

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

Dated: May 6, 1997.

**Elaine Buntin-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 Buntin-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

eligibility levels shall be 135 percent of the DHHS Poverty Guidelines. The level of eligibility is rounded to the next highest multiple of \$5.00.

In determining income eligibility, consideration should be given to the following definitions set forth in 59 FR 15120, March 31, 1994:

*Allowable medical expenses* are annual out-of-pocket expenses for health insurance premiums, health care services, and medications provided to

the applicant, enrollee, or spouse and were not and will not be paid for by Medicare, Medicaid, other insurance, or by any other third party and, shall not exceed 15 percent of the applicable Corporation income guideline.

*Annual income* is counted for the past 12 months and includes: The applicant or enrollee's income and the applicant or enrollee's spouse's income, if the spouse lives in the same residence.

Project directors may count the value of shelter, food, and clothing, if provided at no cost by persons related to the applicant, enrollee or spouse.

Any person whose income is not more than 100 percent of the DHHS Poverty Guideline for her/his specific family unit shall be given special consideration for participation in the Foster Grandparent and Senior Companion Programs.

#### 1997 FGP/SCP INCOME ELIGIBILITY LEVELS

[Based on 125 Percent of DHHS Poverty Guidelines]

States	Family units of			
	One	Two	Three	Four
All, except High Cost Areas, Alaska & Hawaii .....	\$9,865	\$13,265	\$16,665	\$20,065

(For family units with more than four members, add \$3,400 for each additional member in all States except designated High Cost Areas, Alaska, and Hawaii).

#### 1997 FGP/SCP INCOME ELIGIBILITY LEVELS FOR HIGH COST AREAS

[Based on 135 Percent of DHHS Poverty Guidelines]

Area	Family units of			
	One	Two	Three	Four
All, except Alaska & Hawaii .....	\$10,655	\$14,325	\$17,995	\$21,670
Alaska .....	13,325	17,915	22,505	27,095
Hawaii .....	12,245	16,470	20,695	24,925

(For family units with more than four members, add: \$4,590 in Alaska, \$4,225 in Hawaii, and \$3,670 in all other areas for each additional member).

The income eligibility levels specified above are based on 135 percent of the DHHS poverty guidelines and are applicable to the following high cost metropolitan statistical areas and primary metropolitan statistical areas:

#### High Cost Areas

(Including all Counties/Locations Included in that Area as Defined by the Office of Management and Budget).

#### Alaska

(All Locations).

#### California

Los Angeles-Compton-San Gabriel-Long Beach-Hawthorne (Los Angeles County).

Santa Barbara/Santa Maria/Lompoc (Santa Barbara County).

Santa Cruz-Watsonville (Santa Cruz County).

Santa Rosa-Petaluma (Sonoma County).

San Diego-El Cajon (San Diego County).

San Jose-Los Gatos (Santa Clara County).

San Francisco/San Rafael (Marin County).

San Francisco/Redwood City (San Mateo County).

San Francisco (San Francisco County).

Oakland-Berkeley (Alameda County).

Oakland-Martinez (Contra Costa County).

Anaheim-Santa Ana (Orange County).

Oxnard-Ventura (Ventura County).

#### District of Columbia/Maryland/Virginia

District of Columbia and Surrounding Counties in Maryland and Virginia.

MD counties: Calvert, Charles, Cecil, Frederick, Montgomery and Prince Georges Counties.

VA counties: Arlington, Fairfax, Loudoun, Prince William, Stafford, Alexandria City, Fairfax City, Falls Church City, Manassas City and Manassas Park City.

#### Hawaii

(All Locations).

#### Illinois

Chicago-Des Plaines-Oak Park-Wheaton-Woodstock (Cook, DuPage and McHenry Counties).

#### Massachusetts

Fall River (Bristol County).

Boston-Malden (Essex, Norfolk, Plymouth, Middlesex and Suffolk Counties).

Salem-Gloucester (Essex County).

Worcester (Worcester County).

Brockton-Quincy-Braintree (Norfolk County).

Dorchester (Suffolk County).

Fitchburg-Leominster (Worcester County).

#### New Jersey

Bergen-Passaic-Paterson (Bergen and Passaic Counties).

Middlesex-Somerset-Hunterdon (Hunterdon, Middlesex and Somerset Counties).

Monmouth-Ocean-Spring Lake (Monmouth and Ocean Counties).

Newark-East Orange (Essex, Morris, Sussex and Union Counties).

Trenton (Mercer County).

#### New York

Nassau-Suffolk-Long Beach-Huntington (Suffolk and Nassau Counties).

New York-Bronx-Brooklyn (Bronx, Kings, New York, Putnam, Queens, Richmond and Rockland Counties).

Westchester-White Plains-Yonkers-Valhalla (Westchester County).

**Pennsylvania**

Philadelphia-Doylestown-West  
Chester-Media-Norristown (Bucks,

Chester, Delaware, Montgomery and  
Philadelphia Counties).  
The revised income eligibility levels  
presented here are calculated from the

base DHHS Poverty Guidelines now in  
effect as follows:

**1997 DHHS POVERTY GUIDELINES FOR ALL STATES**

States	Family units of			
	One	Two	Three	Four
All, except Alaska & Hawaii .....	\$7,890	\$10,610	\$13,330	\$16,050
Alaska .....	9,870	13,270	16,670	20,070
Hawaii .....	9,070	12,200	15,330	18,460

**Authority:** These programs are authorized pursuant to the Domestic Volunteer Service Act of 1973, as amended (42 U.S.C 4950 *et seq.*). The income eligibility levels are determined by the current guidelines published by DHHS pursuant to Sections 652 and 673 (2) of the Omnibus Budget Reconciliation Act of 1981 which requires poverty guidelines to be adjusted for Consumer Price Index changes.

Dated: May 7, 1997.

**Thomas E. Endres,**

*Director, National Senior Service Corps.*

[FR Doc. 97-12470 Filed 5-12-97; 8:45 am]

BILLING CODE 6050-28-P

Wage Committee, 4000 Defense  
Pentagon, Washington, DC 20301-4000.

Dated: May 7, 1997.

**L.M. Bynum,**

*Alternate OSD Federal Register Liaison  
Officer, Department of Defense.*

[FR Doc. 97-12427 Filed 5-12-97; 8:45 am]

BILLING CODE 5000-04-M

Dated: May 6, 1997.

**L.M. Bynum,**

*Alternate OSD Federal Register Liaison  
Officer, Department of Defense.*

[FR Doc. 97-12426 Filed 5-12-97; 8:45 am]

BILLING CODE 5000-04-M

**DEPARTMENT OF DEFENSE****Office of the Secretary****Meeting of the Advisory Council on  
Dependents' Education**

**AGENCY:** Department of Defense,  
Department of Defense Dependents  
Schools (DoDDS).

**ACTION:** Notice of meeting.

**SUMMARY:** Notice is hereby given of a forthcoming semiannual public meeting of the Advisory Council on Dependents' Education (ACDE). The purpose of this meeting is to review the reports on topics raised during the ACDE team visits in November 1996 to DoD overseas schools in Korea and Japan.

**DATES:** May 29, 1997, 8:30 a.m. to 5 p.m. and May 30, 1997, 8:30 a.m. to 1 p.m.

**ADDRESSES:** This meeting will be held in the Secretary of Defense Conference Room (Room 3E869) in the Pentagon.

**FOR FURTHER INFORMATION CONTACT:** Ms. Amy Huffman, Department of Defense Dependents Schools, 4040 North Fairfax Drive, Arlington, Virginia, 22203-1635. Ms. Huffman can be reached at 703-696-4235, extension 100.

**SUPPLEMENTARY INFORMATION:** Space constraints are such that anyone wishing to attend the meeting should contact Ms. Amy Huffman, above, to ensure that seating space is available. The Advisory Council on Dependents' Education is established under Title XIV, section 1411, of Public Law 95-561, Defense Dependents' Education Act of 1978, as amended (20 U.S.C. section 929). The purpose of the Council is to recommend to the Director, DoDDS, general policies for the operation of the DoDDS, to provide the Director, DoDDS,

**DEPARTMENT OF DEFENSE****Office of the Secretary of Defense****Department of Defense Wage  
Committee; Notice of Closed Meetings**

Pursuant to the provisions of section 10 of Public Law 92-463, the Federal Advisory Committee Act, notice is hereby given that closed meetings of the Department of Defense Wage Committee will be held on June 3, 1997; June 10, 1997; June 17, 1997; and June 24, 1997, at 10:00 a.m. in Room A105, The Nash Building, 1400 Key Boulevard, Rosslyn, VA.

Under the provisions of section 10(d) of Public Law 92-463, the Department of Defense has determined that the meetings meet the criteria to close meetings to the public because the matters to be considered are related to internal rules and practices of the Department of Defense and the detailed wage data to be considered were obtained from officials of private establishments with a guarantee that the data will be held in confidence.

However, members of the public who may wish to do so are invited to submit material in writing to the chairman concerning matters believed to be deserving of the Committee's attention.

Additional information concerning the meetings may be obtained by writing to the Chairman, Department of Defense

**DEPARTMENT OF DEFENSE****Office of the Secretary****Defense Intelligence Agency, Scientific  
Advisory Board; Closed Meeting**

**AGENCY:** Department of Defense, Defense  
Intelligence Agency.

**ACTION:** Notice.

**SUMMARY:** Pursuant to the provisions of Subsection (d) of Section 10 of Public Law 92-463, as amended by Section 5 of Public Law 94-409, notice is hereby given that a closed meeting of the DIA Scientific Advisory Board has been scheduled as follows:

**DATES:** May 28 and May 29, 1997 (8:00 am to 16:00 pm).

**ADDRESSES:** The Defense Intelligence Agency, Bolling AFB, Washington, D.C. 20340-5100.

**FOR FURTHER INFORMATION CONTACT:**

Maj. Michael W. Lamb, USAF,  
Executive Secretariat, DIA Scientific  
Advisory Board, Washington, D.C.  
20340-1328 (202) 231-4930.

**SUPPLEMENTARY INFORMATION:** The entire meeting is devoted to the discussion of classified information as defined in Section 552b(c)(1). Title 5 of the U.S. Code and therefore will be closed to the public. The Board will receive briefings on and discuss several current critical intelligence issues and advise the Director, DIA, on related scientific and technical matters.