Constitution, NW., Washington, DC 20230 or via internet at *MClayton@doc.gov.*

Written comments and recommendations for the proposed information collection should be sent to David Rostker, OMB Desk Officer, Room 10202, New Executive Office Building, Washington, DC 20503 within 30 days of the publication of this notice in the **Federal Register**.

Dated: August 20, 2002.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Office of the Chief Information Officer

[FR Doc. 02–21602 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

Minority Business Development Agency

Online Performance Data Base

ACTION: Proposed collection; comment request.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites other Federal agencies and the general public to take this opportunity to comment on proposed or continuing information collections, as required by the Paperwork Reduction Act of 1995, Pub. L. 104–13 (44 U.S.C. 3506(c)(2)(A)).

DATES: Written comments must be submitted on or before October 25, 2002.

ADDRESSES: Direct all written comments to Madeleine Clayton, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6608, 14th and Constitution Avenue, NW., Washington, DC 20230 or via internet at *Mclayton@doc.gov.*

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Juanita E. Berry, Department of Commerce, Minority Business Development Agency (MBDA), Room 5079, 14th and Constitution Avenue, NW., Washington, DC 20230, or call (202) 482–3262.

SUPPLEMENTARY INFORMATION:

I. Abstract

The Performance Database identifies minority business clients receiving Agency-sponsored business development services in the form of management and technical assistance, the kind of assistance each receives, and the impact of that assistance on the growth and profitability of the client firms. MBDA requires this information to monitor, evaluate, and plan Agency programs which effectively enhance the development of the minority business sector.

II. Method of Collection

Electronic transfer of performance data.

III. Data

OMB Number: 0640–0002.

Agency Form Number: N/A.

Type of Review: Extension of a currently approved collection.

Affected Public: State or local governments, individuals, and profit and non-profit institutions.

Estimated Number of Responses: 240 (approximately 50 respondents with numerous responses).

Estimated Time Per Response: 3–15 minutes per function, as needed (5 functions).

Estimated Total Annual Burden Hours: 4,818.

Estimated Total Annual Cost: $0 (software package is provided by MBDA).

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they will also become a matter of pubic record.

Dated: August 20, 2002.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Electronic Government Division, Office of the Chief Information Officer.

[FR Doc. 02–21601 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–21–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 001214352–2097–02]

Announcing Approval of Federal Information Processing Standard (FIPS) 180–2, Secure Hash Standard; a Revision of FIPS 180–1

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce has approved FIPS 180–2, Secure Hash Standard, and has determined that the standard is compulsory and binding on Federal agencies for the protection of sensitive, unclassified information.

FIPS 180–2, Secure Hash Standard, replaces FIPS 180–1, which was issued in 1992 and which specified an algorithm (SHA–1) for producing a 160-bit output called a message digest. The message digest is a condensed representation of electronic data and is used in cryptographic processes such as digital signatures and message authentication. FIPS 180–2 includes three additional algorithms, which produce 256-bit, 384-bit, and 512-bit message digests. These expanded capabilities are compatible with and support the strengthened security requirements of FIPS 197, Advanced Encryption Standard.

EFFECTIVE DATE: This standard is effective February 1, 2003.

Specifications: FIPS 180–2 is available on the NIST web page at: *http://csrc.nist.gov/encryption/tkhash.html.*

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, Maryland 20899–8930. Email: *elaine.barker@nist.gov.*

SUPPLEMENTARY INFORMATION: A notice was published in the **Federal Register** (66 FR 29287) on May 30, 2001, announcing the proposed FIPS 180–2, Secure Hash Standard, for public review and comment. 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 pages; information was provided about the submission of electronic comments. Comments and responses were received from three private sector organizations

or individuals, and from one federal government organization.

The comments raised technical issues related to the standard, asked for clarification of technical issues, and recommended editorial changes. None of the comments opposed the adoption of the revised Federal Information Processing Standard. All of the editorial and related comments were carefully reviewed, and changes were made to the standard where appropriate. NIST recommended that the Secretary approve FIPS 180–2. Following is an analysis of the comments received.

Comment: NIST should provide a security evaluation of the algorithms added to FIPS 180–2, and give the rationale for the various design choices. Such an analysis would increase confidence in the algorithms and facilitate external evaluation.

Response: The standard provides four secure hash algorithms, which differ in the number of bits of security provided for the data being processed. Secure hash algorithms are designed for use in conjunction with another algorithm, which may have requirements that the hash algorithm have a certain number of bits of security. For example, a digital signature algorithm that provides 128 bits of security may require that the secure hash algorithm also provide 128 bits of security.

NIST believes that these algorithms are secure because it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. It is highly probable that a change to a message will result in a different message digest.

FIPS 180–2 includes the technical specifications for the four algorithms that have been selected to provide 160, 256, 384 and 512 bits of security. NIST anticipates and invites external examination and scrutiny concerning the security of the algorithms.

Comment: NIST should include a note in the standard indicating whether SHA–256 could be truncated to 160 bits for use as an alternative to SHA–1 (also 160 bits).

Response: The use of hash functions will be addressed in application standards (*e.g.*, in the upcoming revision of Federal Information Processing Standard 186–2, the Digital Signature Standard).

Comment: NIST should mention in the standard that SHA–256 constants are easily extracted from the SHA–512 constants.

Response: NIST believes that the decisions concerning the use of constants and how to extract them should be made by those organizations that develop implementations of the standard.

Comment: One comment suggested that there may be weaknesses in the algorithms, and proposed a method to change the standard to address the perceived weaknesses.

Response: It would be more appropriate for the perceived weaknesses to be addressed in application standards such as the Federal Information Processing Standard for the Keyed-Hash Message Authentication Code (HMAC), which has been approved as FIPS 198, as opposed to addressing this in FIPS 180–2 itself. Furthermore, NIST expects to issue guidance on the implementation of secure hash functions.

Authority: Under section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems.

Executive Order 12866: This notice has been determined not to be significant for purposes of E.O. 12866.

Dated: August 19, 2002.

Karen Brown,

Deputy Director, NIST.

[FR Doc. 02–21599 Filed 8–23–02; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[Docket Number: 020729185–2185–01]

Announcement of Graduate Research Fellowships in the National Estuarine Research Reserve System for Fiscal Year 2003

AGENCY: Estuarine Reserves Division (ERD), Office of Ocean and Coastal Resource Management (OCRM), National Ocean Service (NOS), National Oceanic and Atmospheric Administration (NOAA), Department of Commerce (DOC).

ACTION: Notice.

SUMMARY: The Estuarine Reserves Division of OCRM is soliciting applications for graduate fellowship funding within the National Estuarine Research Reserve System. This notice sets forth funding priorities, selection criteria, and application procedures.

The National Estuarine Research Reserve System of NOAA announces the availability of graduate research fellowships. The Estuarine Reserves Division anticipates that 27 Graduate Research Fellowships will be competitively awarded to qualified graduate students whose research occurs within the boundaries of at least one reserve. Minority students are encouraged to apply. The amount of the fellowship is $17,500; at least 30% of total project cost match is required by the applicant. Applicants may apply for between one and three years of funding. Fellowships will start June 1, 2003. A later start date may be requested with justification and will be reviewed by ERD for approval.

DATES: Applications must be postmarked no later than November 1, 2002. Notification regarding the awarding of fellowships will be issued on or about March 1, 2003.

ADDRESSES: Erica Seiden, program coordinator, NOAA/Estuarine Reserves Division, 1305 East-West Highway, N/ORM5, SSMC4, 11616 Floor, Silver Spring, MD 20910, Attn: NERRS GRF. Phone: 301–713–3155 ext. 172 Fax: 301–713–4363, internet: *erica.seiden@noaa.gov.* Web page: *http://www.ocrm.nos.noaa.gov/nerr/fellow.html.* See Appendix I for National Estuarine Research Reserve addresses.

FOR FURTHER INFORMATION CONTACT: For further information on specific research opportunities at National Estuarine Research Reserves, contact the site staff listed in Appendix I or the program specialist listed in the Addresses section above. For application information, contact Erica Seiden of ERD (see contact information above).

SUPPLEMENTARY INFORMATION:

I. Authority and Background

Section 315 of the Coastal Zone Management Act of 1972, as amended (CZMA), 16 U.S.C. 1461, establishes the National Estuarine Research Reserve System (NERRS). 16 U.S.C. 1461 (e)(1)(B) authorizes the Secretary of Commerce to make grants to any coastal state or public or private person for purposes of supporting research and monitoring within a National Estuarine Research Reserve that are consistent with the research guidelines developed under subsection (c). This program is listed in the Catalog of Federal Domestic Assistance (CFDA) under ''Coastal Zone Management Estuarine Research Reserves,'' Number 11.420.

II. Information on the National Estuarine Research Reserve System

The National Estuarine Research Reserve System consists of estuarine areas of the United States and its territories which are designated and