obligations being enforced by States. One of the key debt collection tools used by FMS is administrative offset. As amended by the Debt Collection Improvement Act of 1996 (DCIA), Pub. L. 104–134 (April 26, 1996), 31 U.S.C. 3716 requires Federal disbursing officials to offset payments to collect delinquent debts submitted to FMS by Federal agencies for collection by offset. This process is known as ''centralized administrative offset'' or ''centralized offset.'' In addition, 31 U.S.C. 3716 authorizes the use of centralized offset to collect delinquent debts owed to states. Federal and State agencies submit delinquent debtor information to FMS, and FMS maintains information about individuals in a ''system of records'' for debt collection entitled ''Debt Collection Operations System,'' identified as Treasury/FMS .014.

To implement the centralized offset provisions of the DCIA, FMS matches records concerning Federal payments with its debt collection records. To date, FMS has concentrated its efforts on offsetting Treasury-disbursed payments made by FMS. For this purpose, a comprehensive notice of computer matches was published in the **Federal Register** on August 28, 1997, Volume 62 at page 45699 concerning records contained in FMS' payment systems of records (Payment Issue Records for Regular Recurring Benefit Payments (Treasury/FMS .002) and Payment Records for Other than Regular Recurring Benefit Payments (Treasury/FMS .016)) with records contained in the FMS' Debt Collection Operations System.

FMS is working with other Federal agencies authorized to disburse Federal payments, known as Non-Treasury Disbursing Officials (NTDOs), to implement centralized offset of payments disbursed by Federal agencies other than FMS. *See, for example*, the notice published in the **Federal Register** on September 23, 2002, Volume 67 at page 59596 concerning payments disbursed by the United States Postal Service. This notice concerns the computer matching programs used to facilitate administrative offset involving records from FMS' ''Debt Collection Operations System'' and records from the following system maintained by an NTDO: United States Department of Defense: DFAS Payroll Locator File System (PLFS) (T7330).

The DCIA provides authority for Treasury to waive subsections (o) and (p) of 5 U.S.C. 552a (relating to computer matching agreements and post-offset notification and verification) upon written certification by the head of a state or an executive, judicial, or legislative agency seeking to collect the claim that the requirements of subsection (a) of 31 U.S.C. 3716 have been met. Treasury has exercised its authority to waive the aforementioned requirements, and the waiver will be in effect prior to the commencement of the computer matching program(s) identified in this notice. Interested parties may obtain documentation concerning the waiver from the contact listed above.

NAME OF SOURCE AGENCY:

United States Department of Defense

NAME OF RECIPIENT AGENCY:

Financial Management Service

BEGINNING AND COMPLETION DATES:

These programs of computer matches will commence not earlier than the thirtieth day after this notice appears in the **Federal Register**. The matching will continue indefinitely, or until the waiver from the requirements of 5 U.S.C. 552a(o) and (p) is revoked.

PURPOSE:

The purpose of these programs of computer matches is to identify payments made to individuals who owe delinquent debts to the Federal government or to state governments, as well as individuals who owe past-due support being collected by state governments, which will be collected by offset pursuant to 31 U.S.C. 3716, and to offset such payments where appropriate to satisfy those debts.

AUTHORITY:

Authority for these programs of computer matches is granted under 31 U.S.C. 3716.

CATEGORIES OF INDIVIDUALS COVERED:

Individuals receiving payments from the Federal government which are disbursed by the United States Department of Defense; and individuals who owe debts to the United States and/or a state government, or who owe past-due support being enforced by a state government, and whose debts may be collected by offset in accordance with 31 U.S.C. 3716.

CATEGORIES OF RECORDS COVERED:

Included in these programs of computer matches is information concerning the debtor contained in the Debt Collection Operations System (Treasury/FMS .014) including name, taxpayer identification number, the amount of the indebtedness, the name and address of the state or Federal agency who is principally responsible for collecting the debt, and the name, phone number and address of a state or agency contact. Information contained in the following system: United States Department of Defense: DFAS Payroll Locator File System (PLFS) (T7330), which shall be included in these programs of computer matches shall include name, taxpayer identification number, mailing address, and the amount and type of payment.

Dated: December 9, 2002.

W. Earl Wright, Jr.,

Chief Management and Administrative Programs Officer.

[FR Doc. 02–31587 Filed 12–16–02; 8:45 am]

BILLING CODE 4810–35–P

DEPARTMENT OF THE TREASURY

Departmental Offices; Privacy Act of 1974; System of Records

AGENCY: Departmental Offices, Treasury.

ACTION: Notice of proposed Privacy Act system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the Department of the Treasury (Department) gives notice of a proposed system of records entitled ''Treasury/DO .216—Treasury Security Access Control and Certificates Systems.''

DATES: Comments must be received no later than January 16, 2003. The proposed system of records will be effective January 27, 2003, unless the Department receives comments that would result in a contrary determination.

ADDRESSES: Comments should be sent to Patrick Geary, Director, Physical Security, Department of the Treasury, 1500 Pennsylvania Ave., NW., Washington, DC. E-mail: *patrick.geary@do.treas.gov*

FOR FURTHER INFORMATION CONTACT: Patrick Geary, Office of Security, (202) 622–1058.

SUPPLEMENTARY INFORMATION: The Department of the Treasury is giving notice of a new system of records which is subject to the Privacy Act. The proposed system of records will maintain Treasury headquarters, Departmental Offices (DO), information on all employees and contractors working in DO for the purpose of providing additional physical and cyber security for DO assets. The new system of records covers three principal areas: (1) Physical access to the Treasury headquarters complex, selected spaces in that complex and other DO spaces; (2) Access to cyber information assets; and (3) Physical access to off-site continuity of operations locations. New

identification badges will be issued containing the employee's photograph, fingerprint minutia, a public key (PKI) certificate and the employee's social security number.

DO plans to implement a new Access Control System for Treasury headquarters including the Main Treasury and Annex buildings that will utilize new DO identification badges to be issued because of the September 11, 2001 incidents. The new badge will be used to gain access to cyber assets including the DO desktop PC, the DO LAN, DO laptop and notebook computers. Finally, the new badge will be utilized by selected DO staff and contractors involved and/or designated as key personnel during conditions that require activation of the DO COOP locations. The badge, which includes biometrics, will be used as an additional level of security authentication during conditions that involve activation of COOP sites.

The new system of records report, as required by 5 U.S.C. 552a(r) of the Privacy Act, has been submitted to the Committee on Government Reform and Oversight of the House of Representatives, the Committee on Governmental Affairs of the Senate and the Office of Management and Budget, pursuant to Appendix I to OMB Circular A–130, ''Federal Agency Responsibilities for Maintaining Records About Individuals,'' dated November 30, 2000. This system of records, ''Treasury/DO .216—Treasury Security Access Control and Certificates Systems,'' is published in its entirety below.

Dated: December 3, 2002.

W. Earl Wright, Jr.,

Chief Management and Administrative Programs Officer.

Treasury/DO .216

SYSTEM NAME:

Treasury Security Access Control and Certificates Systems.

SYSTEM LOCATION:

Department of the Treasury, 1500 Pennsylvania Avenue, NW, Washington, DC 20220.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Treasury employees, contractors, media representatives, other individuals requiring access to Treasury facilities or to receive government property, and those who need to gain access to a Treasury DO cyber asset including the network, LAN, desktops and notebooks.

CATEGORIES OF RECORDS IN THE SYSTEM:

Individual's application for security/access badge, individual's photograph, finger print record, special credentials, allied papers, registers, and logs reflecting sequential numbering of security/access badges. The system also contains information needed to establish accountability and audit control of digital certificates that have been assigned to personnel who require access to Treasury DO cyber assets including the DO network and LAN as well as those who transmit electronic data that requires protection by enabling the use of public key cryptography. It also contains records that are needed to authorize an individual's access to a Treasury network.

Records may include the individual's name, organization, work telephone number, Social Security Number, date of birth, Electronic Identification Number, work e-mail address, username and password, country of birth, citizenship, clearance and status, title, home address and phone number, biometric data including fingerprint minutia, and alias names.

Records on the creation, renewal, replacement or revocation of digital certificates, including evidence provided by applicants for proof of identity and authority, sources used to verify an applicant's identity and authority, and the certificates issued, denied and revoked, including reasons for denial and revocation.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 31 U.S.C. 321; the Electronic Signatures in Global and National Commerce Act, Pub. L. 106–229, and E.O. 9397 (SSN).

PURPOSE(S):

The purpose is to: Improve security to both Treasury DO physical and cyber assets; maintain records concerning the security/access badges issued; restrict entry to installations and activities; ensure positive identification of personnel authorized access to restricted areas; maintain accountability for issuance and disposition of security/access badges; maintain an electronic system to facilitate secure, on-line communication between Federal automated systems, between Federal employees or contractors, and or the public, using digital signature technologies to authenticate and verify identity; provide a means of access to Treasury cyber assets including the DO network, LAN, desktop and laptops; and to provide mechanisms for non-repudiation of personal identification and access to DO sensitive cyber systems including but not limited to human resource, financial, procurement, travel and property systems as well as tax, econometric and other mission critical systems. The system also maintains records relating to the issuance of digital certificates utilizing public key cryptography to employees and contractors for purpose of the transmission of sensitive electronic material that requires protection.

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

These records may be used to disclose information to: (1) Appropriate Federal, state, local and foreign agencies for the purpose of enforcing and investigating administrative, civil or criminal law relating to the hiring or retention of an employee; issuance of a security clearance, license, contract, grant or other benefit;

(2) A court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of or in preparation for civil discovery, litigation, or settlement negotiations, in response to a subpoena where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) A contractor for the purpose of compiling, organizing, analyzing, programming, or otherwise refining records to accomplish an agency function subject to the same limitations applicable to U.S. Department of the Treasury officers and employees under the Privacy Act;

(4) A Congressional office in response to an inquiry made at the request of the individual to whom the record pertains;

(5) Third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation;

(6) The Office of Personnel Management, Merit Systems Protection Board, Equal Employment Opportunity Commission, Federal Labor Relations Authority, and the Office of Special Counsel for the purpose of properly administering Federal personnel systems or other agencies' systems in accordance with applicable laws, Executive Orders, and regulations;

(7) Representatives of the National Archives and Records Administration (NARA) who are conducting records management inspections under authority of 44 U.S.C. 2904 and 2906; and

(8) Other Federal agencies or entities when the disclosure of the existence of the individual's security clearance is

needed for the conduct of government business.

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

STORAGE:

Records are stored as electronic media and paper records.

RETRIEVABILITY:

Records are retrieved by individual's name, social security number, electronic identification number and/or access/security badge number.

SAFEGUARDS:

Entrance to data centers and support organization offices are restricted to those employees whose work requires them to be there for the system to operate. Identification (ID) cards are verified to ensure that only authorized personnel are present. Disclosure of information through remote terminals is restricted through the use of passwords and sign-on protocols which are periodically changed. Reports produced from the remote printers are in the custody of personnel and financial management officers and are subject to the same privacy controls as other documents of like sensitivity.

Access is limited to authorized employees. Paper records are maintained in locked safes and/or file cabinets. Electronic records are password-protected. During non-work hours, records are stored in locked safes and/or cabinets in locked room.

Protection and control of any sensitive but unclassified (SBU) records are in accordance with TD P 71–10, Department of the Treasury Security Manual. Access to the records is available only to employees responsible for the management of the system and/or employees of program offices who have a need for such information.

RETENTION AND DISPOSAL:

The records on government employees and contractor employees are retained for the duration of their employment at the Treasury Department. The records on separated employees are destroyed or sent to the Federal Records Center in accordance with General Records Schedule 18.

SYSTEM MANAGER(S) AND ADDRESS:

Departmental Offices: Director, Office of Physical Security, 1500 Pennsylvania Ave., NW., Washington, DC 20220.

NOTIFICATION PROCEDURE:

Individuals seeking notification and access to any record contained in the system of records, or seeking to contest its content, may inquire in accordance with instructions pertaining to individual Treasury components appearing at 31 CFR part 1, subpart C, appendix A.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

The information contained in these records is provided by or verified by the subject individual of the record, supervisors, other personnel documents, and non-Federal sources such as private employers.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

[FR Doc. 02–31261 Filed 12–16–02; 8:45 am]

BILLING CODE 4811–16–P

DEPARTMENT OF THE TREASURY

Customs Service

Modification of National Customs Automation Program Test Regarding Electronic Presentation of Cargo Declarations

AGENCY: U.S. Customs Service, Department of the Treasury.

ACTION: General notice.

SUMMARY: This notice announces modifications to the vessel paperless manifest program test that provides for the electronic transmission of certain vessel cargo declaration information to Customs through the Vessel Automated Manifest System (AMS). Specifically, the changes to the program test relate to the following: (1) Test participants must electronically transmit cargo declaration information to Customs through Vessel AMS 24 hours prior to lading the cargo aboard the vessel at the foreign port; (2) test participants must electronically transmit manifest information on empty containers to Customs through the Empty Container Module within Vessel AMS; and (3) Customs is discontinuing use of the paperless cargo declaration standards checklist that was developed for determining carrier compliance with the test. Public comments are invited on any aspect of the program test as further modified by today's announcement.

DATES: The effective date for test participants to transmit cargo declaration information 24 hours prior to lading the cargo aboard vessels at foreign ports is December 2, 2002. The effective date for test participants to electronically transmit manifest data on empty containers to Customs through the Empty Container Module within Vessel AMS is June 2, 2003. Letters requesting participation in the test and comments concerning any aspect of the test will continue to be accepted throughout the testing period.

ADDRESSES: Written comments regarding the program test and letters requesting participation in the program test should be addressed to the Manifest and Conveyance Branch, Office of Field Operations, U.S. Customs Service, 1300 Pennsylvania Avenue, NW., Room 5.2b, Washington, DC 20229.

FOR FURTHER INFORMATION CONTACT: For operational or policy matters: Julie Hannan, Manifest and Conveyance Branch, (202–927–1364); or Pete Flores, Manifest and Conveyance Branch, (202–927–0333).

For legal matters: Larry L. Burton, Office of Regulations and Rulings, (202–572–8724).

SUPPLEMENTARY INFORMATION:

Background

On September 10, 1996, Customs published a notice in the **Federal Register** (61 FR 47782) announcing a program test to allow the electronic transmission of certain vessel cargo declaration information to Customs through the Automated Manifest System (AMS). The September 10, 1996, notice described the parameters and requirements of the test, informed interested members of the public of the eligibility and application criteria for participation in the test, and requested comments concerning any aspect of the test. The test commenced on February 11, 1997, and, by a notice published in the **Federal Register** (62 FR 66719) on December 19, 1997, the program test was extended and modified with respect to the presentation of manifest information on empty containers. Since its inception, as noted, the test has been running successfully with 35 vessel carriers as participants.

Pertinent Aspects of Current Program Test

As prescribed in the September 10, 1996, program test notice, a participating vessel carrier must electronically transmit to Customs complete and accurate cargo declaration information no less than 48 hours prior to the actual arrival of the vessel at a port in the United States.

Furthermore, as modified by the December 19, 1997, notice, the program test provided that empty containers were to be manifested either by transmitting through the Customs Automated Manifest System (AMS) a list of the empty containers on board the