

For premium payment years beginning in:	The required interest rate is:
Nov. 1996	5.45
Dec. 1996	5.18
Jan. 1997	5.24
Feb. 1997	5.46
Mar. 1997	5.35
Apr. 1997	5.54

Late Premium Payments; Underpayments and Overpayments of Single-Employer Plan Termination Liability

Section 4007(b) of ERISA and § 4007.7(a) of the PBGC's regulation on Payment of Premiums (29 CFR part 4007) require the payment of interest on late premium payments at the rate established under section 6601 of the Internal Revenue Code. Similarly, § 4062.7 of the PBGC's regulation on Liability for Termination of Single-employer Plans (29 CFR part 4062) requires that interest be charged or credited at the section 6601 rate on underpayments and overpayments of employer liability under section 4062 of ERISA. The section 6601 rate is established periodically (currently quarterly) by the Internal Revenue Service. The rate applicable to the second quarter (April through June) of 1997, as announced by the IRS, is 9 percent.

The following table lists the late payment interest rates for premiums and employer liability for the specified time periods:

From	Through	Interest rate (percent)
4/1/91	12/31/91	10
1/1/92	3/31/92	9
4/1/92	9/30/92	8
10/1/92	6/30/94	7
7/1/94	9/30/94	8
10/1/94	3/31/95	9
4/1/95	6/30/95	10
7/1/95	3/31/96	9
4/1/96	6/30/96	8
7/1/96	12/31/96	9
1/1/97	3/31/97	9
4/1/97	6/30/97	9

Underpayments and Overpayments of Multiemployer Withdrawal Liability

Section 4219.32(b) of the PBGC's regulation on Notice, Collection, and Redetermination of Withdrawal Liability (29 CFR part 4219) specifies the rate at which a multiemployer plan is to charge or credit interest on underpayments and overpayments of withdrawal liability under section 4219 of ERISA unless an applicable plan provision provides otherwise. For interest accruing during any calendar

quarter, the specified rate is the average quoted prime rate on short-term commercial loans for the fifteenth day (or the next business day if the fifteenth day is not a business day) of the month preceding the beginning of the quarter, as reported by the Board of Governors of the Federal Reserve System in Statistical Release H.15 ("Selected Interest Rates"). The rate for the second quarter (April through June) of 1997 (i.e., the rate reported for March 17, 1997) is 8.25 percent.

The following table lists the withdrawal liability underpayment and overpayment interest rates for the specified time periods:

From	Through	Rate (percent)
4/1/91	16/30/91	9.00
7/1/91	9/30/91	8.50
10/1/91	12/31/91	8.00
1/1/92	3/31/92	7.50
4/1/92	9/30/92	6.50
10/1/92	6/30/94	6.00
7/1/94	9/30/94	7.25
10/1/94	12/31/94	7.75
1/1/95	3/31/95	8.50
4/1/95	9/30/95	9.00
10/1/95	3/31/96	8.75
4/1/96	12/31/96	8.25
1/1/97	3/31/97	8.25
4/1/97	6/30/97	8.25

Multiemployer Plan Valuations Following Mass Withdrawal

The PBGC's regulation on Duties of Plan Sponsor Following Mass Withdrawal (29 CFR part 4281) prescribes the use of interest assumptions under the PBGC's regulation on Allocation of Assets in Single-employer Plans (29 CFR part 4044). The interest assumptions applicable to valuation dates in May 1997 under part 4044 are contained in an amendment to part 4044 published elsewhere in today's **Federal Register**. Tables showing the assumptions applicable to prior periods are codified in appendix B to 29 CFR part 4044.

Issued in Washington, DC, on this 8th day of April 1997.

John Seal,

Acting Executive Director, Pension Benefit Guaranty Corporation.

[FR Doc. 97-9595 Filed 4-14-97; 8:45 am]

BILLING CODE 7708-01-P

POSTAL SERVICE

Privacy Act of 1974, System of Records

AGENCY: Postal Service.

ACTION: Notice of new system of records.

SUMMARY: This document publishes notice of a new Privacy Act system of records, Collection and Delivery Records—Customer Public Key Certificate Records, USPS 010.090. The new system consists of an electronic database containing limited information about postal customers who have been authorized public key certificates by the Postal Service. A public key certificate is a digital document that can be used to validate the authenticity of a digitally signed document sent by way of the Internet, a service provider, or a value-added network from one customer to another. The Postal Service acts as the certifying authority that assigns and holds public key certificates for participating customers, the records subjects covered by this system.

DATES: Any interested party may submit written comments on the proposed new system of records. This proposal will become effective without further notice on May 27, 1997, unless comments received on or before that date result in a contrary determination.

ADDRESSES: Written comments on this proposal should be mailed or delivered to Payroll Accounting and Records, United States Postal Service, 475 L'Enfant Plaza SW, Room 8650, Washington, DC 20260-5243. Copies of all written comments will be available at the above address for public inspection and photocopying between 8 a.m. and 4:45 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: Betty E. Sheriff, (202) 268-2608.

SUPPLEMENTARY INFORMATION: The Postal Service is conducting a pilot program with several federal agencies. The Postal Service's role is to act as the certifying authority by using and managing X.509 public key certificates containing a person's distinguished name, public key, and other identifying information. Under the program a customer applies to a Registrar (a Postal Service authority) to receive a Postal Service public key certificate. Information collected through the application process is limited to the customer name, address, phone number, electronic mail address, signature, and payment information.

The Registrar then creates a key pair consisting of a public key and a private key. Keys are long, random, bit strings that are unique to the user. That application information, as well as a distinguished name for the user, is transmitted to the Postal Service database covered by this system. The database returns a signed certificate to the Registrar, who enters it onto a disk along with the distinguished name, public key, and private key. The disk is

given to the customer who uses special software, along with the private key, to send and digitally sign documents. The public key and certificate are public data, but the customer is instructed not to disclose the private key and personal identification number (PIN) associated with the private key to a third party.

Maintenance of these records is not expected to affect individual privacy rights because, to the extent that the system covers individuals, limited information about them is kept. A large segment of the population covered by the system is businesses, which are not covered by the Privacy Act. Other than digital components for public key certification, the information kept about a customer is name, distinguished name, public key(s), account, phone number, postal and electronic mail address, and payment information.

Information kept within the database is protected by several layers. The computer housing the database is located in a building with access controlled by guards and a room with access controlled by the use of card keys. Other components of the security architecture are an asynchronous gateway, a network firewall, LAN connection, operating system, database management system, application software, database software security architecture, application software security architecture, and key generation and maintenance. Each of these levels has been subjected to an external audit to ensure security of the system. In addition, internal access to the database is limited to the system administrator, database administrator, and designated support personnel. Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof hardware device. Finally, activities are audited and archived information is protected from corruption, deletion, and modification.

With the above security controls the information will be protected from unauthorized access unless a customer does not heed a warning to keep the private key and PIN secret. If a private key is compromised, the Postal Service will immediately revoke upon notification from the certificate holder the related certificate.

Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments regarding this proposal. A report of the following proposed system has been sent to Congress and to the Office of Management and Budget for their evaluation.

USPS 010.090

SYSTEM NAME:

Collection and Delivery Records—Customer Public Key Certificate Records, USPS 010.090.

SYSTEM LOCATIONS:

Marketing, Headquarters, and Information Systems Service Center, San Mateo, CA.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Business and individual postal customers who apply to receive a public key certificate.

CATEGORIES OF RECORDS IN THE SYSTEM:

The following information is kept with regard to customers who have applied for public key certificates from the Postal Service: Name, address, phone number, electronic mail address, payment information, customer's public key(s), certificate serial numbers, customer's distinguished name, effective dates of authorized certificates, certificate algorithm, date of revocation or expiration of certificate, Postal Service-authorized digital signature, and information supplied by the customer to identify who may have access to public key data related to that customer.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 403 and 404.

PURPOSE(S):

Information within this system is used to issue and manage public key certificates.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

General routine use statements a, b, c, d, e, f, g, h, and j listed in the prefatory statement at the beginning of the Postal Service's published system notices apply to this system. Other routine uses follow:

1. The X.509 certificate and public key associated with a records subject may be disclosed to persons who provide the associated certificate number or distinguished name and who have not been denied access by the records subject.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Paper, automated database, and computer storage media.

RETRIEVABILITY:

Customer name, distinguished name, certificate serial number, and public key.

SAFEGUARDS:

Hard copy records and computers containing information within this system of records are located in a building with entrance access controlled by guards and room access controlled by card readers. Information within the database is protected by a security architecture of several layers that includes an asynchronous gateway, network firewall, operating security system, and database software security architecture. Internal access to the database is limited to the system administrator, database administrator, and designated support personnel. Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof, hardware device. Activities are audited and archived information is protected from corruption, deletion, and modification.

RETENTION AND DISPOSAL:

a. *Pending Public Key Certificate Application Files.* These records are added as received to an electronic database. Move to authorized certificate file when they are updated with the required data. Destroy records not updated within 90 days from the date of receipt.

b. *Public Key Certificate Directory.* These records are maintained in an electronic database and are constantly updated. Destroy records as they are superseded or deleted.

c. *Authorized Public Key Certificate Master File.* These records are maintained in an electronic database for the life of the authorized certificate. Move to the certificate revocation file when certificate is revoked or expired.

d. *Public Key Certificate Revocation List.* Cut off this file at the end of each calendar year. Destroy these records 30 years from the date of cutoff.

SYSTEM MANAGER(S) AND ADDRESS:

Vice President, Technology Applications, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-2403

NOTIFICATION PROCEDURE:

Individuals wanting to know whether information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name and certificate serial number.

RECORD ACCESS PROCEDURES:

Access must be requested in accordance with the Notification Procedure above and the Postal Service

Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

CONTESTING RECORD PROCEDURES:

See Notification Procedure and Record Access Procedures above.

RECORD SOURCE CATEGORIES:

Customers.

Stanley F. Mires,

Chief Counsel, Legislative.

[FR Doc. 97-9590 Filed 4-15-97; 8:45 am]

BILLING CODE 7710-12-P

SECURITIES AND EXCHANGE COMMISSION

Sunshine Act Meeting

Notice is hereby given, pursuant to the provisions of the Government in the Sunshine Act, Pub. L. 94-409, that the Securities and Exchange Commission held a closed meeting on Tuesday, April 8, 1997.

Commissioners, Counsel to the Commissioners, the Secretary to the Commission, and recording secretaries attended the closed meeting. Certain staff members with an interest in the matters were also present.

The General Counsel of the Commission, or his designee, has certified that, in his opinion, one or more of the exemptions set forth in 5 U.S.C. 552b(c) (4), (8), (9)(A) and (10) and 17 CFR 200.402(a) (4), (8), (9)(i) and (10), permit consideration of the scheduled matters at the closed meeting.

Commissioner Johnson, as duty officer, voted to consider the items listed for the closed meeting in a closed session.

The subject matter of the closed meeting held on Tuesday, April 8, 1997, at 11:15 a.m., was:

Matter involving confidential privileged commercial or financial information.
Institution of injunctive action.
Formal order of investigation.

Commissioner Johnson, as duty officer, determined that Commission business required the above change and that no earlier notice thereof was possible.

At times, changes in Commission priorities require alterations in the scheduling of meeting items. For further information and to ascertain what, if any, matters have been added, deleted or postponed, please contact: The Office of the Secretary at (202) 942-7070.

Dated: April 11, 1997.

Johathan G. Katz,

Secretary.

[FR Doc. 97-9888 Filed 4-11-97; 3:54 pm]

BILLING CODE 8010-01-M

DEPARTMENT OF STATE

[Public Notice No. 2530]

Defense Trade Advisory Group; Notice of Upcoming Meeting

The Defense Trade Advisory Group (DTAG) will meet beginning at 8:30 a.m. on Friday, May 16, 1997, in the East Auditorium, U.S. Department of State, 2201 C Street, NW., Washington, DC 20520. This advisory committee consists of private sector defense trade specialists who advise the Department on policies, regulations, and technical issues affecting defense trade.

The open session will include presentations by representatives of the Department of State and the Department of Defense. Reports on DTAG Working Group progress, accomplishments, and future projects will also be presented.

Members of the public may attend the open session as seating capacity allows, and will be permitted to participate in the discussion in accordance with the Chairman's instructions.

As access to the Department of State is controlled, persons wishing to attend the meeting must notify the DTAG Executive Secretariat by COB Monday, May 12, 1997. If you notify the DTAG Secretariat after this date, the DTAG Secretariat cannot guarantee that State's Bureau of Diplomatic Security can complete the necessary background checks required for you to attend the May 16 plenary.

Each person should provide his/her name, company or organizational affiliation, date of birth, and social security number to the DTAG Secretariat at telephone number (202) 647-4231 or fax number (202) 647-4232 (Attention: Catherine Shelton). A list will be made up for Diplomatic Security and the Reception Desk at the C-Street diplomatic entrance. Attendees must carry a valid photo ID with them. They should enter the building through the C-Street diplomatic entrance (22nd and C Streets, NW.) where Department personnel will direct them to the East auditorium.

A working lunch will be held at the Department. Limits on available seating may require that only DTAG members may attend.

For further information, contact Catherine Shelton of the DTAG Secretariat, U.S. Department of State, Office of Arms Transfer and Export Control Policy (PM/ATEC), Room 2422 Main State, Washington, DC 20520-2422. She may be reached at telephone number (202) 647-4231 or fax number (202) 647-4232.

Dated: April 9, 1997.

Martha C. Harris,

Deputy Assistant Secretary for Export Controls, Bureau of Political-Military Affairs.
[FR Doc. 97-9654 Filed 4-14-97; 8:45 am]

BILLING CODE 4710-25-M

DEPARTMENT OF TRANSPORTATION

Office of the Secretary

[OST Docket No. OST-95-141 (50125)]

Department of Transportation (DOT) Order To Address Environmental Justice in Minority Populations and Low-Income Populations

AGENCY: Departmental Office of Civil Rights and Office of the Assistant Secretary for Transportation Policy, DOT.

ACTION: Notice of final DOT Order on environmental justice.

SUMMARY: The Department of Transportation is issuing its final DOT Order, which will be used by DOT to comply with Executive Order 12898, *Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations*. The Order generally describes the process that the Office of the Secretary and each Operating Administration will use to incorporate environmental justice principles (as embodied in the Executive Order) into existing programs, policies, and activities. The Order provides that the Office of the Secretary and each Operating Administration within DOT will develop specific procedures to incorporate the goals of the DOT Order and the Executive Order with the programs, policies and activities which they administer or implement.

FOR FURTHER INFORMATION CONTACT: Ira Laster Jr., Office of Environment, Energy, and Safety, Office of the Assistant Secretary for Transportation Policy, (202) 366-4859, or Marc Brenman, Departmental Office of Civil Rights, (202) 366-1119, U.S. Department of Transportation, 400 7th Street, SW., Washington, DC 20590.

SUPPLEMENTARY INFORMATION: Executive Order 12898, as well as the President's February 11, 1994 Memorandum on Environmental Justice (sent to the heads of all departments and agencies), are intended to ensure that Federal departments and agencies identify and address disproportionately high and adverse human health or environmental effects of their policies, programs and activities on minority populations and low-income populations.