Privacy and Civil Liberties Impact Assessment
for the

Enterprise Content Management (ECM) Program System

June 17, 2016

Reviewing Official
Timothy H. Skinner
Director, Privacy and Civil Liberties Officer
Department of the Treasury
Washington DC 20220

Bureau Certifying Official
Helen G. Foster
Deputy Assistant Secretary for
Privacy, Transparency, and Records
Department of the Treasury
Washington DC 20220

Section 1: Introduction

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment ("PCLIA") when personally identifiable information ("PII") is maintained in a system or by a project. PCLIAs are required for all systems and projects that collect, maintain, or disseminate PII, regardless of the manner in which the information is retrieved.

This assessment is being completed pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget ("OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring information technology ("IT") systems or projects that collect, maintain or disseminate 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.

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/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

Section 2: Definitions

Agency – means any entity that falls within the definition of the term "executive agency"' as defined in 31 U.S.C. § 102.

Certifying Official – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

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 – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – means a program involving pattern-based queries, searches, or other analyses of one 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 that the term "disclosure" refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, "FOIA") or the Privacy Act (5 U.S.C. § 552a), 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 disclosure).

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

Federal information system – means 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.

Final Rule – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

Government information – means 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. If a question does not specifically inquire about or an issue does not clearly involve a Privacy Act system of records, the term should be given its common, everyday meaning. In

certain contexts, the term individual may also include citizens of other countries who are covered by the terms of 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. This term includes, but is not limit to, information contained in a Privacy Act system of records.

Information technology (IT) – means 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, § 6.u. This definition includes all systems that contain PII and are rated as "MODERATE or HIGH impact" under Federal Information Processing Standard 199.

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.

Notice of Proposed Rule Making (NPRM) – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as "notice-and-comment rulemaking." The agency publishes an NPRM to notify the public that the agency is proposing a rule and provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

Personally Identifiable Information (PII) –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.

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; (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.

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

Privacy Act Record – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a (a)(4).

Reviewing Official – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIAs as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

Routine Use – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

Sharing – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term "dissemination" as used in this assessment. It is also synonymous with the term "disclosure" as used in this assessment 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 FOIA or the Privacy Act.

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

System of Records – a group of any 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. 5 U.S.C. § 552a (a)(5).

System of Records Notice – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

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

Section 3: System Overview

Section 3.1: System/Project Description and Purpose

The US Department of the Treasury's Enterprise Content Management (ECM) Program provides an architectural framework to manage unstructured content/data.[1] ECM supports the use of strategies, tools, and methods to collect, store, preserve, manage, and distribute documents within an organization throughout the lifecycle of the content. ECM is based on Microsoft SharePoint and offers both Platform as a Service (PaaS) and Software as a Service (SaaS) solutions; rather than deploying software on an in-house network, users access the application and their data online. The SharePoint platform serves as enterprise collaboration and communication solution, eliminating additional investments in duplicative collaborative technologies, leveraging economies of scale, and connecting separate Bureaus/Offices through the use of the same platform in an integrated environment.

ECM creates, implements, and maintains SharePoint-based IT solutions, including the Treasury Intranet (theGreen/NGI(Next Generation Intranet)), Bureau Intranets, Collaboration Sites, Records Center (for records management), Enterprise Federation (to allow access to the ECM platform for users external to Treasury) and various shared services,. In accordance with the Office of Management and Budget (OMB) Shared First initiative, ECM provides a common platform for Treasury and non-Treasury users to collaborate with a common set of tools. The ECM Program resides within the Departmental Offices (DO), Office of the Chief Information Officer (OCIO), Enterprise Business Solutions (EBS) organization.

OCIO provides leadership to the U.S. Department of Treasury and its Bureaus in all areas of information and technology management and supports Treasury's mission by implementing strategies that improve the efficiency and performance of Treasury information technology (IT) systems and business processes. OCIO has Department-wide responsibility for the direction and development of Treasury's IT strategy, management of IT investments, and leadership of key technology initiatives. As a pillar of Treasury OCIO, EBS provides IT solutions through shared and scalable products, platforms and services. EBS offers its customers a variety of services available through four distinct product suites; ECM, Enterprise Data Management, HR Connect, and Web Solutions. Enterprise Data Management, HR Connect, and Web Solutions are all covered by separate Privacy and Civil Liberties Impact Assessments (PCLIAs).

The personally identifiable information (PII) in the ECM environment is used to identify users and their basic contact information (mailing addresses, email addresses, phone numbers). It

[1] Unstructured data is data that does not follow a specified format (e.g. text within documents, logs, survey results, e-mails).

supports the mission of the Department by providing an agency-wide technology based strategy to document capture, manage, access, integrate, measure and store information in repositories, and workflow functions to carry out its mission.

This ECM PCLIA covers the ECM platform. There are a number of services hosted on the ECM platform, developed by ECM or other programs, which are not covered by this PCLIA. The business owners of each of these services are responsible for working with their respective Privacy Office to determine if a PCLIA is required and, if so, to complete it.

This ECM PCLIA does not cover all of the possible types of PII that may be maintained in the ECM environment. More detailed information regarding the specific PII and PII types that are maintained in SharePoint (within ECM) are identified in the SharePoint PCLIA. A separate PCLIA is conducted for SharePoint because ECM users maintain PII in the SharePoint environment in order to perform their Treasury duties. The SharePoint PCLIA, therefore, sets out the minimum standard for SharePoint privacy and security requirements; Treasury Bureaus/Offices may build more detailed controls and technical enhancements into their respective sites.

Each SharePoint site contains a detailed privacy notice which discusses the policy for posting PII and how the PII can be used.

ECM hosts the services listed below:

ECM Services:

Automated Transaction and Asset Management System (ATAMS)	P4P
Briefing Book	Treasury Appointment Center
Cyber Analysis and Reporting Dashboard (CARD)	Treasury Computer Security Incident Response Center (TSCIRC)
eCase (IRS CC)	Treasury Federal Information Security Management Act (FISMA) Information Management System (TFIMS)
eCase Department of the Interior (DOI)	WebTrack
eCase Suspension and Debarment (S&D)	International Affairs (IA) Clearance Tracker (CT)
eComplaints	Office of the Assistant Secretary for Management (ASM) CT
EPM (Enterprise Portfolio Manager) Live	Legislative Affairs CT
Ethics Tracker	Privacy CT
Franchise Fund	Bureau of Engraving and Printing (BEP) CT
GoFOIA (Freedom of Information Act)	Fiscal CT
Integrated Apportionment Tracker (IAT)	Mint CT
International Affairs (IA) Financials (also referred to as IA Multi-Lateral Development Banks (IAMDB) 150 Accounts)	Exec Sec CT
OFS AMS	OCIO CT
OFS Barista	IRS SSM
OFS Services Framework	OFAC OFACIA Reorganization

SharePoint Investment Knowledge Exchange (SPIKE)	OFAC Workflow Proxy
OFM Budget Reprogramming Request Workflow	

Table 1 - ECM Hosted Services

In addition to these services, the ECM environment could potentially maintain datasets of PII not listed in this PCLIA that may have been collected, acquired, and/or used by employees in performing their Treasury duties. These PII datasets are assessed in the PCLIAs for those specific operational environments; e.g. the Office for Human Resources' HR Connect system.

PII within ECM is obtained from a variety of sources and can be (i) created by Department of the Treasury employees and contractors, (ii) submitted by individuals to the Department of the Treasury, or (iii) submitted via other Government partners.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
☐ **0 – 999**	☐ **1000 – 9,999**	☐ **10,000 – 99,999**
☒ **100,000 – 499,999**	☐ **500,000 – 999,999**	☐ **1,000,000+**

Section 3.2: Authority to Collect

The statutory authorities for operating this system or performing this project are:

ECM is used to manage general Department of the Treasury business and is authorized by 5 U.S.C. 301 (Department regulations for the operations of the department), and 31 U.S.C. 321 (General Authority of the Secretary of the Treasury).
ECM also provides for capabilities to manage and respond to Freedom of Information Act (FOIA) and Privacy Act requests, required under Freedom of Information Act, 5 U.S.C. 552 and the Privacy Act of 1974, 5 U.S.C. 552a (Records Maintained on Individuals).

Section 4: Information Collection

Section 4.1: Relevant and Necessary

The Privacy Act requires, "each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be fulfilled by statute or by executive order of the President." See 5 U.S.C. § 552a(e)(1).

The Privacy Act allows federal agencies to exempt records from the relevant and necessary requirement if certain conditions are met. This includes issuing a Notice of Proposed Rulemaking (hereinafter "NPRM") to solicit public opinions on the proposed exemption and issuing a Final Rule after addressing any concerns raised by the public in response to the NPRM. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 4.1(a) Please check all of the following that are true:

1. ☐ None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. ☒ All of the PII maintained in the system or by the project is part of a system of records and none of it is exempt from the Privacy Act relevant and necessary requirement;
3. ☐ All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;
4. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and
5. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and some of the records to which the Privacy Act applies may be exempt from the relevant and necessary requirement.

Section 4.1(b) ☒ Yes ☐ No ☐ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(c) ☒ Yes ☐ No ☐ N/A With respect to PII currently maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements

Section 4.1(d) ☒ Yes ☐ No With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement is there a process to continuously reevaluate and ensure that the PII remains relevant and necessary?

4.1.a - All of the PII maintained in the system or by the project is part of a system of records and none of it may be exempt from the Privacy Act relevant and necessary requirement.

4.1.b – To the extent possible, assessments are conducted prior to collection as part of the requirements and design phases in the ECM development lifecycle to determine which PII types were relevant and necessary to meet requirements.

4.1.c – Based on the assessments conducted as part of the requirements and design phases, the PII collected is limited to only that which is relevant and necessary to meet the system's or project's mission requirements (though there may be exceptions).

4.1. d – OCIO regularly reviews its user access processes and collections of PII to ensure the appropriate information is captured to ensure access to and security of Treasury systems.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must collect various types of information. The checked boxes below represent the types of information maintained by ECM. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – Authority to Collect.

Biographical/General Information		
☒ Name	☐ Gender	☐ Group/Organization Membership
☐ Date of Birth	☐ Race	☐ Military Service Information
☐ Home Physical/Postal Mailing Address	☐ Ethnicity	☐ Personal Home Phone or Fax Number
☐ Zip Code	☐ Personal Cell Number	☐ Alias (including nickname)
☒ Business Physical/Postal Mailing Address	☐ Business Cell Number	☐ Business Phone or Fax Number
☐ Personal e-mail address	☐ Nationality	☐ Mother's Maiden Name
☒ Business e-mail address	☐ Country of Birth	☐ Spouse Information
☐ Personal Financial Information (including loan information)	☐ City or County of Birth	☐ Children Information
☐ Business Financial Information (including loan information)	☐ Immigration Status	☐ Information about other relatives.
☐ Marital Status	☐ Citizenship	☐ Professional/personal references or other information about an individual's friends, associates or acquaintances.
☐ Religion/Religious Preference	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ 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.)	☐ Network communications data	☐ Cubical or office number
☒ Contact lists and directories (known to contain personal information)	☐ Contact lists and directories (not known to contain personal information, but uncertain)	☒ Contact lists and directories (known to contain only business information)
☐ Education Information	☐ Resume or curriculum vitae	☐ Other (please describe):
☐ ☐ Other (please describe):	☐ Other (please describe): _____	☐ Other (please describe): _____

Identifying Numbers	
☐ Full Social Security number	☐ Health Plan Beneficiary Number
☐ Truncated/Partial Social Security number (e.g., last 4 digits)	☐ Alien Registration Number
☐ Personal Taxpayer Identification Number	☐ Business Taxpayer Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Credit Card Number	☐ Business Credit Card Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Vehicle Identification Number	☐ Business Vehicle Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal License Plate Number	☐ Business License Plate Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ File/Case ID Number (individual)	☐ File/Case ID Number (business) (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Professional License Number	☐ Business Professional License Number (If known:

	☐ sole proprietor; ☐ non-sole proprietor)
☐ Employee Identification Number	☐ Patient ID Number
☐ Business Bank Account Number	☐ Personal Bank Account Number
☐ Commercially obtained internet navigation/purchasing habits of individuals	☐ Government obtained internet navigation/purchasing habits of individuals
☐ Business License Plate Number (non-sole-proprietor)	☐ Driver's License Number
☐ Personal device identifiers or serial numbers	☐ Other Identifying Numbers (please describe):_____
☐ Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)	☐ Other Identifying Numbers (please describe):_____

Medical/Emergency Information Regarding Individuals		
☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Patient ID Number
☐ Mental Health Information	☐ Disability 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		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance/Background Check Information
☐ Civil/Criminal History Information/Police Records (government source)	☐ Credit History Information (government source)	☐ Bank Secrecy Act Information
☐ Civil/Criminal History Information/Police Records (commercial source)	☐ Credit History Information (commercial source)	☐ National Security/Classified 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 or generated by 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 (e.g., web navigation habits)
☐ Passwords generated by or assigned to 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
☐ Biometric information used to access Treasury facilities or IT	☐ Video of individuals derived from security cameras	☐ Public Key Information (PKI).
☐ 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.	☒ Internet Protocol (IP) Address
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe): _____

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

Section 4.3: Sources of information and the method and manner of collection

ECM collects data including but not limited to name, contact information, demographic information, or similar data. A large portion of PII processed via ECM is not collected directly from individuals but is retrieved from other sources, including the DO Outlook Global Address Book (GAL).

The information that ECM collects directly for an individual is generally limited to name, contact information, and other similar limited data about Treasury employees and contractors used to facilitate daily business functions, as well as names and basic contact information of members of the public who have chosen to engage with Treasury. Generally, this information is collected through means such as in-person contacts or via email.

Source name: DO Outlook Global Address Book (GAL)
Specific PII identified in Section 4.2 that was acquired from this source: Name**,** Business Physical/ Postal Mailing Address, Business e-mail address, Contact lists and directories (known to contain personal information), Contact lists and directories (known to contain only business information), User ID assigned to or generated by a user of Treasury IT
Manner in which information is acquired from source by ECM: (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): _____
☐ 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: _____

Section 4.4: Privacy and/or civil liberties risks related to collection

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

When Federal agencies use a form to obtain information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on her/him, if any, of not providing all or any part of the requested information." 5 U.S.C § 522a (e) (3).

Section 4.4(a) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project collected directly from an individual? **Section 4.4(b)** ☐ Yes ☐ No ☒ N/A Was the information collected from the individual using a form (paper or electronic)? **Section 4.4(c)** ☐ Yes ☐No ☒ N/A If the answer to Section 4.4(b) was "yes," was the individual notified (on the form in which the PII was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website). ☐ 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.
4.4(b): Compliance with Privacy Act requirements is the responsibility of the system/information owner that stores the information in SharePoint or uses it in other ECM systems. Additionally, ECM provides Terms of Use for all users of SharePoint/MySites that read, in part: *"It is important to remember that all applicable laws, regulations, departmental policies, and directives for sound information management continue to apply in this environment. This includes all records management, Freedom of Information Act (FOIA), and Privacy Act requirements. Federal privacy laws, regulations, and policies apply to the*

use of SharePoint just as with any other federal government application. Department policy is to minimize the amount of Personally Identifiable Information (PII) collected and used only to that which is necessary. Offices should, therefore, be cognizant of any PII stored in SharePoint. Certain basic information about users, such as names and titles, are pre-populated on the profile page. When deciding whether to populate additional fields in the profile page, users should consider that many of these fields are PII and there are risks associated with sharing such information. While the profile page is ordinarily accessible only within the Treasury community, all information added to it is subject to public release through the FOIA, litigation, and as otherwise required by law. Accordingly, you should never post information you would not wish to have publicly available. You should not, for example, include your home or personal cell phone numbers. A photo, if you choose to upload one, must be of yourself wearing professional business attire."

Use of Social Security Numbers

Social Security numbers ("SSN") are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has the ability to harm the individual and requires more protection when used. Therefore, and in an effort to reduce risk to individuals and federal agencies, OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (May 22, 2007) required agencies to reduce the use of SSNs in agency systems and programs and to identify instances in which the collection is superfluous. In addition, OMB mandated agencies to explore alternatives to agency use of SSNs as personal identifiers for Federal employees and members of the public.

In addition, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a) (2) (A)-(B).

Section 4.4(d) ☐ Yes ☒ No ☐ N/A Does the system or project maintain SSNs?

Section 4.4(e) ☐ Yes ☐ No ☒ N/A Are there any alternatives to the SSNs as a personal identifier? If yes, please provide a narrative explaining why other alternatives to identify individuals will not be used.

Section 4.4(f) ☐ 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 SSN? If yes, please check the applicable box:

☐ SSN disclosure is required by Federal statute or Executive Order ; or

☐ 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. *If checked, please provide the name of the system of records in the space provided below.*

Section 4.4 (g) ☐ Yes ☐ No ☒ N/A When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain what means are used to provide notice.

ECM does not collect SSNs. However, due to the nature of SharePoint, users are able to set-up and post content

that includes PII, including SSNs. Detailed notice is provided by ECM to each site user on each SharePoint site on the policy for posting PII and how the PII can be used.

First Amendment Activities

The Privacy Act provides that Federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

Section 4.4(h) ☐ Yes ☒ No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment? **Section 4.4(i)** If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

☒ N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

☐ 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.
☐ N/A, the system or project does not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment.

Section 5: Maintenance, use, and sharing of the information

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

Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see Section 4.2), 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.

The personally identifiable information (PII) in the ECM environment is used to identify users and their basic contact information (mailing addresses, email addresses, phone numbers). It supports the mission of the Department by providing an agency-wide technology based strategy to document capture, manage, access, integrate, measure and store information in repositories, and workflow functions to carry out its mission. Additionally, due to the nature of SharePoint, users are able to post content that includes PII for other business reason. Detailed notice is provided by ECM to each site user on each SharePoint site on the policy for posting PII and how the PII can be used.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The Privacy Act requires that Federal agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

Section 5.1(a) ☐ Yes ☒ No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination 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)? **Section 5.1(b)** ☐ Yes ☒ No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under federal programs? **Section 5.1(c)** ☐ Yes ☐ No ☒ N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?
The information maintained in ECM is not used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations Act of 2007 ("9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy reports available at: http://www.treasury.gov/privacy/annual-reports.

Section 5.1(d) ☐ Yes ☒ No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act?
Information maintained in ECM is not used to conduct "data-mining" activities. No privacy and civil liberties risks were identified.

Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 2 above), an agency may exempt the system of records (or a portion of the records) from this requirement.

Section 5.2(a) ☐ Yes ☒ No Is all or any portion of the information maintained in the system or by the project: (a)

part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in section (e)(5) of the Privacy Act?
The information maintained in ECM is generally not exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the Privacy Act, as amended, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 5.2(b) ☐ Yes ☒ No Is any of the information maintained in the system or by the project (a) part of a system of records and (b) used as part of a matching program? **Section 5.2(c)** ☐ Yes ☐ No ☒ N/A Is there a matching agreement in place that contains the information required by Section (o) of the Privacy Act? **Section 5.2(d)** ☐ Yes ☐ No ☒ N/A Are assessments made regarding the accuracy of the records that will be used in the matching program? **Section 5.2(e)** ☐ 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?
Information maintained in ECM is not used as part of a matching program.

Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

Section 5.2(f) ☐ Yes ☒ No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?
Information maintained in ECM is not used to make an adverse determination about individuals.

Merging Information About Individuals

Section 5.2(g) ☐ Yes ☒ No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)? **Section 5.2(h)** ☐ Yes ☐ No ☒ N/A Once merged, is the information used in making determinations about individuals (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.)? **Section 5.2(i)** ☐ Yes ☐ No ☒ N/A Are there documented policies or procedures for how information is merged? **Section 5.2(j)** ☐ Yes ☐ No ☒ N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged? **Section 5.2(k)** ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?
ECM does not perform large scale, automated, analytical processes that might result in information regarding an individual being merged with information from other files or systems.

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

Section 5.2(l) ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt system of records), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information? **Section 5.2(m)** ☐ Yes ☐ No ☒ N/A Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt system of records)?
Information maintained in ECM is not used to make an adverse determination about individuals.

Accuracy, Completeness, and Timeliness of Information Received from the Source

Section 5.2(n) ☐ Yes ☒ No Did Treasury or the Bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?
Treasury did not receive any information in bulk from an original source that gave assurances regarding the accuracy, timeliness, and completeness of the information.

Disseminating Notice of Corrections of or Amendments to PII

Section 5.2(o) ☒ Yes ☐ No ☐ N/A Where feasible and appropriate, is there a process in place for

disseminating corrections of or amendments to the PII maintained in the system or by the project to all internal and external information-sharing partners? **Section 5.2(p)** ☒ Yes ☐ No ☐ N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?
There is a process in place for correcting PII in HR Connect (link) that will then be disseminated to the GAL. Notifications of corrections would be done via HR Connect, not ECM.

Section 5.3: Information sharing within the Department of the Treasury

Internal Information Sharing
Section 5.3(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with other Treasury Bureaus? **Section 5.3(b)** ☒ Yes ☐ No ☐ N/A Does the Treasury Bureau or Office that receives the PII limit access to those Treasury officers and employees who have a need for the PII in the performance of their official duties (i.e., those who have a "need to know")?
While ECM does not explicitly share PII with other bureaus, ECM is a collaborative tool, and is used throughout the Department; it also draws info from the GAL, which includes department wide info.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII
Section 5.3(c) ☐ 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 that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling, or disclosure of the PII?
PII in ECM is not subject to a MOU.

Internal Information Sharing Chart	
NOTE: ECM does not explicitly share PII with other bureaus	
Internal Recipient's Name (e.g., bureau or office)	N/A
Purpose of the Sharing	N/A
PII Shared	N/A
Applicable Statutory or Regulatory or Restrictions on Information Shared	N/A
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	N/A
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of PII Received	N/A
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	N/A

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

External Information Sharing
Section 5.4(a) ☐ Yes ☒ No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?
Information maintained in ECM is not shared with agencies, organizations, or individuals external to Treasury.

Accounting of Disclosures

Section 5.4(b) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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? *See* 5 U.S.C § 552a(c).

Section 5.4(c) ☐ 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?

Section 5.4(d) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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?

Section 5.4(e) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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?

Section 5.4(f) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, 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?

Information maintained in ECM is not shared externally.

Statutory or Regulatory Restrictions on Disclosure

Section 5.4(g) ☐ Yes ☒ No In addition to the Privacy Act, are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?

Information maintained in ECM is not shared externally.

Memorandum of Understanding Related to External Sharing

Section 5.4(h) ☐ Yes ☒ No ☐ N/A Has Treasury (including Bureaus and Offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares PII maintained in the system or by the project?

Information maintained in ECM is not shared externally.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

Section 5.4(i) ☐ Yes ☒ No 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, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its Bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?

Information maintained in ECM is not shared externally.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

Section 5.4(j) ☐ Yes ☒ No 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?

There are no MOUs between a source or recipient of information and ECM.

External Information Sharing
Section 5.4(k) ☐ Yes ☒ No Is information from the system or project shared externally?
Information maintained in ECM is not shared externally.

Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act
Section 5.4(l) ☒ Yes ☐ No ☐ N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))?
Information maintained in ECM is not disclosed.

Section 6: 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 System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 6.1: Privacy Act System of Records Notice (SORN)

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

System of Records
Section 6.1(a) ☒ Yes ☐ No 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 4.2 above) **Section 6.1(b)** ☒ Yes ☐ No ☐ N/A Was a SORN published in the *Federal Register* for this system of records?
• DO .007—General Correspondence Files. • Treasury .017—Correspondence and Contact Information

Section 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. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Paperwork Reduction Act Compliance
Section 6.2(a) ☐ Yes ☒ No Does the system or project 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)?

Section 6.2(b) ☐ Yes ☐ No ☒ N/A Does the project or system involve a new collection of information in identifiable form for 10 or more persons from outside the federal government?

Section 6.2(c) ☐ Yes ☐ No ☒ N/A Did the project or system complete an Information Collection Request ("ICR") and receive OMB approval?

ECM does not obtain information from individuals and organizations who/that are not federal personnel or an agency of the federal government.

Section 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 NARA for permanent retention upon expiration of this period.

NARA Records Retention Requirements
Section 6.3(a) ☒ Yes ☐ No Are the records used in the system or by the project covered by NARA's General Records Schedules ("GRS") or Treasury/Bureau Specific Records Schedule (SRS)? **Section 6.3(b)** ☒ Yes ☐ No Did NARA approve a retention schedule for the records maintained in the system or by the project? **Section 6.3(c)** ☐ Yes ☐ No ☒ N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA's GRS or Treasury/Bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?
For DO organizations using the ECM SharePoint platform, records are covered under the Departmental Offices (DO) Functional Schedule, N1-056-03-010. Bureau organizations apply equivalent retention schedules. Retention of records in the SharePoint environment is consistent with the approved retention schedule for the original records collection. SharePoint is an extension of the systems that use it. Therefore the retention schedules applicable to records in particular systems or IT solutions control the records, both inside and outside the SharePoint site. In-place records management functionality allows records to be managed in the same SharePoint library as non-records, while maintaining appropriate security and dispositions for records. This functionality allows temporary records with short dispositions to live out their entire lifecycle in-place; they never need to reach Records Center because they can be effectively and securely managed in-place. Records Center is a specially configured SharePoint site set up for the long-term and secure storage of permanent and long-term temporary records while ensuring accessibility. When a record is moved to Records Center, it is assigned to a library and folder based on the record's disposition schedule and maintained in the folder until its final disposition. SharePoint users have the primary responsibility to apply the foregoing records management features – and, as a threshold matter, identify and apply the records schedule(s) that is most appropriate to the records they maintain in SharePoint. However, in the absence of a specific records schedule identified by the SharePoint user, data in the SharePoint environment will be managed under the Departmental Offices (DO) Functional Schedule (number N1-056-03-010), in particular item 1.b. (materials documenting Treasury program management functions). Departmental Offices will work with the Treasury Bureaus to identify comparable (i.e. general program management) records schedules to apply to Bureau data that would not otherwise be

scheduled in SharePoint."

Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act ("FISMA") Security Assessment & Authorization (SA&A) 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
Section 6.4(a) ☒ Yes ☐ No ☐ N/A Is the system a federal information system subject to FISMA requirements? **Section 6.4(b)** ☒ Yes ☐ No ☐ N/A Has the system or project undergone a SA&A and received ATO?
The ECM Platform is currently undergoing a new SA&A.
Access Controls and Security Requirements
Section 6.4(c) ☒ Yes ☐ No Does the system or project include access controls to ensure limited access to information maintained by the system or project?
Access Controls are provided through the use of SharePoint Security Groups. The group permissions can be managed either Out-of-the-Box or via the SharePoint Admin Users module. Permissions are managed by system owners who are members of the Administration Group, who can manage permissions and add/remove users from system.
Security Risks in Manner of Collection
Section 6.4(d) ☐ 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)?
For ECM, no security, privacy, or civil liberties risks were identified with respect to the manner in which the information stored by ECM is collected from sources.
Security Controls When Sharing Internally or Externally
Section 6.4(e) ☐ 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 or external parties?
No information is transferred from ECM to internal or external parties.

Monitoring of Individuals
Section 6.4(f) ☐ Yes ☒ No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?
ECM does not have the capability to identify, locate, and monitor individuals or groups of people.

Audit Trails
Section 6.4(g) ☒ Yes ☐ No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?
Audit trails are regularly reviewed for appropriate use and handling of PII maintained in ECM.

Section 6.5: Section 508 of the Rehabilitation Act of 1973

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 and Compliance With the Rehabilitation Act
Section 6.5(a) ☒ Yes ☐ No Will the project or system involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)? *The Rehabilitation Act is not applicable* **Section 6.5(b)** ☒ Yes ☐ No ☐ N/A Does the system or project 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?
ECM complies 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.

Section 7: Redress

Access Under the Freedom of Information Act and Privacy Act
Section 7.0(a) ☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek records under the Freedom of Information Act and Privacy Act?
The Treasury/Bureaus FOIA and PA disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.

Privacy Act Access Exemption
Section 7.0(b) ☐ Yes ☒ No Was any of the information that is maintained in system of records and used in the system or project exempted from the access provisions of the Privacy Act?

Additional Redress Mechanisms
Section 7.0(c) ☐ Yes ☒ No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), 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)?
ECM does not 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).