3 candidate algorithms, and to provide NIST with information for narrowing the field of algorithms to be considered for SHA-3.

NIST plans to narrow the field of candidates to approximately five candidate algorithms for further analysis during Round 2, based upon its own analysis, public comments, and all other available information. It is envisioned that this narrowing will be done primarily on security, efficiency, and intellectual property considerations. For those candidate algorithms not selected for Round 2, the rights to use the algorithms will be returned to their respective submitters.

Before the start of the Round 2 evaluation period, the submitters of the Round 2 candidate algorithms will have the option of providing updated optimized implementations for use during the second phase of evaluation. During the course of the Round 1 evaluations, it is conceivable that some small deficiencies may be identified in even some of the most promising candidates. Therefore, for the Round 2 evaluations, small modifications to the submitted algorithms will be permitted for either security or

efficiency purposes. Submitters may submit minor changes (no substantial redesigns), along with a supporting explanation/justification that must be received by NIST prior to the beginning of Round 2. (Submitters will be notified by NIST of the exact deadline.) NIST will determine whether or not the proposed modification would significantly affect the design of the algorithm, requiring a major re-evaluation; if such is the case, the modification will not be accepted. If modifications are submitted, new reference and optimized implementations and written descriptions shall be provided by the start of Round 2. This will allow a public review of the modified algorithms during the entire course of the Round 2 evaluation.

Note: All proposed changes for Round 2 must be proposed by the submitter; no proposed changes (to the algorithm or implementations) will be accepted from a third party.

Round 2 will consist of a twelve to fifteen month public review of the Round 2 candidate algorithms. During the public review, NIST will evaluate the candidate algorithms as outlined in the two sections below. After the end of the public review period, NIST intends to hold the Third SHA-3 Candidate Conference. (The exact date is to be scheduled.)

Following the Third SHA-3 Candidate Conference, NIST will select the algorithm(s) for SHA-3. The selected algorithm(s) will be incorporated into a draft FIPS, which will be announced in the **Federal Register** for public comment.

It should be noted that this schedule for the SHA-3 development is somewhat tentative, depending upon the type, quantity, and quality of the submissions. Specific conference dates and public comment periods will be announced at appropriate times in the future.

6.B Round 1 Technical Evaluation

NIST will invite public comments on all complete and proper submissions. NIST's Round 1 analysis is intended, at a minimum, to be performed as follows:

i. *Correctness check*: The KAT and MCT values included with the submission will be used to test the correctness of the reference and optimized implementations, once they are compiled. (It is more likely that NIST will perform this check of the reference code - and possibly the optimized code as well - even before accepting the submission package as "complete and proper.")

ii. *Efficiency testing*: Using the submitted optimized implementations, NIST intends to perform various computational efficiency tests, including the calculation of the time required to compute message digests for various length messages.

iii. *Other testing*: Other features of the candidate algorithms may be examined by NIST.

Platform and Compilers

The above tests will initially be performed by NIST with the following tools, at a minimum.

i. NIST Reference Platform: Wintel personal computer, with an Intel Core 2 Duo Processor, 2.4GHz clock speed, 2GB RAM, running Windows Vista Ultimate 32-bit (x86) and 64-bit (x64) Edition.

ii. Compiler (Note that the selection of this compiler is for use by NIST in Rounds 1 and 2, and does not constitute a direct or implied endorsement by NIST.): the ANSI C compiler in the Microsoft Visual Studio 2005 Professional Edition.

At a minimum, NIST intends to perform an efficiency analysis on the reference platform; however, NIST invites the public to conduct similar tests and compare results on additional platforms (e.g., 8-bit processors, Digital Signal Processors, dedicated CMOS, etc.).

Note: any changes to the intended platform/compiler will be noted on <http://www.nist.gov/hash-competition>.

6.C Round 2 Technical Evaluation

At the end of the Round 1 technical evaluation and the Second SHA-3 Candidate Conference, NIST intends to narrow the field of candidate algorithms to approximately five candidates, in order to focus the remaining efforts of both NIST and the public. NIST intends to perform its own analysis of the submissions, and make that information publicly available. NIST's Round 2 analysis will, at a minimum, be performed as follows. Note: the same platform and compilers from Round 1 will be used for Round 2 unless indicated on <http://www.nist.gov/hash-competition>.

i. *Message digest sizes*: Round 2 testing by NIST will be performed on the required message digest sizes as specified in Section 3. Note: If the submitter chooses to submit updated optimized implementations prior to the beginning of Round 2, then some of the tests performed in Round 1 may be performed again using the new optimized implementations. This will be done to obtain updated measurements.

ii. *Efficiency testing*: Using the submitted optimized implementations, NIST intends to perform various computational efficiency tests for the minimum message digest sizes specified in Section 3, including the calculation of the time required to compute message digests for various length messages.

NIST welcomes comments regarding the efficiency of the candidate algorithms when implemented in hardware. NIST may specify the finalist algorithms using a Hardware Description Language, to compare the estimated hardware efficiency of the candidate algorithms.

NIST may perform efficiency testing using additional platforms. NIST welcomes public input regarding efficiency testing on additional platforms.

iii. *Other testing*: Other features of the candidate algorithms may be examined by NIST. If appropriate, analyses from the Second SHA-3 Candidate Conference and the public evaluation during Round 1 may warrant the testing of specific features.

7. Miscellaneous

This section is intended to address some of the questions/comments raised in the review of the draft evaluation criteria.

- When evaluating algorithms, NIST will make every effort to obtain public input and will encourage the review of the candidate algorithms by outside organizations; however, the final decision as to which algorithm(s) will be selected for SHA-3 is the responsibility of NIST.

- NIST intends to develop a validation program for hash algorithm conformance testing, with the goal of having testing available by the time SHA-3 is incorporated into the revised Secure Hash Standard.

- NIST does NOT have a fixed timetable for the completion of the hash function competition. NIST reserves the right to extend the length of the technical review period for each round. If necessary, NIST may also insert additional rounds of such technical evaluations.

- NIST does not intend to select a wholly distinct algorithm for each of the minimally required message digest sizes. It is strongly recommended that no submission be so constructed.

- NIST will not target a specific application or platform for implementing the candidate hash algorithms, as the evaluation of candidate algorithms takes place. One factor that will be taken into consideration for each candidate algorithm is its flexibility - the ability to implement the algorithm securely and efficiently on a wide variety of platforms and applications (see Section 4.C).

- Since SHA-3 is intended to augment the existing NIST-approved hash algorithm toolkit, which includes the SHA-2 family of hash functions, NIST does not intend to select an additional "backup" hash algorithm for SHA-3. If circumstances arise (e.g., a discovery of a significant security flaw) that could not be satisfactorily addressed by modifying the selected SHA-3 algorithm, NIST would likely consider the other finalist algorithms. If a significant period of time has elapsed since the hash algorithm selection, NIST would likely examine other algorithms that may have been developed in the intervening period.

- Exportability decisions regarding submissions and, eventually, products implementing the selected SHA-3 algorithm(s) will be made by the appropriate U.S. Government regulatory authorities. NIST is a non-regulatory agency of the U.S. Department of Commerce.

- If no appropriate algorithms are submitted in response to this call, NIST expressly reserves the right to cease this process and examine other possible courses of action.

- Submitters are strongly encouraged to submit only one algorithm each (presumably the one in which the submitter has the greatest confidence). The submission of similar, yet distinct, algorithms by the same submitter may delay the public evaluation process and may well raise public questions as to the submitter's level of confidence in his/her candidates.

- For conference and resource allocation planning purposes, it would be appreciated if those planning to submit candidates could notify the individuals listed in the **FOR FURTHER INFORMATION CONTACT** Section as soon as possible.

Appreciation

NIST extends its appreciation to all submitters and those providing public comments during the SHA-3 development process.

Dated: October 29, 2007.

Richard F. Kayser,

Acting Deputy Director, NIST.