Title of Panel: AES and Beyond

Panel Chair: Elaine Barker, NIST
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Phone: 301-975-2911
Fax: 301-948-1233
Email: ebarker@nist.gov

Panelists: 1. Jim Foti, NIST
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Phone: 301-975-5237
Fax: 301-948-1233
Email: James.Foti@nist.gov

2. Submitter of the selected AES algorithm, TBD

3. Bill, Burr, NIST
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Phone: 301-975-2914
Fax: 301-948-1233
Email: William.Burr@nist.gov

4. Member of user organization, TBD (possibly IETF)

Session Abstract: The end of the AES development process is now in sight. The algorithm has been selected, and the draft standard is ready for public comment. After nearly four years of intensive effort, what has been accomplished? What has been learned? What would we do differently? What are the next steps in making AES the international standard that was intended?

And - what lies beyond AES? NIST is in the process of initiating a number of other cryptographic activities, including a standard specifying modes of operation for symmetric key block ciphers (e.g., AES), an HMAC standard, a key management standard, a new and enlarged hash function that is consistent with the AES key sizes, and an increase in key sizes for the Digital Signature Algorithm (DSA).

Summary of panelist topics:
Jim Foti – Mr. Foti will discuss his perceptions of the AES process and its results. Subjects to be addressed include: What has been accomplished? What has been learned? What would we do differently? What are the next steps in making AES the international standard that was intended?

Submitter of the selected AES algorithm - The exact content of this presentation can only be assumed at this point, but it should probably be a discussion of: why they decided to submit an algorithm, how they went about development of the algorithm, and where they go from here.

Bill Burr – Mr. Burr will discuss other cryptographic efforts under way at NIST, providing our timelines and methods of proceeding with these efforts.

Member of a user organization - The exact content of this presentation can only be assumed at this point, but it should probably be a discussion of: How the organization plans to use the results of NIST's cryptographic standards (e.g., AES), what effect they will have on the community, and when the cryptography will be available.

Audience Background: Representatives from government, industry, academia and standards organizations who are interested in cryptographic security mechanisms.

Biographies:

Elaine Barker has been involved in cryptographic activities for over 30 years, the last 17 at NIST. While at NIST, she has been involved with the development of a number of Federal Information Processing Standards (FIPS) and American National Standards Institute (ANSI) standards, including AES, HMAC, Password Usage, Data Authentication, FIPS 140-1 (Cryptographic Modules), Key Management , Digital Signature Algorithm, Secure Hash Algorithm, Triple DES, ECDSA, and Certificate Management. Ms. Barker is currently the manager of the cryptographic standards program at NIST.

Jim Foti is a member of NIST's Computer Security Division. Since joining NIST in 1992, Jim has worked specifically in the area of Cryptographic Standards and Guidance. This has included providing support for the FIPS 140-1 Cryptographic Module Validation Program and the Advanced Encryption Standard development effort.

Bill Burr is the acting manager of the Security Technology Group at the National Institute of Standards and Technology and chairman of the Federal PKI Technical Working group. Bill has had a 25 year career at NIST in Information Technology Standards, was the Chairman of the SCSI interface standards committee in the 1980s and has been working on PKI issues for about five years.