Tentative Timeline for the Hash Algorithm Competition:

In response to a SHA-1 vulnerability announced in Feb. 2005, NIST held a Cryptographic Hash Workshop on Oct. 31-Nov. 1, 2005 to assess the status of its approved hash functions. While NIST continues to recommend a transition from SHA-1 to the approved SHA-2 family of hash functions (SHA-224, SHA-256, SHA-384, and SHA-512), NIST has also decided that it would be prudent in the long-term to develop one or more hash functions through a public competition, similar to the development process for the Advanced Encryption Standard (AES).

A tentative timeline for developing the new hash functions was presented, and discussed at length, at the Second Cryptographic Hash Workshop held on August 24-25, 2006 at UCSB. At the workshop, there seemed to be a pretty strong sense that, although the general theory and understanding of hash functions leaves a lot to be desired, and is not as good as our understanding of block ciphers when NIST started the AES competition, it's still better to get on with the competition, rather than to keep refining our understanding to identify the precise selection criteria for the competition. Based on this public feedback, NIST has decided to start the process sooner, and has adjusted the timeline accordingly.

The proposed timeline takes the following factors into consideration:

- The development process would be similar to that of the AES development (see Appendix A), although the hash function development timeline is subject to adjustment.

- As in the AES competition, NIST intends to schedule the hash function workshops in conjunction with other workshops and conferences, perhaps having back-to-back events to minimize travel by interested parties and to maximize attendance.

- FIPS 180-2 (the Secure Hash Standard) is scheduled for a review in 2007 and again in 2012. A reasonable goal is to complete the hash function competition process, and publish the augmented and revised Hash Function Standard by 2012.

The proposed timeline for the development of new hash functions is listed below, followed by the timeline of the AES development process for reference. As there are many uncertainties in the competition process of new hash functions, this timeline is tentative at best, and is subject to change at NIST's discretion. In essence, NIST does NOT have a fixed timetable for completion of the hash function competition. Comments about the proposed timeline should be sent to **hash-function@nist.gov.**

Tentative Timeline (Subject to Change) for the Development of New Hash Functions:

Note: The estimated milestones are by calendar year quarters, where:
1Q = January - March
2Q = April - June
3Q = July – September
4Q = October - December

- 8/2006 Second Cryptographic Hash Workshop: Assess current status, discuss hash function development strategy, and encourage further research.

- 4Q/2006 Draft the preliminary minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions.

Year 1 (2007):

- 1Q Publish the preliminary minimum acceptability requirements, submission requirements, and evaluation criteria for public comments.

  Present the draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions at the RSA Conference and at FSE 2007.

- 2Q Public comments period ends on 4/27/2007. Resolve comments.

- 4Q Finalize and publish the minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions.

  Request submissions for new hash functions.

Year 2 (2008):

- 4Q Submission deadline for new hash functions.

Year 3 (2009):

- 2Q Review submitted functions, and select candidates that meet basic submission requirements.

  Host the First Hash Function Candidate Conference to announce first round candidates. Submitters present their functions at the workshop.

  Call for public comments on the first round candidates.

Year 4 (2010):

- 2Q Public comment period ends.

  Note: Depending on the number and quality of the submissions, NIST may either extend the length of the initial public comment period to allow sufficient time for the public analysis of the candidate algorithms, or may include additional rounds of analysis in order to successively reduce the number of candidate algorithms for further consideration as finalist algorithms. In these cases, NIST may host multiple workshops to discuss analysis results on candidate algorithms until it is ready to select the finalists.

  Note that subsequent dates in the timeline assume that the initial comment period will not be extended or additional rounds will not be required.

- 2Q Hold the Second Hash Function Candidate Conference. Discuss the analysis results on the submitted candidates. Submitters may identify possible improvements for their algorithms.

- 3Q Address the public comments on the submitted candidates; select the finalists. Prepare a report to explain the selection.

  Announce the finalists. Publish the selection report.

- 4Q Submitters of the finalist candidates announce any tweaks to their submissions.

  Final round begins.

Year 5 (2011):

- 4Q Public comment period for the final round ends.

Year 6 (2012):

- 1Q Host the Final Hash Function Candidate Conference. Submitters of the finalist algorithms discuss the comments on their submissions.

- 2Q Address public comments, and select the winner. Prepare a report to describe the final selection(s).

  Announce the new hash function(s).

- 3Q Draft the revised hash standard.

  Publish the draft standard for public comments.

- 4Q Public comment period ends. Address public comments.

  Send the proposed standard to the Secretary of Commerce for signature.

Appendix A. AES Development Timeline

01/02/1997	Published draft minimum acceptability requirements, evaluation criteria, and submission requirements for public comments. Announced a public workshop to address these requirements.
04/02/1997	Public comment period ended.
04/15/1997	AES Evaluation Criteria/Submission Requirements Workshop. Discussed the draft minimum acceptability requirements, evaluation criteria, and submission requirements.
09/12/1997	Called for new algorithms.
	[NIST reviewed the algorithms and selected the first round winners – 15 algorithms]
08/20-22/1998	First AES Candidate Conference (AES1), Ventura, California Kicked off Round 1 of the AES Development Effort. Announced 15 candidates.
09/14/1998	Called for public comments on the 15 candidates.
03/22-23/1999	Second AES Candidate Conference (AES2), Rome. Discussed analysis results on the 15 candidate algorithms.
04/15/1999	Public comment period ended.
08/09/1999	Announced 5 finalists; Round 1 Report described the selection of the finalists.
xx/xx/xxxx	Set up discussion forum to discuss the 5 candidate algorithms.
04/13-14/2000	Third AES Candidate Conference (AES3), NYC. Submitters of the 5 finalists discussed comments on their algorithms.
05/15/2000	Public comment period ended on the 5 finalists.
10/02/2000	Announced the AES.
02/xx/2001	Draft FIPS-197 announced for public comments.
11/26/2001	FIPS-197 published.