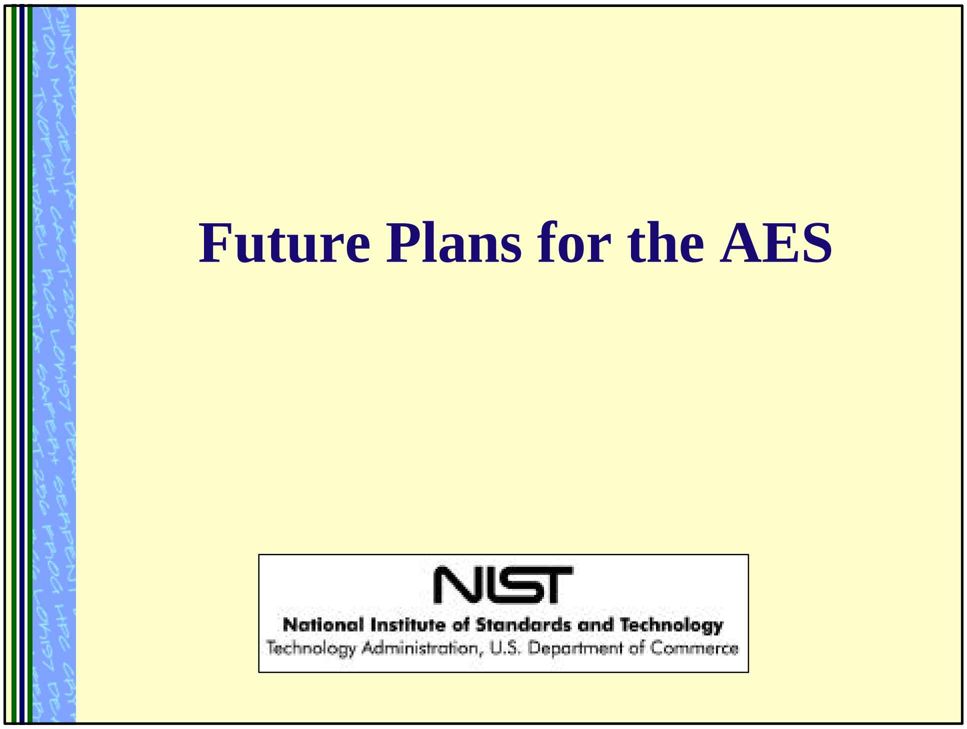
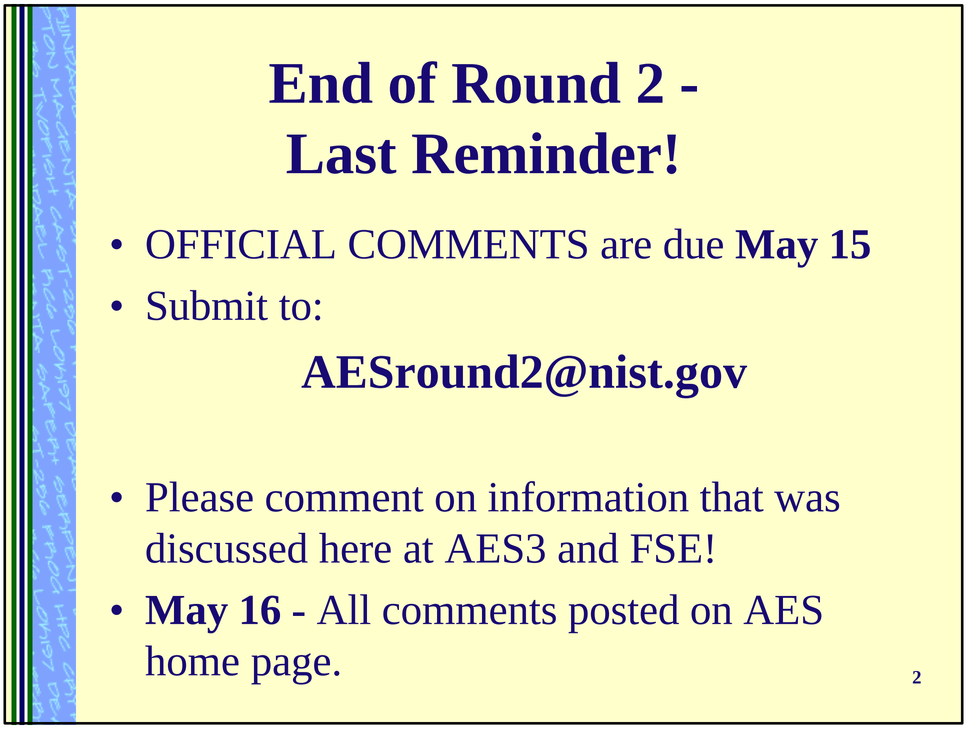


Future Plans for the AES

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

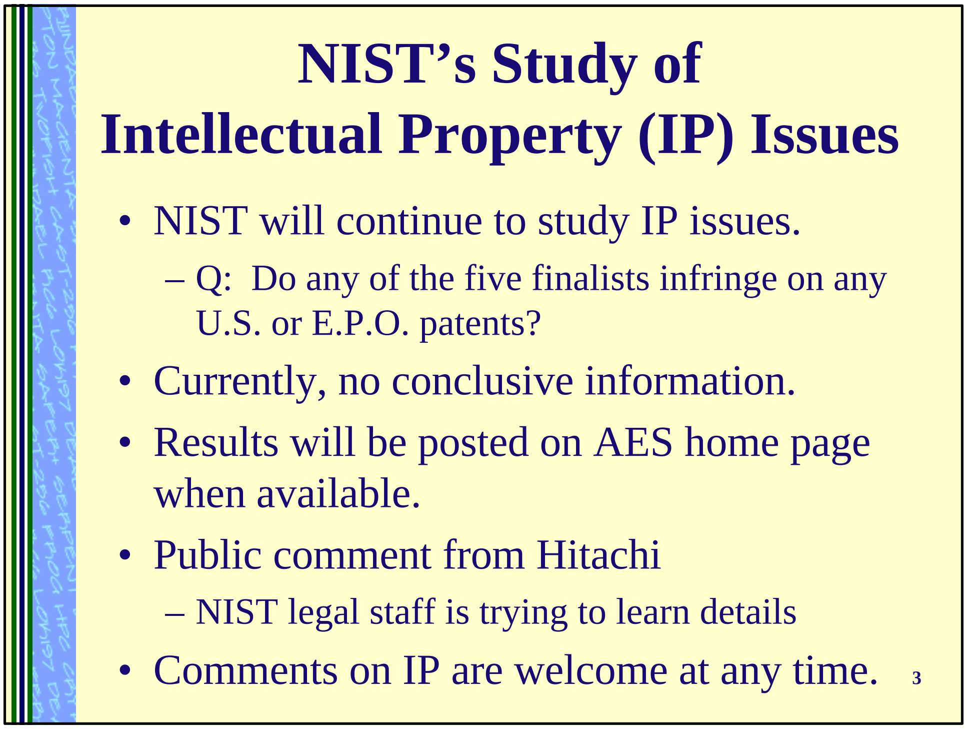


End of Round 2 - Last Reminder!

- OFFICIAL COMMENTS are due **May 15**
- Submit to:

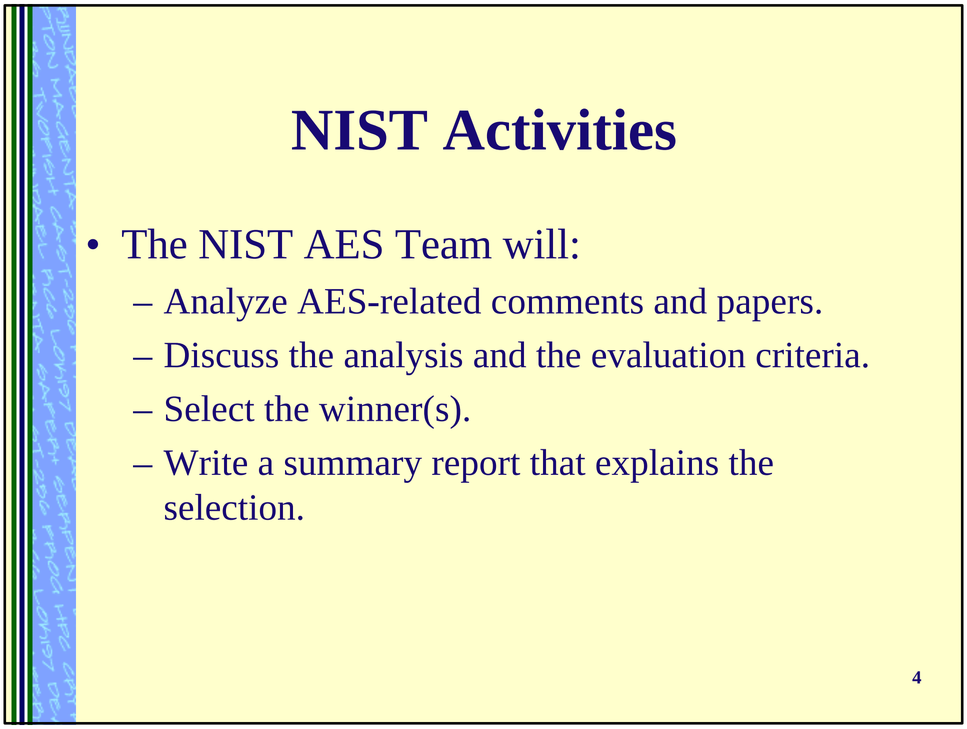
AESround2@nist.gov

- Please comment on information that was discussed here at AES3 and FSE!
- **May 16 -** All comments posted on AES home page.



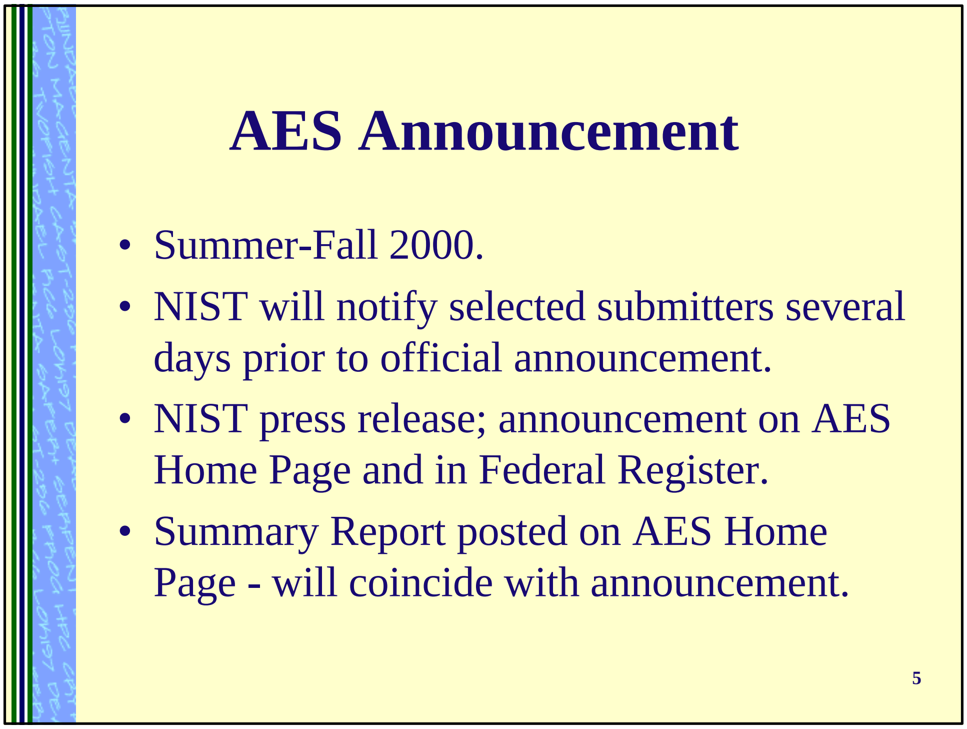
NIST's Study of Intellectual Property (IP) Issues

- NIST will continue to study IP issues.
  - Q: Do any of the five finalists infringe on any U.S. or E.P.O. patents?
- Currently, no conclusive information.
- Results will be posted on AES home page when available.
- Public comment from Hitachi
  - NIST legal staff is trying to learn details
- Comments on IP are welcome at any time.



NIST Activities

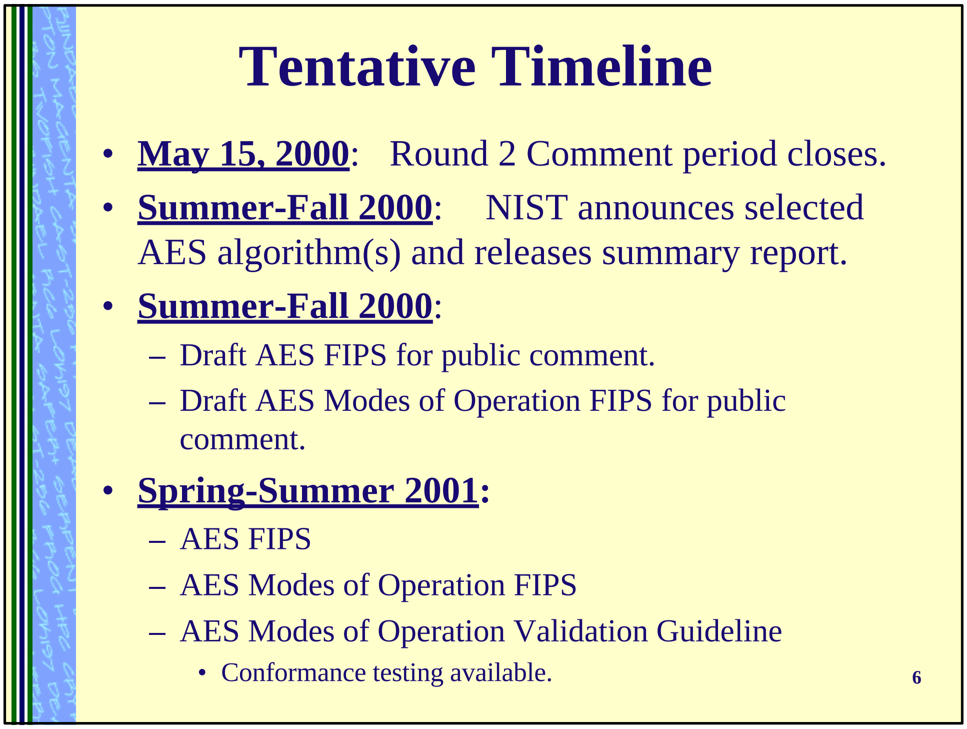
- The NIST AES Team will:
  - Analyze AES-related comments and papers.
  - Discuss the analysis and the evaluation criteria.
  - Select the winner(s).
  - Write a summary report that explains the selection.



AES Announcement

- Summer-Fall 2000.
- NIST will notify selected submitters several days prior to official announcement.
- NIST press release; announcement on AES Home Page and in Federal Register.
- Summary Report posted on AES Home Page - will coincide with announcement.

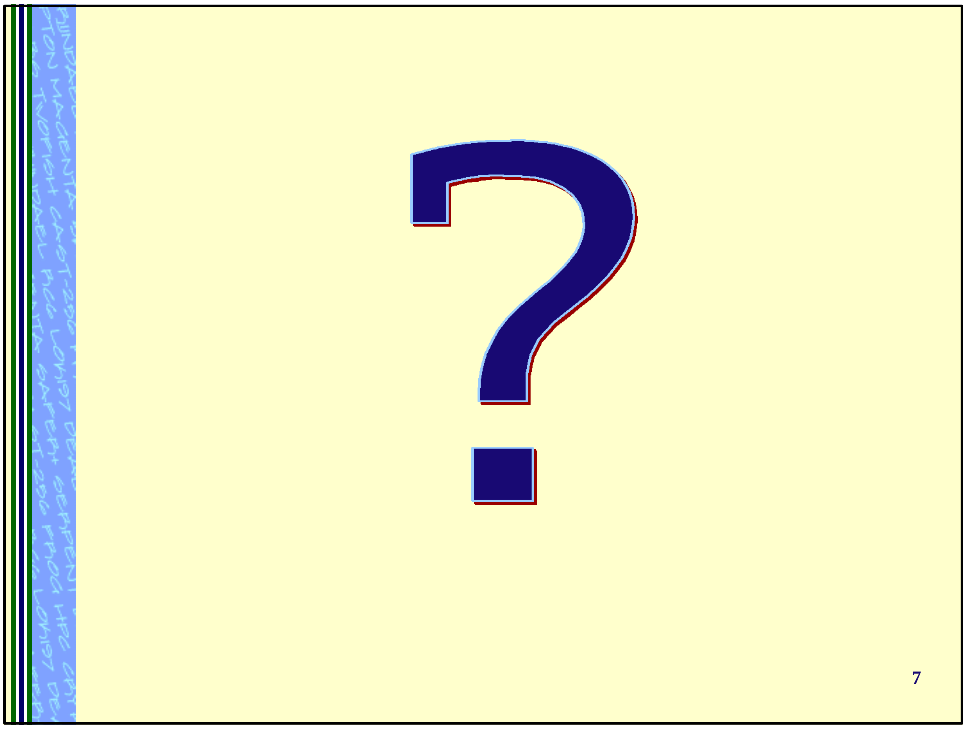
5



Tentative Timeline

- **<u>May 15, 2000</u>**: Round 2 Comment period closes.
- **<u>Summer-Fall 2000</u>**: NIST announces selected AES algorithm(s) and releases summary report.
- **<u>Summer-Fall 2000</u>**:
  - Draft AES FIPS for public comment.
  - Draft AES Modes of Operation FIPS for public comment.
- **<u>Spring-Summer 2001</u>:**
  - AES FIPS
  - AES Modes of Operation FIPS
  - AES Modes of Operation Validation Guideline
    - Conformance testing available.

6



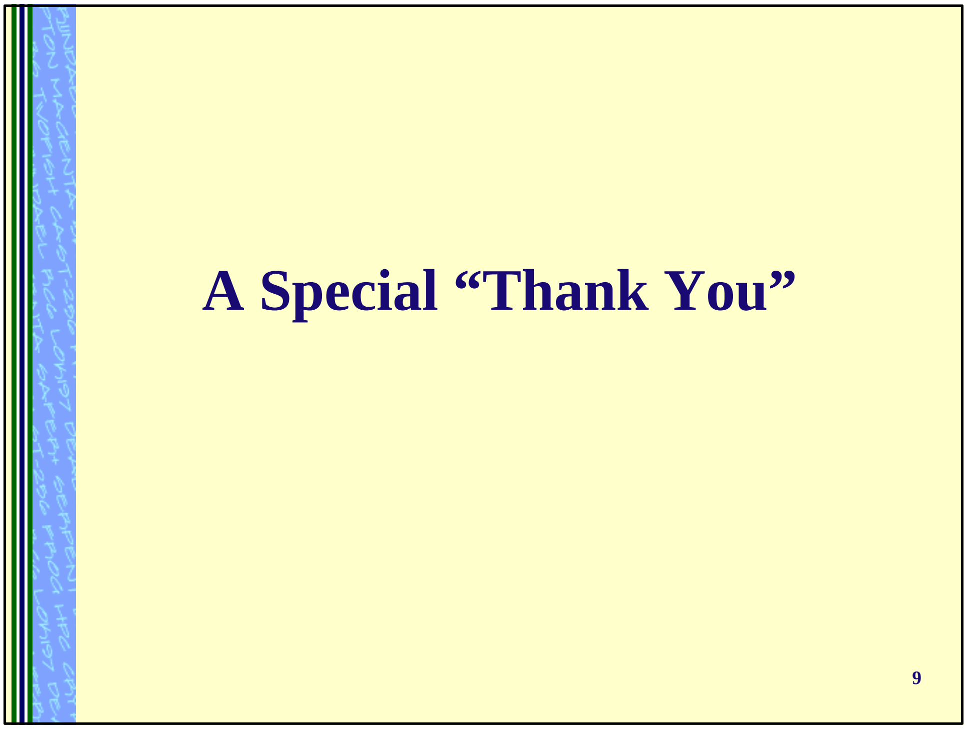
?

7

Thanks!

- Speakers
- Program Committee
- Algorithm Submitters
- FSE Committee
- NIST Staff & Hotel Staff
- Attendees

8



A Special “Thank You”