Privacy and Civil Liberties Impact Assessment
for the

System to Administer Retirement (STAR)

February 15, 2017

System Owner
Nancy Ostrowski
Director for the Office of D.C. Pensions
Department of the Treasury
202-622-2214

Reviewing Official
Ryan Law
Deputy Assistant Secretary for Privacy, Transparency, and Records
Department of the Treasury
202-622-8098

Section 1.0: Introduction

This Privacy and Civil Liberties Impact Assessment (PCLIA) is being completed pursuant to Section 208 of the e-Government Act of 2002 (e-Gov Act), 44 U.S.C. § 3501, and Office of the Management and Budget (OMB) M-03-22, which require agencies to conduct a Privacy Impact Assessment (PIA) before:

1. developing or procuring IT systems or projects that collect, maintain or disseminate personally identifiable information (PII) from or about members of the public, or

2. initiating, a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities or employees of the federal government are not included.

It is the policy of the Department of the Treasury and its Bureaus to conduct a PCLIA on systems or projects that maintain PII to identify potential privacy and civil liberties risks. PCLIAs are required for all systems and projects that collect, maintain, or disseminate PII, regardless of whether information is retrieved using PII.

This PCLIA provides the following information regarding the system or project: (1) an overview of its purpose and functions; (2) a description of the information collected; (3) a description of the how information is maintained, used and shared; (4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and (5) an overview of the redress procedures available to individuals who may be affected by the use or sharing of information by the system or project.

Section 2.0: Definitions

Agency – means any entity that falls within the definition of the term “executive agency”' as defined in section 102 of title 31, United States Code, or “agency”, as defined in section 3502 of title 44, United States Code.

Collect (including “collection”) – means the retrieval, receipt, gathering or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

Contractors and service providers - include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining.--The term ``data mining'' means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where-- (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of

terrorist or criminal activity on the part of any individual or individuals; (B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (C) the purpose of the queries, searches, or other analyses is not solely-- (i) the detection of fraud, waste, or abuse in a Government agency or program; or (ii) the security of a Government computer system.

Disclosure – When it is clear from its usage in this manual that the term "disclosure" refers to records provided to the public in response to a request under the Freedom of Information Act (FOIA) (5 U.S.C. § 552) or the Privacy Act, its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms "sharing" and "dissemination" as defined in this manual.

Dissemination – as used in this manual, is synonymous with the terms "sharing" and "disclosure" (unless it is clear from the context that the use of the term "disclosure" refers to a FOIA/Privacy Act response).

E-Government - the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery.

Federal information system - a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

Government information - information created, collected, used, maintained, processed, disseminated, or disposed of by or for the Federal Government.

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. In certain contexts, the term individual may also include citizens of the European Union or others, but only to the extent they are covered by an international or other agreement that involves information stored in the system or used by the project.

Information – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. If any of the information used in the system or project is not contained in a Privacy Act system of records, you still must respond unless the question clearly limits the discussion to a Privacy Act "system of records."

Information life cycle - the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information management - the planning, budgeting, manipulating, and controlling of information throughout its life cycle (from the time it is acquired or collected until its disposal).

Information system life cycle - the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

Information technology (IT) – any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage

devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

Major Information system - embraces "large" and "sensitive" information systems and means "a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." OMB Circular A-130, Section 6.u.

National Security systems – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

Personally Identifiable Information (PII) - **"**means, any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of this term also incorporates by reference the definition of PII in OMB Memorandum 06-19[1] and the definition of term "Information in Identifiable Form" as defined in § 208(d)[2] of the E-Government Act of 2002, Pub. L.107-347, 116 Stat. 2899 and as further defined in OMB M 03-22.[3]

Privacy Act Record –any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Privacy and Civil Liberties Impact Assessment (PCLIA) - a PCLIA is:

(1) a *process* conducted to:
   a. identify privacy and civil liberties risks in systems, programs and other activities that maintain PII;

[1] **"**Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

[2] "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

[3] "Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)"

b. ensure that information systems**,** programs and other activities comply with legal, regulatory, and policy requirements;
c. analyze the privacy and civil liberties risks identified;
d. identify remedies, protections and alternative or additional privacy controls necessary to mitigate those risks; and
e. provide notice to the public of privacy and civil liberties protection practices.

(2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

Privacy policy in standardized machine-readable format - a statement about website privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser.

Protected Information – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

Reviewing Official - the Department or Bureau CIO or other agency head designee, who is other than the official procuring the system or who conducts the PCLIA.

Routine Use - with respect to the disclosure of a record outside of the Department of the Treasury (i.e., external sharing), the use of such record for a purpose which is compatible with the purpose for which it was collected.

Sharing –federal agency initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of government information. It does not include responses to requests for agency records under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act. It is synonymous with the term "dissemination" as used in this manual. It is also synonymous with the term "disclosure" as used in this manual unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under the Freedom of Information Act (5 U.S.C. § 552) or the Privacy Act. For National Security systems, the term "sharing" also includes the delivery of finished or raw intelligence products to consumers or customers in the intelligence community to the extent they contain PII ("dissemination" as that term is used in the Intelligence Community).

System – as the term used in this manual, includes both federal information systems and information technology.

System Developer – Treasury personnel (or a contractor) who designs, develops, and integrates a system for the system owner. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

System of Records (a/k/a Privacy Act System of Records) - a group of any Privacy Act Records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System Owner - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Section 3.0: System Overview

3.1 Purpose

The Secretary of the Treasury has administrative and financial responsibility for benefits under the District of Columbia Judges' Retirement Plan (Judges' Plan) and for benefits earned with respect to service on or before June 30, 1997, under the District of Columbia Police Officers and Firefighters' Retirement Plan (Police and Firefighters' Plan) and District of Columbia Teachers' Retirement Plan (Teachers' Plan) (all three plans collectively, the Plans). The District of Columbia has administrative and financial responsibility for benefits earned with respect to service after June 30, 1997, under the Police and Firefighters' Plan and Teachers' Plan. The Office of D.C. Pensions (ODCP) exercises the Secretary's responsibilities pursuant to a delegation of authority from the Secretary to ODCP's Director. The District of Columbia Retirement Board (DCRB) currently serves as ODCP's benefits administrator for the Police and Firefighters' Plan and Teachers' Plan. ODCP administers the Judges' Plan internally.

The System to Administer Retirement (STAR) automates the determination of eligibility, calculation of pension benefits and delivery of benefit payments under the Plans. STAR provides the capability to automatically calculate an annuitant's gross annuity payment, and for annuitants under the Police and Firefighters' Plan and Teachers' Plan whose benefits are funded by both the federal and District governments, determine the federal and District portions of benefit payments. STAR uses personally identifiable information (PII) to calculate and make benefit payments to annuitants. The data also are retrieved for actuarial purposes to determine current and future liabilities of the District of Columbia and the federal government. Earnings information is shared with the Internal Revenue Service (IRS) and state and D.C. tax offices for income tax purposes. Health and life insurance plan providers are provided information regarding premium/plan payments. Information also is shared with auditors and actuaries while performing audits and actuarial and validations of the D.C. pension funds and operations.

3.2 Authority

The Balanced Budget Act of 1997, Pub. L. No. 105-33, as amended, establishes the Secretary of the Treasury's responsibilities for the Plans described above.

Section 4.0: Information collection

Relevant and Necessary
☐ Yes ☒ No ☐ N/A Does your bureau or office exempt all Privacy Act Records used in the system or project from the relevance and necessity requirements in § 552a(e)(1)? ☒ Yes ☐ No Before collecting and maintaining the information for use in the system/project, was any assessment conducted (e.g., during Paperwork Reduction Act analysis) to determine which personally identifiable information types (see Section 4.2 below) were relevant and necessary to meet the system/project mission requirements?
☒ Yes ☐ No ☐ N/A Is the PII currently used in the system/project (see Section 4.2), limited only to that which is relevant and necessary to meet the mission requirements of the system/project?
☒ Yes ☐ No ☐ N/A Is a process in place by which the PII maintained by the system/project can be continuously reevaluated to ensure that it is limited only to that which is relevant and

necessary to meet the mission of the system/project?
Before collecting and maintaining the information for use in the STAR, ODCP determined that, at a minimum, the system must include annuitants' names, addresses, dates of birth, social security numbers, retirement data, income, payment, and health and life insurance benefit management information. For annuitants that have elected survivor or beneficiary benefits, STAR also contains beneficiary names, addresses, dates of birth, social security numbers, financial information, information regarding entitlement events, representative payees, survivor compensation, and direct deposits to bank accounts for some individuals. In preparation for updating the system of records notice and the PCLIA, ODCP reviewed the PII it maintains and confirmed that it only maintains the PII that is relevant and necessary to meet its mission.

4.2 Personally identifiable information and/or information types or groupings

Please select the appropriate boxes below to identify the types or groupings of information collected by the IT system/project. If the IT system/project uses groupings or information that are not listed below, please add them using the additional spaces provided.

Biographical/General Information Regarding Individuals		
☒ Name	☒ Gender	☒ Employee in the District of Columbia government, the federal government, and other entities upon which federal and District of Columbia benefit payments may be based. Private Sector Group/Organization Membership.
☒ Birth Date	☐ Race/Ethnicity	☒ Military Service Information
☒ Home Physical Mailing Address	☒ Citizenship	☒ Marital Status
☒ Personal Cell Number	☐ Nationality	☐ Mother's Maiden Name
☒ Personal Home Phone or Fax Number	☒ Country of Birth	☒ Spouse Information
☒ Personal e-mail address	☐ City or County of Birth	☒ Children Information
☐ Alias (including	☐ Immigration	☒ Information

nickname)	Status	about other relatives.
☒ Education Information	☐ Religion/Religious Preference	☐ References or other information about an individual's friends, associates or acquaintances.
☒ Personal Financial Information (including loan information)	☐ Passport Information	☐ Global Positioning System (GPS)/Location Data
☐ Sexual Orientation	☐ User names, avatars etc.	☐ Secure Digital (SD) Card or Other Data stored on a card or other technology
☐ Cell tower records (e.g., logs. user location, time etc.)	☐ Contact lists and directories	☐ Other (please describe) ----------
☐ Network communications data	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ Other (please describe) ----------

Identifying Numbers Assigned to Individuals	
☒ Full Social Security Number	☒ Personal Bank Account Number
☐ Truncated Social Security Number (e.g., last 4 digits)	☒ Health Plan Beneficiary Number
☒ Employee Identification Number	☐ Credit Card Number
☒ Taxpayer Identification Number	☐ Patient ID Number
☐ File/Case ID Number	☐ Vehicle Identification Number
☐ Alien Registration Number	☐ Driver's License Number
☐ Personal device identifiers or serial numbers	☐ License Plate Number
☐ Internet Protocol (IP) Address (where known to belong to an individual or unknown whether the IP address belongs to an individual or organization)	☐ Professional License Number
☐ Other (please describe):_____	

Medical/Emergency Information Regarding Individuals		
☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Patient ID Number
☐ Mental Health	☐ Disability Information	☐

Information		Emergency Contact Information (e.g., a third party to contact in case of emergency)
☐ Other (please describe): _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g. hair, eye color, weight, height, sex, gender etc.)	☐ Signatures	☐ Vascular scans
☐ Fingerprints	☐ Photos	☐ Retina/Iris Scans
☐ Palm prints	☐ Video	☐ Dental Profile
☐ Voice audio recording	☐ Scars, marks, tattoos	☐ DNA Sample or Profile
☐ Other (please describe): _____ __	☐ Other (please describe): _____ __	☐ Other (please describe): _____ _____ __

Specific Information/File Types That Include Information Regarding Individuals		
☒ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance Information
☐ Civil/Criminal History Information/Police Records	☐ National Security/Classified Information	☐ Bank Secrecy Act Information
☐ Protected Information (as defined in Treasury Directive 25-10)	☐ Case files	☐ Personnel Files
☐ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☐ Other (please describe): _____ _____

Audit Log and Security Monitoring Information

☒ User ID assigned to a user of Treasury IT	☒ Date and time an individual accesses a facility, system, or other IT	☒ Files accessed by a user of Treasury IT
☐ Passwords generated by a user of Treasury IT	☒ Internet or other queries run by a user of Treasury IT	☒ Contents of files accessed by a user of Treasury IT
☐ Video of individuals derived from security cameras	☐ Biometric information used to access Treasury facilities or IT	☐ Public Key Information.
☐ Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices	☐ Still photos of individuals derived from security cameras.	☐ Other (please describe): _____ _____

Other	
☐ Other (please describe: _____	☐ Other (please describe: _____
☐ Other (please describe: _____	☐ Other (please describe: _____

4.3 Sources of information and the method and manner of collection

In the boxes provided below, please list the sources for each personal identifier or grouping identified in Section 4.2 above. One chart must be filled out for each source. Please add columns as necessary.

SOURCES

1. **District of Columbia HR Office for Police Officers**
2. **District of Columbia HR Office for Teachers**
3. **District of Columbia HR Office for Fire Fighters**
4. **District of Columbia HR Office for Judges**
5. **Office of Pay & Retirement Service (OPRS)**
6. **DC Office of Personnel (DCOP)**
7. **Police & Fire Fighter Retirement Relief Board**

Information Acquired from this source: Personnel Information (the same information is collected from each of these sources and it is collected in the same manner)

Manner in which information is acquired from source by the Treasury project/system: (select all that apply):

☒ From a paper or electronic form provided to individuals, the public or members of a particular group

Please identify the form name (or description) and/or number (e.g., OMB Control Number):

Health Benefits Registration Form (SF 2809) OMB No. 3206-0160

Notice of Change in Health Benefits Enrollment (SF 2810)

Life Insurance Election-FEGLI (SF 2817) OMB No. 3206-0230

Designation of Beneficiary Federal Group Life Insurance (FEGLI) Program (SF 2823) OMB No. 3206-0136

Individual Retirement Record (IRR) (SF 2806)

Direct Deposit Sign-Up Form (SF 1199A) OMB No. 1510-0007 Withholding Certificate for Pension or Annuity Payments (W-4P) OMB No. 1545-0074
☒ Received in paper format other than a form.
☐ Delivered to the project on disk or other portable device and uploaded to the system.
☒ Accessed and downloaded or otherwise acquired via the internet
☒ Email
☒ Scanned documents uploaded to the system.
☐ Bulk transfer
☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☒ Fax
☒ Extracted from notes of a phone interview or face to face contact
☐ Other: Please describe: _____
☐ Other: Please describe: _____

4.4 Privacy and/or civil liberties risks related to collection

Please select the appropriate boxes below and provide narrative responses as directed in the space provided immediately below the question.

Notice of Authority, Principal Uses, Routine Uses, Effect of not Providing Information

☒ Yes ☐ No Is any of the information maintained in the system or project collected directly from an individual?

☒ Yes ☐ No Was the individual notified about the following at the point where the information was collected (e.g., in a form or on a website) (please check all boxes next to information that was provided to the individual).

☒The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.

☒ Whether disclosure of such information is mandatory or voluntary.

☒ The principal purpose or purposes for which the information is intended to be used.

☒ The individuals or organizations outside of Treasury with whom the information may be will be shared.

☒ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

No privacy and civil liberties risks were identified.

Social Security Numbers

☒ Yes ☐ No ☐ N/A Does the system or project collect or maintain Social Security numbers (SSNs)?

☒ Yes ☐ No ☐ N/A Were steps taken to eliminate the unnecessary use of SSNs and explore alternatives to the use of SSNs as a personal identifier?

☒ Yes ☐ No ☐ N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their social security account number?

☒ SSN disclosure is required by Federal statute;
☐ the SSN is disclosed to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual; or
☐ when the information is collected, individuals are given notice whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Full social security numbers (SSNs) are collected in STAR; however, annuitants are identified in STAR by their Employee ID (EMPLID) instead of their SSN. The STAR system is coded to truncate SSNs on reports, queries and other systems point that do not need the full number (e.g., routine identification of deceased annuitants, earnings and leave statements, tax forms). SSNs are also required in order to report tax withholdings on distributions under 26 U.S.C. § 6047(d).

Access to STAR is limited based on users' role. Only users in specific roles have access to SSNs. All STAR users receive annual cyber security and privacy awareness training. All STAR users are also required to read and sign STAR rules of behavior and non-disclosure statements.

First Amendment Activities

☐ Yes ☒ No Do you maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? ☒ N/A *Please check all of the following exceptions (any one of which allows the maintenance of such information) that apply :*

☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.
☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity.
☐ There is a statute that expressly authorizes its collection.

No privacy and civil liberties risks were identified

Section 5.0: Maintenance, use and sharing of the information

The following questions require a clear description of the project's or system's use of information.

5.1 Describe how and why the system/project uses the information it collects and maintains.

List all uses of the information collected and maintained, including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

STAR includes retirement service history records of employee service in the District of Columbia government, the federal government, and other entities upon which federal and District of Columbia benefit payments may be based.

The information resides in electronic and paper form at the various DC HR Offices and DC Courts. When a person retires, their personnel folder containing the forms is sent to 1) the District of Columbia Retirement Board (DCRB) as benefits administrator for the police officers, firefighters, and teachers; or 2) to ODCP as benefits administrator for the judges.

Forms are not scanned into the STAR system. DCRB and ODCP manually enter into STAR, information needed to calculate the annuitants benefit payment. A second level review of the data entered into STAR is conducted to validate that the information was entered and calculated correctly. In addition, a monthly sample size of newly processed benefit payments are quality reviewed to validate that the information was entered and calculated correctly. Annually, a sample size of benefit payments made throughout the fiscal year are audited as part of the ODCP financial audit. The hardcopy personnel folders are maintained at either DCRB or ODCP.

The forms in the personnel folder include: *The forms without OMB number (SF 2810 and SF 2806) indicates that the Paperwork Reduction Act (PRA) does not apply to those forms because the information collection on those forms are from Federal employees and not the members of the public.*

a. Health Benefits Registration Form (SF 2809) OMB No. 3206-0160
b. Notice of Change in Health Benefits Enrollment (SF 2810)
c. Life Insurance Election-FEGLI (SF 2817) OMB No. 3206-0230
d. Designation of Beneficiary Federal Group Life Insurance (FEGLI) Program (SF 2823) OMB No. 3206-0136
e. Individual Retirement Record (IRR) (SF 2806)
f. Direct Deposit Sign-Up Form (SF 1199A) OMB No. 1510-0007
g. Withholding Certificate for Pension or Annuity Payments (W-4P) OMB No. 1545-0074

The STAR system contains the name, address, date of birth, social security number, retirement data (hire data, leave of absences, salary information, contributions and termination date), income, payment, and health and life insurance benefit management information for covered employees and the name, address, date of birth, social security number for the covered employee's beneficiaries and other relatives as needed. It may also contain information regarding entitlement events, representative payees, survivor compensation, and direct deposits to bank accounts.

Information about other relatives includes name, address, date of birth, and social security number on relatives (including children) collected for health benefit purposes if annuitant is enrolled in self plus one or self and family, and information collected for survivor and beneficiary payments.

A representative payee is a person or an organization appointed by the Social Security Administration (SSA) as a payee to receive the Social Security or Supplemental Security Income (SSI) benefits for anyone who cannot manage or direct the management of his or her benefits (e.g., due to disability).

Survivor compensation includes information needed to pay a survivor benefit to the designated beneficiary of an annuitant (usually a spouse or child) upon the death of the annuitant. Children can be beneficiaries. The age limit for children to collect benefits is 18 years of age; age 22 if the child is in school. After age 22, there is no benefit to the child unless they are disabled.

Please select the appropriate boxes below and provide narrative responses as directed in the space provided immediately below the question.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them
☒ Yes ☐ No Is it possible that the information maintained by the system/project may be used by Treasury in making adverse determinations about an individual's rights, benefits, and privileges under Federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)? ☒ Yes ☐ No ☐ N/A Will Treasury share information in the system with any third party who will use the information to make adverse determinations about an individual's rights, benefits, and privileges under Federal programs? ☒ Yes ☐ No ☐ N/A Does the system/project collect information (to the greatest extent practicable) directly from the individual who is the subject of the information?
Annuitants are informed of information collected on them through several methods including their retirement benefits letter, the STAR System of Records Notice (SORN), and annual privacy notices on the annuitant earnings and leave statement. Annuitants can contact their Benefits Administrator to appeal a decision made against them by the Benefits Administrator as a result of adverse action.
Data-mining
☐ Yes ☒ No Is the system/project information used to conduct "data-mining" as defined in the Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?
No privacy and civil liberties risks were identified.

5.2 Ensuring accuracy, completeness, and timeliness of information maintained, used and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements
☐ Yes ☒ No Is all or any portion of the information used by the system or project contained in a system of records that has been exempted from any of the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) and (e)(6) of the Privacy Act?
No privacy and civil liberties risks were identified.
Computer Matching
☐ Yes ☒ No Is any of the information maintained in the project or system contained in a system of records and used as part of a computer matching program? ☐ Yes ☐ No ☒ N/A Is there a published computer matching agreement in place containing the information required in Section (o) of the Privacy Act? ☐ Yes ☐ No ☒ N/A Are assessments made regarding the accuracy of the records that will be used in the matching program? Title 552a, Section (o)(J). ☐ Yes ☐ No ☒ N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings; or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

No privacy and civil liberties risks were identified.

Merging information about individuals

☒ Yes ☐ No Is the information maintained by the system/project (whether or not a system of records or a computer matching program) compared with information from any internal or external paper or electronic sources (e.g., other files or systems) for the purpose of merging information related to a particular individual?

☒ Yes ☐ No ☐ N/A Is the information merged regarding an individual used in making adverse determinations about that individual's rights, benefits, and privileges under Treasury programs (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)?

☒ Yes ☐ No ☐ N/A Have any procedures been established for merging information derived from multiple sources (paper or electronic) that is believed to be about the same individual?[i] \

☒ Yes ☐ No ☐ N/A Have any procedures been established to address partial matches (where some, but not all of the information being merged matches an individual) during the merge process

☒ Yes ☐ No ☐ N/A Are steps taken by the system/project to ensure the accuracy, relevance, timeliness, and completeness of the merged information as is reasonably necessary to assure fairness to the individual in making the determination??

Although ODCP does not have written procedures for merging information derived from multiple sources (paper or electronic) that is believed to be about the same individual, a process is in place.

Teachers | Police | Fire Fighter process of forming "Official Retirement Record":
Specifically, the Office of Pay and Retirement Services (OPRS) creates and forwards an Individual Retirement Record (IRR) for retiring teachers, police officers and fire fighters to DCRB Benefits Department. An IRR contains salary history, service history, leave without pay status, suspension dates, taxability, and contribution information for all members of the Plans. The IRR, along with information provided by the DC Human Resource (HR) Offices and the Police and Fire Fighter Retirement Relief Board (PFRRB), are used to create the "official retirement file" for the retiring teachers, police officers and fire fighters.

The hardcopy file is reviewed against an audit checklist to ensure that all appropriate information is in the hardcopy folder before information is entered into STAR. If discrepencies are identified during the merging of the records, DCRB resolves these issues through its internal process that does not involve ODCP.

Once the information has been gathered, DCRB merges the information to create the official retirement file that includes Board Order (*Police/Fire only*), all Personnel Action Forms (PAFs) supporting service history, a retirement application (*Teachers only*), the IRR, Military Discharge Certificate (DD-214), Personnel Card (*7-Card for Teachers only*) which includes personnel actions, effective date and corresponding salary changes; evidence of purchases of creditable service, health insurance forms, life insurance forms, tax elections, direct deposit forms, and other employee personal data (e.g., military service documents and unused sick leave) necessary for processing.

Judges process of forming "Official Retirement Record":
The Judges' IRR is maintained by the Department of Interior (DOI) and forwarded to ODCP at the time the judge retirements. An ODCP Program Analyst creates the "official retirement file" using the IRR and information provided by the D.C. Courts' Human Resources Office, including all PAF supporting service history, a retirement application, DD-214s, evidence of purchases of creditable

service, health insurance forms, life insurance forms, tax elections, direct deposit forms, and other employee personal data necessary for processing, e.g. , military service documents and unused sick leave.

The hardcopy file is reviewed against an audit checklist to ensure that all appropriate information is in the hardcopy folder before information is entered into STAR. If discrepancies are identified during the merging of the records, ODCP mitigates them by reaching out to the DC Courts HR office or to the individual annuitant to confirm the correct information.

Process of checking multiple sources to identify unreported deaths:
In determining if there are unreported deaths, ODCP uses vendor death audit services: Berwyn Report, Pension Benefit Information, Inc. and the Federal Do Not Pay (DNP) system to perform a weekly review of the entire annuitant population.

Specifically, the Bureau of the Fiscal Service runs the entire annuitant population's social security numbers and dates of birth against death databases (the Social Security Administration, Berwyn Report, Pension Benefit Information, Inc., and the Federal Do Not Pay (DNP) system) for matches.

The results reported by the vendor death audit services are provided to the Benefits Administrator (DCRB or ODCP) who will terminate future payments if findings are an exact match on social security number and name. DCRB conducts additional research through internal procedures that do not include ODCP to confirm the status of the annuitant prior to terminating future payments when findings are less than an exact match. ODCP reaches out to DC Courts, researches public obituaries, and reaches out to the annuitant's beneficiary to confirm the status of the annuitant prior to terminating future payments when findings are less than an exact match.

Once future payments have been stopped, the Benefits Administrator instructs the Bureau of the Fiscal Service to recover any payments issued after death or loss of eligibility.

Ensuring Fairness in Making Adverse Determinations About Individuals

☒ Yes ☐ No ☐ N/A Are reasonable steps taken to ensure that all information maintained by the system or project that is used by Treasury to make any adverse determination about an individual's rights, benefits, and/or privileges (whether or not it is in an exempt system of records) is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?

For data being entered into STAR, we rely on the accuracy of the information from DC HR Offices and DC Courts. The DC offices obtain their information directly from the annuitant. STAR calculated/processed data is validated through ODCP's oversight and quality control process described below.

The joint ODPC/DCRB approach to quality assurance is to have pension processing and other transactions reviewed at various levels in order to ensure that activities and transactions are being properly performed and recorded. The Quality Plan will be used in conjunction with the Quality Assurance (QA) Approach. The QA Approach outlines the procedures that DCRB and ODCP follow to monitor the quality of retirement cases and benefit processing. Some cases have multiple payments and reviews occur on each of the payments. There may be multiple levels of review. The levels of review are dependent upon the type of activity.

Initially, the individual performing the transaction will review his/her own work. This is considered to be the first level of review. All tasks will have a level one review.

The second level review is conducted by a designated DCRB reviewer who will review the work performed by other DCRB staff members. All cases will have second level review in STAR and a review sheet generated by STAR will be filed in the case file to document the second level review. All second level reviews must be completed after final proration of gross is calculated. Level two review tasks include, but are not limited to, new annuitant processing, recalculations, and one-time payments.

In addition, ODCP will perform a third level review of a sample of the processing and/or transactions in order to ensure that they are being handled appropriately or to identify processes or procedures that may need to be updated or modified. ODCP performs a third level review of at least 25% of new annuitant cases. The planned reviews may be adjusted based upon findings. ODCP contractors perform additional reviews. Third level reviewers sign and date the Benefits Review Form when a review is performed by ODCP or notations are made in the Quality Review Tracking Tool if case review is performed by ODCP contractors.

A DCRB Manager or designee may also perform a third level review of a subset of all new annuitant cases to complement the review completed by ODCP.

ODCP assesses the quality findings to ensure the error rates are within tolerance levels. If they are outside of the tolerable range, ODCP analyzes the findings. If deemed warranted, ODCP increases the review population. The tolerance levels are 5% or less for monetary errors and 5% or less for all other errors.

Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

☒ Yes ☐ No Do you have any policies or standard operating procedures in place that address the accuracy, completeness, and timeliness of information used in the project or system to make any adverse determination about an individual's rights, benefits, and/or privileges (whether or not it is in an exempt system of records)?

☐ Yes ☒ No Does the project or system use any software or other technical solutions designed to improve the information accuracy, completeness, and timeliness of information used in the project or system to make any adverse determination about an individual's rights, benefits, and/or privileges (whether or not it is in an exempt system of records)?

For data being entered into STAR, we rely on the accuracy of the information from DC HR Offices and DC Courts. The DC offices obtain their information directly from the annuitant. STAR calculated/processed data is validated through ODCP's oversight and quality control process described below.

The joint ODPC/DCRB approach to quality assurance is to have pension processing and other transactions reviewed at various levels in order to ensure that activities and transactions are being properly performed and recorded. The Quality Plan will be used in conjunction with the Quality Assurance (QA) Approach. The QA Approach outlines the procedures that DCRB and ODCP follow to monitor the quality of retirement cases and benefit processing. Some cases have multiple payments and reviews occur on each of the payments. There may be multiple levels of review. The levels of review are dependent upon the type of activity.

Initially, the individual performing the transaction will review his/her own work. This is considered to be the first level of review. All tasks will have a level one review.

The second level review is conducted by a designated DCRB reviewer who will review the work performed by other DCRB staff members.All cases will have second level review in STAR and a review sheet generated by STAR will be filed in the case file to document the second level review. All second level reviews must be completed after final proration of gross is calculated. Level two review tasks include, but are not limited to, new annuitant processing, recalculations, and one-time payments.

In addition, ODCP will perform a third level review of a sample of the processing and/or transactions in order to ensure that they are being handled appropriately or to identify processes or procedures that may need to be updated or modified. ODCP performs a third level review of at least 25% of new annuitant cases. The planned reviews may be adjusted based upon findings. ODCP contractors perform additional reviews. Third level reviewers sign and date the Benefits Review Form when a review is performed by ODCP or notations are made inQuality Review Tracking Tool if case review is performed by ODCP contractors.

A DCRB Manager or designee may also perform a third level review of a subset of all new annuitant cases to complement the review completed by ODCP.

ODCP assesses the quality findings to ensure the error rates are within tolerance levels. If they are outside of the tolerable range, ODCP analyzes the findings. If deemed warranted, ODCP increases the review population. The tolerance levels are 5% or less for monetary errors and 5% or less for all other errors.

Accuracy, Completeness, Timeliness Information Received from the Source

☐ Yes ☒ No Did the bureau or office receive any guarantee, assurance or other information from any information source(s) regarding the accuracy, relevance, timeliness and completeness of the information?

The DC HR Offices collects its data directly from annuitants. The HR Offices certify the data for completeness and accuracy through an internal process that does not include ODCP, before transmitting it to DCRB.

ODCP has a quality assurance process under which it reviews at least 25% of the new annuitant cases processed by DCRB to ensure the accuracy of the information input into STAR. In addition, benefits analysts conduct and document reviews in STAR prior to payments being made.

To mitigate risk, as noted, STAR calculated/processed data is validated through ODCP's oversight and quality control process. DCRB, as the benefit administrator for the Police Officers and Firefighters' Plan and Teachers' Plan, handles its oversight and quality control process and additional research through internal procedures that do not include ODCP.

Annuitants can contact their Benefits Administrator to have their calculations reconsidered and/or to appeal a decision made against them by the Benefits Administrator.

5. 3 Information sharing within the Department of the Treasury.

Internal Information Sharing

☒ Yes ☐ No Is PII from the system/project shared with other Treasury bureaus?

☒ Yes ☐ No Does the recipient limit access to the PII shared to those Treasury officers and employees who have a need for the PII in the performance of their duties (i.e., those who have a "need to know")?

ODCP grants STAR access to the Pension Payroll group at the Bureau of the Fiscal Service, so that the Pension payroll group can execute their job duties to support benefits administration and payroll operations to process monthly benefit payments and associated tax and insurance carrier payments. This group is made up of payroll specialist, payroll analyst, supervisor, and manager.

The payroll specialist, payroll analyst and supervisor utilize STAR to:

- Process payroll payments and associated tax and insurance deductions
- Prepare third party reporting
- Split benefits reconciliation
- Debt management
- Prepare recipient 1099R forms and monthly, quarterly and annual tax filings
- Mail preparation and management

ODCP grants STAR access to the D.C. Pension Benefit Administration group within ODCP so that they can execute their job duties to process retirement and survivor benefits for members in the D.C. Judges' Retirement Plan. This group consists of two Program Analysts, a Human Resources Specialist and a supervisor. They utilize STAR to do the following, but not limited to the activities below:

- Calculate retirement benefit payments
- Calculate survivor benefit payments
- Set up health and life insurance elections
- Set up direct deposit elections
- Enter tax withholdings elections
- Perform annuitant maintenance (i.e. address changes, tax withholding changes, etc.)
- Run reports and queries
- Respond to annuitants' phone calls and correspondence

ODCP grants STAR access to the Information System Security group at the Bureau of the Fiscal Service and the ODCP STAR Technical Group within ODCP so that they can execute their job duties of developing and maintaining the STAR system. This group is made up of application developers, system, application and database administrators and technical management oversight.

- The developer has access to modify STAR system code and mitigate system processing errors, and develop and run queries and reports.
- The system, application and database administrators maintain the STAR configuration, security posture, and establish and manage all STAR user accounts.
- The ODCP Technical Group has access to audit user account profiles, run security queries and reports, track system modifications, review audit logs.

ODCP Technical Group reviews all STAR user requests for consideration and approval. All STAR users must submit a STAR Access Request Form for ODCP's review and approval before receiving access to STAR. The request forms are stored in a secure location on-site at ODCP and with the Bureau of the Fiscal Service, which is ODCP's system production support provider. ODCP requires all parties who have been granted

access to STAR information to take annual security and privacy training, as well as sign rules of behavior and non-disclosure agreements regarding the protection of STAR data.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII

☐ Yes ☒ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency or an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling or disclosure of the PII shared with Treasury?

5.4 Information sharing with external (i.e., outside Treasury) organizations and individuals.

External Information Sharing

☒ Yes ☐ No Is PII maintained by the system or project shared with agencies, organizations or individuals external to Treasury?

Accounting of Disclosures

☒ Yes ☐ No With respect to records used in the system or project that are subject to the Privacy Act of 1974, do you maintain a paper or electronic log or other record of the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made?

☐ Yes ☐ No ☒ N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to Privacy Act requests in a timely fashion?

☐ Yes ☐ No ☒ N/A With respect to records used in the system or project that are subject to the Privacy Act of 1974, do you retain the log or other record of the date, nature, and purpose of each disclosure for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?

☐ Yes ☒ No With respect to records used in the system or project that are subject to the Privacy Act of 1974, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to make the accounting available to the individual named in the record at his request?

☐ Yes ☒ No With respect to records used in the system or project that are subject to the Privacy Act of 1974, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made?

Statutory or Regulatory Restrictions on Disclosure

☐ Yes ☒ No In addition to the Privacy Act of 1974, are there any other statutory or regulatory restrictions (e.g., 26 U.S.C. § 6103 limits disclosure of tax returns and return information) on the sharing of any of the information or records contained in the system?

No privacy and civil liberties risks were identified

Memorandum of Understanding/Other Agreements Related to External Sharing

☒ Yes ☐ No ☐ N/A Does Treasury (including bureaus and offices) have an MOU or other agreement with any external, agencies, organizations or individuals with which/whom it shares PII maintained by the project or system

Memorandum of Understanding/Other Agreements Limiting Treasury's Use/Disclosure of PII

☐ Yes ☒ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency or an international agreement or treaty) that limits or places conditions on Treasury's external sharing of the PII (i.e., outside Treasury)?

Memorandum of Understanding/Other Agreements Limiting Treasury's Use/Disclosure of PII

☒ Yes ☐ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling or disclosure of PII shared by Treasury?

External Recipient's Name	DC Retirement Board	Various ODCP Contractors
Purpose of the Sharing	Annuity calculations	Calculate Actuarial Evaluations for Actuarial Reports; project work;
PII Shared	Yes	Yes
Content of Applicable Routine Use/Citation to the SORN	Federal Register / Vol. 79, No. 1 / Thursday, January 2, 2014 / Notices Treasury/DO .214 D.C. Pensions Retirement Records	Federal Register / Vol. 79, No. 1 / Thursday, January 2, 2014 / Notices Treasury/DO .214 D.C. Pensions Retirement Records
Applicable Statutory or Regulatory or Restrictions on Information Shared	The Balanced Budget Act of 1997, as amended	The Balanced Budget Act of 1997, as amended
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Providing/Originating Agency (including description of restrictions imposed on use, maintenance,	None	None

and disclosure of PII)		
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partners (including description of restrictions imposed on use, maintenance, and disclosure of PII)	**DCRB MOU and ISA.doc -** This MOU sets forth the understanding of the parties with respect to the guidelines and procedures for establishing a management agreement between ODCP and DCRB for the development, management, operation, and security of a connection between STAR, owned and administered by ODCP, and the DCRB network (DCRB LAN), the DCRB intranet, the DCRB Service History Portal, the DCRB FileNet System, and the DCRB Data Management System). In addition, this MOU sets forth the understanding of the parties with respect to the requirements for protecting STAR Personally Identifiable Information (PII). Both Parties agree to work together to ensure the joint security of the connected systems and the data they store, process, and transmit, as specified in the ISA. Each Party certifies that its respective system is designed, managed, and operated in compliance with all relevant laws, regulations, and policies. With respect to requests for STAR data, Treasury and	**Actuarial Contract.pdf –** Contract to provide the Department of the Treasury with actuary services to make actuarial determinations and reports as required by Public Law 105-33, as amended and to produce an experience study of the demographic rates used in the reports. The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software produced under this contract, shall be government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the contracting officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not

	DCRB agree to the following requirements: DCRB must provide ODCP with a statement explaining the intended use of the STAR data. This is usually provided through a request for data to the STAR Helpdesk or through a STAR Change Request that goes before the STAR Change Control Board. DCRB must provide documentation to ODCP outlining the minimum security controls including, but not limited to system encryption levels, physical security for printed media, data destruction protocols for retired servers/retired backup tapes, etc. DCRB must agree to the following limitations and constraints of sharing STAR PII with third parties: It will be the responsibility of DCRB to require the protection of the STAR data being provided to the third party. Use appropriate safeguards to prevent use or disclosure of the STAR data other than as permitted by this Agreement. DCRB must inform ODCP of how (paper,	abrogate any other government rights. The Contractor, or any entity or representative acting on behalf of the Contractor, shall not refer to the equipment or services furnished pursuant to the provisions of this contract in any news release or commercial advertising, or in connection with any news release or commercial advertising, without first obtaining explicit written consent to do so from the Contracting Officer. Should any reference to such equipment or services appear in any news release or commercial advertising issued by or on behalf of the Contractor without the required consent, the Government shall consider institution of all remedies available under applicable law, including 31 U.S.C. 333, and this contract. Further, any violation of this provision may be considered during the evaluation of past performance in future competitively negotiated acquisitions. **TIRNO-13-Z-00016 Contract.pdf** – This contract provides production support and develops and deploys new Functionality for the STAR system. ODCP

	electronic, fax, etc.), with whom, why, and the frequecy of providing STAR data to third party contractors. Changes must also be communicated to ODCP at the time of change. DCRB must review security controls in place by the third party contractors prior to storing STAR data with them (this includes off-site storage facilities not approved by the Treasury). DCRB must agree to the following criteria for observation of the security controls of the organization receiving PII from ODCP. The criteria may include one or more of the following: Observations - intended to provide ODCP with information to assess the entity's security posture (e.g. physical, network, and application) to ensure it meets ODCP's acceptable risk level. Observations may be performed by ODCP staff or tasked to contractors. Such observations may include, but are not limited to, the following: xamination of system documentation and audit findings	will leverage this contract to access supplemental resources to support maintaining and enhancing STAR. The information processed by STAR is considered to be sensitive, but unclassified data; containing personal information about individuals. As such, the Contractor is required to treat all data with confidentiality. Contract employees will be required to sign a non-disclosure agreement that outlines their responsibilities to protect the data and comply with the STAR Security Plan. The Contractor shall ensure that all applicable personnel working on this order, including subcontractors, meet the following security requirements for contractors to protect against unauthorized disclosure of Sensitive but Unclassified (SBU) data. SBU data includes, but is not limited to, information that is protected from disclosure by the Privacy Act, 5 U.S.C. § 552a. 1) All applicable personnel shall be United States citizens or have lawful permanent resident status.

	Review of any system security assessments and corrective action plans Witnessing various system functionality demonstrations Conducting physical walk-throughs of the requestors' site.DCRB must provide in its request for data, an effective date and termination date.DCRB must agree to the following conditions of term and termination. Term. The term of each data request shall commence on of the first day the data is provided to DCRB and it will terminate 1 year from Commencement Date. Should DCRB desire to keep the data request for a longer period, a justification in writing should be made to the Director of ODCP. Termination by Recipient. DCRB may terminate data requests at any time by notifying the Director of ODCP. The STAR data protection requirements outline in this MOU will still be in place for all STAR data that DCRB has obtained during the term. Termination by Covered Entity. ODCP may terminate data requests at any time by providing thirty (30) days prior	2) All applicable personnel shall be subject to a National Agency Check, Law and Credit (NACLC) investigation in accordance with the Department of the Treasury Security Manual (TD P 71-10). Applicable personnel shall not begin working on this Task Order until all security forms have been properly completed and submitted to the Contracting Officer's Technical Representative for processing, as follows: a) Completed fingerprint cards b) Non-disclosure Agreement c) Fair Credit Reporting Act Release d) SF 85-P, "Questionnaire for Public Trust Positions" 3) The Contractor shall ensure that all documentation relative to the System to Administer Retirements (STAR) be developed, processed, accessed, safeguarded, transmitted, and destroyed in accordance with TD P 71-10. 4) Applicable personnel shall wear Treasury issued identification badges when working in Government facilities. 5) Applicable personnel are prohibited from removing Treasury information and/or data

	written notice to DCRB. For Breach. ODCP shall provide written notice to Recipient within ten (10) days of any determination that DCRB has breached a material term of this Agreement. ODCP shall allow DCRB an opportunity to remedy said alleged material breach upon mutually agreeable terms. Failure to agree on mutually agreeable terms for remedy within thirty (30) days shall be grounds for the immediate termination of all data requests to DCRB.	from STAR. 6) Applicable personnel, who undergo NACLC investigations that reveal, but are not limited to, the following, may be unacceptable under this contract: conviction of a felony, a crime of violence or a serious misdemeanor; a record of arrests for continuing offenses; or failure to file or pay Federal income tax. The Government reserves the right to determine if a Contractor employee assigned to a task shall continue with the task. The Contractor shall agree to remove the person assigned within one day of official notification by the Government and provide a replacement within five days. New hires or substitutions of personnel are subject to the NACLC investigation requirement. All information collected under this contract shall be considered procurement sensitive. Contractor staff must be a United States citizen or possess alien status in the United States and be able to pass a Government background investigation, if required, by the Department of the Treasury.

		During the period of this task, access to Department of the Treasury facilities for Contractor representatives shall be granted as deemed necessary by the Government. All contractor employees whose duties under this contract require their presence at any Treasury, or Treasury Bureau facility shall be clearly identifiable by a distinctive badge furnished by the Government. In addition, corporate identification badges shall be worn on the outer garment at all times. It is the sole responsibility of the Contractor to provide this corporate identification. Upon the termination of the employment of any contractor personnel working on this task, all government furnished identification shall be returned to the issuing office. All on-site contractor personnel shall abide by security regulations applicable to that site. The contractor may be requested to sign a non-disclosure agreement regarding all deliverables and other pertinent information relative to this requirement. All information provided by the government shall be

		returned to the government at the conclusion of this contract. In addition the contractor must have provided the personnel associated with this contract, all security awareness training and all other requirements contained in the FISMA regulations, NIST guidelines and all other public law which shall include those requirements of the Federal Acquisition Regulations (FAR). All Treasury contractors are required to take annual security awareness and privacy awareness training. Classified information will NOT be made available to the contractor. Neither the contractor nor any of its employees will disclose any information specifically identified as confidential at or prior to disclosure to contractor by Treasury (the "Information") for any purpose other than in furtherance of the consulting services to be rendered by the contractor to Treasury. All retirement, personnel, and payroll records or information pertaining to specific individuals in the custody of either Treasury or the Government of the

		District of Columbia to which the contractor has access shall be treated as confidential Information. The contractor will take all steps reasonable and necessary so that the confidentiality of the Information in the contractor's possession will be maintained by it.
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/ magnetic disk/portable device/email fax/other (please describe if other)	Paper, oral discussion, portable device, email, fax.	Paper, oral discussion, portable device, email, fax.

Section 6.0: Legal compliance with Federal information management requirements

Responses to the questions below address the practical, policy and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) The Privacy Act of 1974 System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Government Act of 2002 security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

6.1 Privacy Act System of Records Notice (SORN)

For all collections of PII that meet certain requirements, the Privacy Act requires that the agency publish a SORN in the *Federal Register*.

System of Records
☒ Yes ☐ No ☐ N/A Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in Section 3.1 above) ☒ Yes ☐ No ☐ N/A Was a SORN published in the Federal Register for this system of records?
Federal Register / Vol. 79, No. 1 / Thursday, January 2, 2014 / Notices Treasury/DO .214 D.C. Pensions Retirement Records

6.2 The Paperwork Reduction Act

The PRA requires OMB approval before a federal agency may collect standardized data from 10 or more respondents within a 12 month period. The Office of Management and Budget requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the Paperwork Reduction Act, a new electronic collection of [personally identifiable information] for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

Paperwork Reduction Act Compliance
☒ Yes ☐ No Does the project or system maintain information obtained from individuals and organizations who are not federal personnel or an agency of the Federal government (i.e., outside the federal government)? ☒ Yes ☐ No ☐ N/A Does the project or system involve a new collection of information in identifiable from for 10 or more persons from outside the Federal government? ☐ Yes ☒ No ☐ N/A Did the project or system complete an Information Collection Request (ICR) for the collection and receive OMB approval?
Most of the data used in the STAR system is data obtained from various District of Columbia Human Resources offices and DC Courts. This data is used to calculate retirement benefits. Additional data is collected annually in relation to health, life elections and tax purposes. The forms collected include: a. Health Benefits Registration Form (SF 2809) OMB No. 3206-0160 b. Notice of Change in Health Benefits Enrollment (SF 2810) c. Life Insurance Election-FEGLI (SF 2817) OMB No. 3206-0230 d. Designation of Beneficiary Federal Group Life Insurance (FEGLI) Program (SF 2823) OMB No. 3206-0136 e. Individual Retirement Record (IRR) (SF 2806) f. Direct Deposit Sign-Up Form (SF 1199A) OMB No. 1510-0007 g. Withholding Certificate for Pension or Annuity Payments (W-4P) OMB No. 1545-0074

6.3 Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the National Archives for permanent retention upon expiration of this period.

NARA Records Retention Requirements
☒ Yes ☐ No Has the National Archives and Records Administration (NARA) approved a records retention schedule for the records used in the project or system
NARA retention schedule (N1-056-09-0001). Records on a claim for retirement, including salary and service history, survivor annuity elections, and tax and other withholdings are destroyed after 115 years from the date of the former police officers, firefighter's, teacher's or judge's birth; or 30 years after the date of

his/her death, if no application for benefits is received. If a survivor or former spouse receives a benefit payment, such record is destroyed after his/her death. All other records covered by this system may be destroyed in accordance with approved District and Department guidelines. Paper records are destroyed by shredding or burning. Records in electronic media are electronically erased using accepted techniques.

6.4 E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act (FISMA) Security Assessment & Authorization process is required before a federal information system may receive Authority to Operate (ATO). Different security requirements apply to National Security Systems.

Federal Information System Subject to FISMA/ Security Assessment and Authorization

☒ Yes ☐ No ☐ N/A Is the system a federal information system subject to the requirements in the Federal Information Security Act?

☒ Yes ☐ No ☐ N/A Has the system or project undergone a Security Assessment and Authorization and received Authority to Operate?

Access Controls and Security Requirements

☒ Yes ☐ No Does the system include access controls to ensure limited access to the information in the system?

Security Risks in Manner of Collection

☐ Yes ☒ No In section 4.3 above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy or civil liberties risks identified with respect to the manner in which the information is collected from the source(s

Security Controls When Sharing Internally or Externally

☒ Yes ☐ No ☐ N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal Treasury or external parties?

STAR utilizes the required controls for a moderate FISMA system.

ODCP mitigated privacy and security risks identified, e.g. through passwords,firewalls, and limited access. STAR was last re-certified and accredited May 31, 2016. Annual system test & evaluation was completed May 30, 2015 by the Bureau of the Fiscal Service, Security Branch.

Rules of behavior and/or disclosure agreements have been signed by all parties with access to STAR data. These documents outline the proper behavior in regards to handling STAR data. In addition, electronic data is encrypted as it is extracted from STAR. Although data is not encrypted at rest, the STAR databases and servers are protected through the passwords, firewalls, and limited access restrictions is in place by Fiscal Service.

National Security System

☐ Yes ☒ No Is the system a National Security system?

Monitoring of Individuals
☐ Yes ☒ No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?
Audit Trails
☒ Yes ☐ No Are audit trails regularly reviewed to ensure appropriate use, handling and disclosure of PII maintained by the project or system inside and outside of the Department?
STAR Administrators review audit trails on a regular basis. In addition, the audit trails are reviewed annually during the system assessment and ODCP's financial audit.

6.4 Section 508 of the Rehabilitation Act of 1973 Compliance

When federal agencies develop, procure, maintain or use Electronic and Information Technology (EIT), Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

Applicability of the Rehabilitation Act
☒ Yes ☐ No Will the project or system involve the development, procurement, maintenance or use of Electronic and Information Technology (EIT) as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) ("Section 508")?
Compliance With the Rehabilitation Act
☒ Yes ☐ No ☐ N/A Does the project or system comply with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities? STAR is based on Oracle/PeopleSoft's "commercial off-the-shelf" (COTS) software for human resources, pensions, and payroll administration. The components which make up the STAR system are subject to testing for accessibility using a variety of techniques including expert heuristic review, visual inspection, manual operation, and testing with various automated tools by both disabled and non-disabled users. The outcome of testing is reported using the Voluntary Product Accessibility Template (VPAT).

Section 7.0: Redress

Please select the appropriate boxes below and provide narrative responses as directed in the space labeled "*ADD explanatory responses as directed above here*"

Freedom of Information Act and Privacy Act Redress
☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek information and redress under the Freedom of Information Act and Privacy Act?
The Treasury FOIA Regulations can be found at 31 CFR Part 1, Subpart A.
Privacy Act Access Exemption
☐ Yes ☒ No Is the system exempt from the access provisions of the Privacy Act?
Additional Redress Mechanisms

☒ Yes ☐ No With respect to information maintained by the project or system, does the bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under Federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury etc.)?
For police officers, firefighters, and teachers, individuals may access their own information by requesting it from DCRB. For judges, individuals may access their own information by requesting it from ODCP. The Summary Plan Description (SPD) for each plan explains an individual's right to request copies of records. For police officers, firefighters, and teachers, DCRB and DC HR Offices have procedures in place for correcting inaccurate or erroneous information. For judges, ODCP and DC Court HR Offices have procedures in place for correcting inaccurate or erroneous information. Again, the SPD for each plan explains an individual's right to amend/correct records.