Billing Code: 4810-25

DEPARTMENT OF THE TREASURY

Privacy Act of 1974; System of Records

AGENCY: Departmental Offices, Department of the Treasury.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of the Treasury ("Treasury" or the "Department"), Departmental Offices proposes to modify a current Treasury system of records titled, "Department of the Treasury/Departmental Offices - .216 Treasury Security Access Control and Certificates Systems System of Records."

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. The new routine uses will be applicable on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*] unless Treasury receives comments and determines that changes to the system of records notice are necessary.

ADDRESSES: Comments may be submitted to the Federal eRulemaking Portal electronically at http://www.regulations.gov. Comments can also be sent to the Deputy Assistant Secretary for Privacy, Transparency, and Records, Department of the Treasury, Departmental Offices, 1500 Pennsylvania Avenue NW, Washington, DC 20220, Attention: Revisions to Privacy Act Systems of Records. All comments received, including attachments and other supporting documents, are part of the public record and subject to public disclosure. All comments received will be posted without change to

www.regulations.gov, including any personal information provided. You should submit only information that you wish to make publicly available.

FOR FURTHER INFORMATION CONTACT: For general questions and privacy issues please contact: Deputy Assistant Secretary for Privacy, Transparency, and Records (202-622-5710), Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

SUPPLEMENTARY INFORMATION:

In accordance with the Privacy Act of 1974, the Department of the Treasury ("Treasury") Departmental Offices (DO) proposes to modify a current Treasury system of records titled, "Treasury/Departmental Offices .216 - Treasury Security Access Control and Certificates Systems." This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of system of records maintained by the agency (5 U.S.C. 552a(e)(4)).

The Treasury Security Access Control and Certificates System improves security for both Treasury and DO physical and cyber assets by: maintaining records concerning the security/access badges Treasury issues; risk assessments (including background checks) to validate the decision to grant access (or not) to Treasury facilities and cyber assets; restricting entry to installations and activities; ensuring positive identification of personnel and others authorized to access restricted areas; maintaining accountability for issuance and disposition of security/access badges; maintaining an electronic system to facilitate secure on-line communication between federal automated systems, federal employees or contractors, and/or the public, using digital signature technologies to

authenticate and verify identity; providing a means of access to Treasury cyber assets including the DO network, local area 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 using public key cryptography to employees and contractors for the purpose of transmission of sensitive electronic material that requires protection. Treasury is authorized to collect and share this information for the above purposes under the following statutes and Executive Orders: 5 U.S.C. 301; 31 U.S.C. 321; 18 U.S.C. 3056A(3) and E.O. 9397 (SSN).

The purpose of this report is to give notice of a modified system of records notice – Treasury/Departmental Offices .216 Treasury Security Access Control and Certificates Systems. Treasury is modifying this existing SORN to: (1) add a new authority; (2) add a new category of records (and data elements); (2) clarify and make more explicit disclosures that are currently the subject of existing routine uses; and (3) add two routine uses to replace an existing routine use on the same subject (as required by OMB).

(1) Additional Authority

Treasury is modifying this existing SORN to add an authority. This new authority, 18 U.S.C. 3056A(3), establishes a "permanent police force," under the USSS Uniformed Division, and the USSS authority to protect the Treasury Buildings and grounds. The EOP requires prospective Main Treasury and Freedman's Bank Building visitors

(including new Treasury employees who have not yet been badged) to provide records necessary for the Executive Office of the President (EOP) and USSS to conduct risk assessments (including background investigations) to determine suitability for access to Main Treasury and the Freedman's Bank Building because of the proximity of these facilities to the White House. This authority, permits sharing between Treasury and USSS for the purposes of protecting the Main Treasury, the Freedman's Bank Building, and their occupants.

(2) Adding a New Category of Records/Data Elements

Treasury is also modifying this SORN to include a new category of records the Executive Office of the President (EOP) requires from all visitors to the White House Complex to assist the EOP in conducting risk assessments before prospective visitors are allowed to enter Main Treasury and/or the Freedman's Bank Building. The new category of records will allow the collection of the names of countries/locations a prospective visitor has visited in the last 30 days before completing the form (including the dates reflecting when they entered and left each country/location visited). The EOP added these new data elements to enhance its risk assessments when considering visitor requests. The collection of these new records will improve personnel and visitor health and safety in accordance with EOP requirements. These purposes are consistent with the overall purpose of this system of records.

Treasury is also modifying the SORN to add a data element (personal email address) to the category of records that is incidentally collected via an existing data field. The current SORN identifies "work email address" as a data element collected in this

system of records. The data field in one of the forms in which data in this system is collected requires "Email." Experience has shown that some visitors are entering personal email addresses. Treasury is making this modification for the purpose of clarifying data collected in this field.

Treasury is also modifying the SORN to make explicit data elements collected that are already encompassed in another existing category of records in the existing SORN. The existing categories of records includes "home address." In some instances, when collecting records for inclusion in this system of records, the entire home address is not required and only components of the address (City and State of Residence) are collected. For purposes of clarification, City of Residence and State of Residence are added as separate data elements in the Categories of Records to avoid confusion.

(3) Clarifying and making more explicit disclosures that are currently the subject of existing routine uses

This is more of a clarification than a new routine use, but Treasury is also adding a new routine use (routine use 11) to make more explicit the disclosure of records to EOP and USSS that are pertinent to risk assessments (including background investigations). These disclosures are already covered under routine uses 1 and 5, but the new routine use language will make clear that the EOP and USSS are recipients of disclosures of records from this system of records.

Treasury is also adding two modified routine uses (new routine uses 9 & 10) to replace existing routine use 9 which covers the same subject (breach mitigation). The term "modified" is used because these new routine uses replace an existing routine use on

the same subject. These modifications were required by Office of Management and Budget (OMB) Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," dated January 3, 2017.

Other changes throughout the document are editorial in nature and consist primarily of correction of citations, updates to addresses, authorities, notification procedure, and clarification to the storage and safeguards. Other changes throughout the document are editorial in nature and consist primarily of correction of citations, updates to addresses, and clarification to the storage and safeguards.

Treasury has evaluated the effect of these modified systems on individual privacy and determined that the impact on individual privacy is outweighed by the risks associated with securing Treasury's physical and cyber assets and the physical safety and health of Treasury visitors, personnel, and facilities.

Treasury will include this modified system in its inventory of record systems. Below is the description of the modified Treasury/Departmental Offices .216 - Treasury Security Access Control and Certificates Systems System of Records.

Treasury has provided a report of this system of records to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and OMB, pursuant to 5 U.S.C. 552a(r) and OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," dated December 23, 2016.

Ryan Law,

Deputy Assistant Secretary for Privacy, Transparency, and Records.

SYSTEM NAME AND NUMBER:

Treasury/DO .216 - Treasury Security Access Control and Certificates Systems.

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION:

a. Physical records are maintained at Department of the Treasury, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

b. Visitor records are maintained at Department of the Treasury, Departmental Offices, Chief Information Officer, 1750 Pennsylvania Avenue NW, Washington, DC 20220.

SYSTEM MANAGER(S):

Departmental Offices:

a. Director, Office of Security Programs, 1500 Pennsylvania Avenue NW, Washington, DC 20220.

b. Chief Information Officer, 1750 Pennsylvania Avenue NW, Washington, DC 20220.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; 31 U.S.C. 321; 18 U.S.C. 3056A(3) and E.O. 9397 (SSN).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to: improve the security of Treasury Departmental Offices (DO) physical and cyber assets as well as the physical safety of Treasury visitors, personnel and facilities; issue security/access badges; restrict entry to installations and activities; ensure positive identification of personnel authorized access to restricted areas;

conduct background checks to validate the decision to grant access (or not); maintain accountability for issuance and disposition of security/access badges; maintain an electronic system to facilitate secure, on-line communication between Federal automated systems, and between Federal employees or contractors, and the public, using digital signature technologies to authenticate and verify identity; provide a means of access to Treasury cyber assets including the DO network, local area 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 the purpose of transmission of sensitive electronic material that requires protection.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Treasury employees, contractors, media representatives, and other individuals requiring access to Treasury facilities or 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 or access to Main Treasury or the Freedman's Bank Building;
- Personal device identifier/Serial numbers certificate details;

- Individual’s photograph;
- Fingerprint records;
- Special credentials;
- Treaty or agreement papers;
- Registers;
- Logs reflecting sequential numbering of security/access badges;
- Travel history information

The system also contains information needed to establish accountability and audit control of digital certificates that have been assigned to personnel who require visitor access, access to Treasury DO cyber assets including 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, and Treasury facilities.

Records may include the individual’s:

- Name (first, middle, last);
- Gender;
- Organization;
- Work / personal telephone number;
- Social Security Number;
- Date of birth;
- Electronic Identification Number;
- Work / personal e-mail address;

- Username and password;
- Country of birth;
- Citizenship;
- City of Residence;
- State of Residence;
- Names of countries/locations visited in the past 30 days (including travel start and end date(s));
- Clearance and status;
- Title;
- Work / home address and phone number;
- Biometric data including fingerprint minutia;
- Audit logs and security monitoring information such as Appointment ID number, Appointment Date and time, Appointment type, Location, Room number, salesforce ID;
- Specific aids or services for the disabled;
- Alias names; and
- Records on the creation, renewal, replacement or revocation of electronic access, ingress/egress rights, digital certificates including evidence provided by applicants for proof of identity, sources used to verify an applicant's identity and authority, the certificates, and electronic access and ingress/egress rights issued, denied, and revoked, including reasons for denial and revocation.

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.

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

In addition to those disclosures generally permitted under the Privacy Act of 1974, 5 U.S.C. 552a(b), records and/or information or portions thereof maintained as part of this system may be disclosed outside Treasury as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) To 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) To 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 court order where relevant or potentially relevant to a proceeding, or in connection with criminal law proceedings;

(3) To 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) To a congressional office from the record of an individual in response to an inquiry from that congressional office made pursuant to a written Privacy Act waiver at the request of the individual to whom the record pertains;

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

(6) To 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) To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906;

(8) To 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;

(9) To appropriate agencies, entities, and person when (1) the Department of the Treasury and/or Departmental Offices suspects or has confirmed that there has been a breach of the system of records; (2) the Department of the Treasury and/or Departmental Offices has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Department of

the Treasury and/or Departmental Offices (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department of the Treasury's and/or Departmental Offices' efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm;

(10) To another Federal agency or Federal entity when the Department of the Treasury and/or Departmental Offices determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach; and

(11) To the Executive Office of the President and the United States Secret Service to allow risk assessments (including background investigations) to determine if prospective visitors to Main Treasury and the Freedman's Bank Building should be granted or denied access to Department of the Treasury areas secured by USSS, or to areas in proximity to persons protected by USSS.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored electronically or on paper in secure facilities in a

locked drawer behind a locked door.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by an individual's name, social security number, email address, electronic identification number and/or access/security badge number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

In accordance with National Archives and Records Administration General Records Schedule 5.2 item 20, records are maintained on government employees and contractor employees for the duration of their employment at the Treasury Department. Records on separated employees are destroyed or sent to the Federal Records Center. Records on members of the public seeking access to a Treasury facility protected by USSS are temporary records and are destroyed after USSS makes Treasury facility access determinations.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable Treasury automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances.

Entrance to data centers and support organization offices is 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 similar 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 a 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.

Temporary records are collected by Treasury on behalf of the USSS so they can determine whether members of the public will be granted or denied access to Department of the Treasury areas secured by the USSS. Those temporary records are only available to Treasury and authorized employees, and are maintained in password protected systems or locked containers until transmitted to the USSS.

RECORD ACCESS PROCEDURES:

See “Notification Procedures” below.

CONTESTING RECORD PROCEDURES:

See "Notification Procedures" below.

NOTIFICATION PROCEDURES:

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.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Notice of this system of records was last published in full in the *Federal Register* on November 7, 2016 (81 FR 78298) as the Department of the Treasury/Departmental Offices .216 - Treasury Security Access Control and Certificates Systems.

[FR Doc. 2020-04669 Filed: 3/6/2020 8:45 am; Publication Date: 3/9/2020]