conducted extensive studies of patent-related activity and the operation of the patent system, and issued reports including recommendations for reform. *See* Stephen A. Merrill, Richard C. Levin & Mark B. Myers, A Patent System for the 21st Century (2004); Federal Trade Commission, To Promote Innovation: The Proper Balance of Competition and Patent Law and Policy (Oct. 2003).

1. Do the reports fully capture the role of patents and developments in patent-related activity (*e.g.,* applications, grants, licensing, and litigation) over the past 25 years?

2. Are the concerns or problems regarding the operation of the patent system identified in the two reports well-founded?

3. Which, if any, of the recommendations for changes to the patent system made in those two reports should be adopted?

4. Are there other issues regarding the operation of the patent system not addressed in either report that should be considered by the Antitrust Modernization Commission? Please be specific in identifying any issue and the reasons for its importance.

IX. Regulated Industries

1. What role, if any, should antitrust enforcement play in regulated industries, particularly industries in transition to deregulation? How should authority be allocated between antitrust enforcers and regulatory agencies to best promote consumer welfare in regulated industries?

2. How, if at all, should antitrust enforcement take into account regulatory systems affecting important competitive aspects of an industry? How, if at all, should regulatory agencies take into account the availability of antitrust remedies?

3. What is the appropriate standard for determining the extent to which the antitrust laws apply to regulated industries where the regulatory structure contains no specific antitrust exemption? For example, in what circumstances should antitrust immunity be implied as a result of a regulatory structure?

4. How should courts treat antitrust claims where the relevant conduct is subject to regulation, but the regulatory legislation contains a ''savings clause'' providing that the antitrust laws continue to apply to the conduct?

5. Should Congress and regulatory agencies set industry-specific standards for particular antitrust violations that may conflict with general standards for the same violations?

6. When a merger or acquisition involves one or more firms in a regulated industry, how should authority for merger review be allocated between the antitrust agencies (DOJ and FTC) and the relevant regulatory agency?

a. Are there additional costs and delay when two agencies (one antitrust, one regulatory) both analyze the antitrust effects of the same merger? Are there benefits to such dual review?

b. Should regulatory agencies defer to antitrust analysis by the antitrust agencies, or should both the antitrust and regulatory agencies conduct separate antitrust analyses in performing merger reviews? Should the antitrust agencies have primary responsibility or simply an advisory role with respect to antitrust analysis in merger review?

In your response, please refer specifically to the following contexts:

i. Mergers or acquisitions involving financial institutions. *See* 12 U.S.C. 1467a, 1828, 1842.

ii. Mergers or acquisitions involving certain media companies (*e.g.,* radio or television broadcasters, satellite, and cable companies) and common carriers. *See* 47 U.S.C. 214, 310.

iii. Mergers or acquisitions of rail carriers subject to approval by the Surface Transportation Board. *See* 49 U.S.C. 11321, 11323–24.

iv. Mergers or acquisitions involving motor carriers of passengers. *See* 49 U.S.C. 14303.

v. Pooling agreements among certain motor carriers. *See* 49 U.S.C. 14302.

vi. Certain agreements involving domestic and foreign airlines. *See* 49 U.S.C. 41308–09. vii. Acquisitions of assets of natural gas companies. *See* 15 U.S.C. 717f.

viii. Mergers or acquisitions of electric power companies. *See* 16 U.S.C. 824b.

ix. License applications subject to the approval of the U.S. Nuclear Regulatory Commission. *See* 42 U.S.C. 2135.

x. Issuance of federal coal leases. *See* 30 U.S.C. 184(l).

xi. Issuance or transfer of licenses for exploration of hard minerals in deep seabed sites. *See* 30 U.S.C. 1413(d).

xii. Issuance of oil and gas leases on submerged lands of the Outer Continental Shelf. *See* 43 U.S.C. 1337(c).

Dated: May 16, 2005.

By direction of the Antitrust Modernization Commission.

Andrew J. Heimert,

Executive Director & General Counsel, Antitrust Modernization Commission.

[FR Doc. 05–10025 Filed 5–18–05; 8:45 am]

BILLING CODE 6820–YM–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 040602169–5002–02]

Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: The Secretary of Commerce has approved the withdrawal of FIPS 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation. These FIPS are withdrawn because FIPS 46–3, DES, no longer provides the security that is needed to protect Federal government information. FIPS 74 and 81 are associated standards that provide for the implementation and operation of the DES. Federal government organizations are now encouraged to use FIPS 197, Advanced Encryption Standard (AES), which was approved for Federal government use in November 2001. FIPS 197 specifies a faster and stronger algorithm than the DES for encryption. For some applications, Federal government departments and agencies may use the Triple Data Encryption Algorithm to provide cryptographic protection for their information. This algorithm and its uses have been specified in NIST Special Publication 800–67, Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher, issued in May 2004. FIPS 197 and SP 800–67 are available on NIST's Web pages. The content of these withdrawn standards will remain available at *http://csrc.nist.gov/publications/fips/index.html* as reference documents and these three FIPS will be listed as withdrawn, rather than current FIPS.

DATES: These standards are withdrawn as of May 19, 2005.

FOR FURTHER INFORMATION CONTACT: Mr. William Barker (301) 975–8443, *wbarker@nist.gov,* National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

SUPPLEMENTARY INFORMATION: In July 2004, a notice was published in the **Federal Register** proposing the withdrawal of FIPS 46–3, DES; FIPS 74,

Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation. The **Federal Register** notice solicited comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. In addition to being published in the **Federal Register**, the notice was posted on the NIST Web site.

Comments and questions were received from thirteen private sector organizations or individuals, and two federal government organizations. Seven of the submitted comments supported the withdrawal of the DES. Five comments recognized the inadequacy of the DES and did not oppose the withdrawal, but raised transition issues or suggested that NIST keep the specifications available for private sector organizations that wish to use them or make provisions for continued use of the DES. One industry organization and two individuals opposed the withdrawal of the DES, citing the large investments made in DES technology by their organizations and others.

Following is an analysis of the comments dealing with technical and transition issues.

Comment: NIST should consider allowing the continued use of DES implementations that only decrypt data, enabling agencies to recover the data that they have already encrypted using the DES.

Response: NIST guidance contained in draft Special Publication 800–57, Recommendation for Key Management, Part 1 General Guideline, covers this situation. SP 800–57 expands on guidance issued in Special Publication 800–21, Guideline for Implementing Cryptography in the Federal Government, and recommends that agencies re-encrypt information that had been encrypted using an algorithm and key size that no longer provide adequate protection. Thus, Federal government information that has been encrypted with the DES should be re-encrypted using a FIPS-approved algorithm and an appropriate key size that agencies determine will provide adequate security for the information for the remainder of its life.

Comment: NIST should note certain limits that might be reached when using two-key Triple DES. The recommended safe default when using two-key Triple-DES is to re-key before encrypting 2^{40} blocks.

Response: These specific applications and requirements are outside the scope of the recommended action to withdraw FIPS 46–3 and two associated standards.

Comment: NIST should retain the availability of the technique in FIPS 74 that specifies the encryption of numeric data into numeric data. This technique is used to protect customer data that a bank might share with a telemarketing firm.

Response: NIST will place FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, on NIST's Web page at *http://www.itl.nist.gov/fipspubs/* under Withdrawn FIPS. The standard will be marked as inadequate for the protection of Federal government information.

Comment: NIST should provide a timetable and a transition strategy for the discontinuation of the use of DES implementations. NIST should clarify the transition from the use of applied and embedded DES products.

Response: A proposed transition strategy for validating algorithms and cryptographic modules has been posted for public comment on NIST's Web page at *http://csrc.nist.gov/cryptval/* under ''Notices.'' The transition plan addresses the use by Federal agencies of DES implementations, which are incorporated in cryptographic modules, and which have been validated under the Cryptographic Module Validation Program. The transition plan allows Federal agencies and vendors to make a smooth transition to stronger cryptographic algorithms such as AES or Triple-DES.

Comment: The DES should be retained because it is widely used in the market.

Response: NIST believes that the DES no longer provides adequate protection for Federal government information, and therefore recommends withdrawal of FIPS 46–3 and associated standards. When FIPS 46–3 was reaffirmed in 1999, the standard stated that NIST could no longer support the use of single DES for many applications, and that agencies with legacy single DES systems should start the transition to Triple DES. The specifications for the standards that have been withdrawn will be placed on NIST's Web page at *http://www.itl.nist.gov/fipspubs/* under Withdrawn FIPS. All of the withdrawn standards will be marked as inadequate for the protection of Federal government information, but will be available to private sector organizations that wish to use them.

Comment: FIPS 46–3 and associated standards are used in the commercial world and serve important functions, including use by the entertainment industry for real-time broadcast security, to prevent unrestricted copying of files, and for the security of digital television signals. The standards should be reaffirmed for use by non-government organizations or made available in electronic form to non-government organizations that wish to use them.

Response: The specifications for FIPS 46–3 (DES) and the associated standards will be placed on NIST's Web page at *http://www.itl.nist.gov/fipspubs/* under Withdrawn FIPS. All of the withdrawn standards will be marked as inadequate for the protection of Federal government information, but will be available to private sector organizations that wish to use them.

Comment: NIST should issue the Triple-DES as a FIPS and encourage implementers to use both the TDES and the Advanced Encryption Standard in their products.

Response: Although both AES and three-key TDES are considered adequate for the protection of Federal government information for many years, TDES is less efficient and is slightly less secure than AES. In order to encourage the use of AES over TDES, AES has been published as a Standard (FIPS 197), whereas TDES was published as a NIST Recommendation (Special Publication 800–67).

Therefore, as of the date of this **Federal Register** notice, FIPS 46–3, Data Encryption Standard is withdrawn as it no longer provides the security that is needed to protect Federal government information. FIPS 74, Guidelines for Implementing and Using the NBS Encryption Standard and FIPS 81, DES Modes of Operation, are also withdrawn, as they are associated standards that provide for the implementation and operation of the DES.

Authority: Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 and the Federal Information Security Management Act of 2002, Public Law 107–347.

E.O. 12866: This notice has been determined to be significant for the purposes of E. O. 12866.

Dated: May 12, 2005.

Hratch G. Semerjian,

Acting Director, NIST.

[FR Doc. 05–9945 Filed 5–18–05; 8:45 am]

BILLING CODE 3510–CN–P