

Technology Management Reform Act of 1996, OMB Circular A-130, and Executive Order 13011.

Dated: May 6, 1997.

Elaine Bunten-Mines,

Director, Program Office.

[FR Doc. 97-12341 Filed 5-12-97; 8:45 am]

BILLING CODE 3510-CN-M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 960924271-6271-01]

RIN 0693-ZA10

Announcing Plans to Develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange

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

ACTION: Notice; request for comments.

SUMMARY: NIST is planning to develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange. This notice solicits comments regarding techniques for consideration specifically including RSA, Diffie-Hellman, and Elliptic Curve techniques. This standard will be for use in designing and implementing public-key based key agreement and exchange systems which Federal departments and agencies operate or which are operated for them under contract. More than one algorithm may be specified, consistent with sound security practices, to enable Federal departments and agencies enhanced flexibility in the design, implementation, and use of cryptographic systems.

DATES: Comments should be received on or before August 11, 1997.

ADDRESSES: Written comments should be sent to: Director, Information Technology Laboratory, ATTN: Key Agreement/Exchange FIPS, Technology Building, Room A231, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Electronic comments should be sent to: KEYEX@NIST.GOV

Comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Reference and Records Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Miles Smid, Manager, Security

Technology Group, Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone (301) 975-2938.

SUPPLEMENTARY INFORMATION: NIST is planning to develop a Federal Information Processing Standard for Public-Key Based Cryptographic Key Agreement and Exchange. This standard will be for use in designing and implementing public-key based key agreement and exchange systems which Federal departments and agencies operate or which are operated for them under contract. More than one algorithm may be specified in the standard, consistent with sound security practices, to enable Federal departments and agencies enhanced flexibility in the design, implementation, and use of cryptographic systems.

Algorithms approved for inclusion shall be either: (1) Freely available or (2) available under terms consistent with the American National Standards Institute (ANSI) patent policy.

The Administration policy is that cryptographic keys used by Federal agencies for encryption (i.e., to protect the confidentiality of information) shall be recoverable through an agency or third-party process and that keys used for digital signature (i.e., for integrity and authentication of information) shall not be recoverable. Agencies must be able to ensure that signature keys cannot be used for encryption. Any algorithms proposed for digital signature must be able to be implemented such that they do not support encryption unless keys used for encryption are distinct from those used for signature and are recoverable.

The distinction between signature and encryption keys will be facilitated in the public key infrastructure by using X.509v3 public key certificates.

This standard would specify the mathematical algorithm(s) approved for use by Federal agencies for using public key cryptographic key exchange/agreement (e.g., to exchange the encryption key[s] used by two parties for data encryption). This standard will be complemented by the activities of the "Technical Advisory Committee to Develop a Federal Information Processing Standard for Federal Key Management Infrastructure," which is working on recommendations for a federal standard on encryption key recovery (independent of the underlying mathematical algorithm[s] used to exchange the encryption key[s]).

NIST solicits comments from interested parties, including industry, voluntary standards organizations, the public, and State and local governments concerning developing such a standard, and concerning the availability,

security, and adequacy of existing standards for public key-based key agreement and exchange.

Comments are particularly sought with respect to the RSA, Diffie-Hellman, and elliptic curve techniques. In addition, parties believing their patents or other intellectual property pertain to any of these three techniques are asked to comment and provide specifics of the nature of their claims.

This work is pursuant to NIST's responsibilities under the Computer Security Act of 1987, the Information Technology Management Reform Act of 1996, OMB Circular A-130, and Executive Order 13011.

Dated: May 6, 1997.

Elaine Bunten-Mines,

Director, Program Office.

[FR Doc. 97-12340 Filed 5-12-97; 8:45 am]

BILLING CODE 3510-CN-M

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

Foster Grandparent and Senior Companion Programs; Income Eligibility Levels

AGENCY: Corporation for National and Community Service.

ACTION: Revision of income eligibility levels.

SUMMARY: This Notice revises the schedules of income eligibility levels for participation in the Foster Grandparent Program (FGP) and the Senior Companion Program (SCP) of the Corporation for National and Community Service (Corporation) published in 61 FR 14558 on April 2, 1996.

DATES: These guidelines go into effect May 13, 1997.

FOR FURTHER INFORMATION CONTACT: Ruth Archie, National Senior Service Corps, Corporation for National and Community Service, 1201 New York Avenue NW, Washington, DC 20525, or by telephone at (202) 606-5000 ext. 289.

SUPPLEMENTARY INFORMATION: The revised schedules are based on changes in the Poverty Guidelines issued by the Department of Health and Human Services (DHHS) published in 62 FR 10856, March 10, 1997. In accordance with program regulations, the income eligibility level for each State and the District of Columbia is 125 percent of the DHHS Poverty Guidelines, except in those areas determined by the Corporation to be of a higher cost of living. In such instances, the income