

Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions


Review the following steps to complete this questionnaire:

- 1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.
- 2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.
- 3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.
- 4) Save/Exit the Questionnaire.** You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA Name:	OS - MTTs-C - QTR1 - 2025 - OS2325154	PIA ID:	2738482
Name of Component:	OS - OS - OS - HHS OGC Matter and Time Tracking Cloud System	Name of ATO Boundary:	HHS OGC Matter and Time Tracking Cloud System
Overall Status:		PIA Queue:	
Submitter:		# Days Open:	41
Submission Status:	Submitted	Submit Date:	2/14/2025
Next Assessment Date:	N/A	Expiration Date:	3/10/2028
Office:		OPDIV:	OS
Security Categorization:	Moderate	OpDiv PIA ID:	OS2325154
Legacy PIA ID:		Make PIA available to Public?:	No
1:	Identify the Enterprise Performance Lifecycle Phase of the system.		Operations and Maintenance
2:	Is this a FISMA-Reportable system?		Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		Yes
4:	ATO Date or Planned ATO Date.		3/4/2025
5:	Is the system or electronic information collection, agency or contractor operated?		Agency

PTA

PTA		
PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	Microsoft Dynamics CRM updated from 2016 to 2019. Microsoft Sharepoint On Prem (For OGC Intranet) updated from 2016 to 2019
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:

Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.

Matter and Time Tracking System - Cloud (MTTS-C) is a centralized cloud based system that enables a sophisticated analysis of current & projected workloads across the Office of the General Counsel (OGC); provides a robust data capture, workflow, timekeeping & reporting solution that enables better strategic planning & performance-based budgeting.

MTTS-C is a modernization of the legacy OGC Case Management system. Modernization of the system enables it and OGC to fulfill and satisfy OGC's Information Technology (IT) Records Management Lifecycle requirements. The requirements cover the

lifecycle of a record from Records Creation to Records Management and Use to Records Disposition. These core requirements include other workflow and records management activities such as virtual work collaboration, document management, case management, records Management, e-Discovery, as well as others.

Additionally, MTTS-C hosts the Electronic Financial Disclosure System (EFDS) application which allows employees who are required to submit an annual financial disclosure report to submit electronically to ethics officials pursuant to 5 C.F.R. 2634 and the Ethics In Government Act of 1978 (as amended). EFDS is considered a child application of MTTS-C and

operates under the same ATO.

PTA - 5:

List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.

Currently, MTTTS-C is predominantly being used to plan workloads. It contains case file numbers and hours assigned to those cases. It has the capacity to upload information. MTTTS-C stores all documents related to cases, including notes, case development information, legal research, correspondence, pleadings, evidence, court calendars, task lists, statutes of limitations and other critical deadlines, time and expense entries, budgets, and e-mails. Information in the system may include personally identifiable information (PII). Information includes the names of attorneys, contractors, paralegals, and other legal staff assigned to particular cases. Uploaded materials may contain virtually any relevant information, including PII of the litigants, witnesses, judges, or other stakeholders. Direct contractors have access to the system. Both direct contractors and federal employees utilize HHS credentials to access the system. User credentials are not stored within the system. OGC attorneys, paralegals, legal and IT support staff have access to case information. All PII is collected by the client Operating Divisions (OPDiv)/Staffing Divisions(StaffDiv), then provided to OGC for legal use. Types of PII may include Social Security Number, Date of Birth, Name, Biometric Identifiers, Mother's Maiden Name, e-mail address, mailing address, phone numbers, medical notes, medical records number, financial account info, certificates, legal documents, education records, military status, employment status, or taxpayer ID. Categories of individuals may include Employees, Public Citizens, Business Partners/Contacts (Federal, state, local agencies). The EFDS application collects information regarding a filer's assets, earned income, liabilities, outside positions, agreements or arrangements, and gifts and travel reimbursements. According to the Office of Government Ethics, the purpose of the financial disclosure system is to prevent conflicts of interest and to identify potential conflicts by providing for a systematic review of the financial interests of both current and prospective employees. Types of PII that EFDS may collect can include Name, E-mail address, phone numbers, mailing address, financial account info, and employment status. Each data point above will be maintained in the system for a period of 6 years from the date of filing. After the 6 year retention period as expired - unless there is a reason to maintain the records for a longer period (i.e. investigation or directed by Congress) - the records will be purged from the system.

PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is
PTA - 5B:	Please identify the type of user credentials used to access the system.	
PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	<p>MTTS-C is used to record the hours each attorney works on assigned cases, or is predicted to work on individual cases in the future. It also has the capacity to upload documents related to specific cases including notes, case development information, legal research, correspondence, pleadings, evidence, court calendars, task lists, statutes of limitations and other critical deadlines, time and expense entries, budgets, and e-mails. Because the system has the capacity to upload documents, any PII relevant to a case may appear in a case document. Types of PII may include Social Security Number, Date of Birth, Name, Biometric Identifiers, Mother's Maiden Name, e-mail address, mailing address, phone numbers, medical notes, medical records number, financial account info, certificates, legal documents, education records, military status, employment status, or taxpayer ID. Categories of individuals may include Employees, Public Citizens, Business Partners/Contacts (Federal, state, local agencies).</p> <p>EFDS collects information that is only required to be reported on the Confidential Financial Disclosure Report (Office of Government Ethics 450 (OGE 450)) pursuant to 5 C.F.R. 2634 and the Ethics In Government Act of 1978 (as amended). The system will collect an employee's name, position title, grade, official mailing address, official phone number, and official e-mail address. Additional information that is collected is an employee's financial holdings including Assets, Earned Income, Liabilities, Outside Positions, Agreements/Arrangements, Gifts and Travel Reimbursements. Types of PII that EFDS may collect can include Name, E-mail address, phone numbers, mailing address, financial account info, and employment status.</p>
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No

PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	<p>MTTS-C hosts three URL's for internal HHS use only:</p> <p>https://ogcintranet.hhs.gov - OGC Intranet site used for information dissemination for OGC personnel only.</p> <p>https://ogccms.hhs.gov - Time Records and Client System (TRACS) - A resource for OGC personnel to record hours on cases, and a database of matters worked on across OGC.</p> <p>These two URL's can only be accessed through an HHS issued laptop on the HHS network (or via VPN) by utilizing the Active Directory network credentials of each user (ITSC account).</p> <p>https://efds.hhs.gov/ - A digital version of Ethics Financial Disclosure Forms OGE 450 and the Outside Activities Reporting System. This URL is only accessible through HHS issued laptops on the HHS network (or via VPN) by utilizing PIV card through AMS authentication. This site is accessible across HHS.</p>
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	Yes
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	
PTA - 17:	Does the mobile application contain links to non-federal government websites external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	

PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA		
PIA		
PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Name Mother Maiden Name Email Address Phone numbers Medical records (PHI) Certificates Education Records Military Status Taxpayer ID Date of Birth Biometric Identifiers Mailing Address Medical Records Number Financial Account Info Legal Documents Employment Status
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000

<p>PIA - 4:</p>	<p>For what primary purpose is the PII used?</p>	<p>Employee information is used to manage caseloads and to track time associated to a case and client. Other PII may be kept as a part of the repository of legal case materials.</p> <p>For Electronic Financial Disclosure System (EFDS), the primary purpose for which personally identifiable information (PII) is used is to identify each employee filed record and allow for ethics officials to contact said employee using their official contact information as provided in the system if there are questions regarding an employee's filed form. If any personal information (i.e. personal home address, personal phone numbers, personal email) are provided on the form, the employee is directed to replace that information with the official information of the organization to which they are assigned. Additionally, what is known as PII for purposes of the Office of Government Ethics (OGE) 450, an employee is required to provide the same information on the hardcopy of the OGE 450 if an employee chooses to file hardcopy.</p> <p>According to the Office of Government Ethics, the primary purpose of the use of the various financial information is to prevent conflicts of interest and to identify potential conflicts by providing for a systematic review of the financial interests of both current and prospective employees.</p>
<p>PIA - 5:</p>	<p>Describe any secondary uses for which the PII will be used (e.g. testing, training or research).</p>	<p>N/A</p>
<p>PIA - 6:</p>	<p>Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.</p>	<p>Although the Social Security Number (SSN) and Taxpayer ID have no specific function within Matter and Time Tracking System Cloud (MTTS-C), they may be included as part of a legal document. The primary purpose of MTTS-C is not to collect SSN's or Taxpayer ID's.</p> <p>EFDS does not collect SSN's or Taxpayer ID's</p>

PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	<p>The SSN and Taxpayer ID have no specific use within MTTS-C but may be included as part of a legal document. The primary purpose of MTTS-C is not to collect SSN's or Taxpayer ID.</p> <p>Any basis for Office of the General Counsel (OGC) to possess SSN information derives from a request for legal advice on an Health and Human Services (HHS) program statute that authorizes the collection of SSN information, and only then, if the program office provides the information as part of its request. Legal authority derives from E.O. 9397. While MTTS-C doesn't solicit the SSN directly, It does maintain legal and financial documents that may contain the SSN.</p> <p>No individual will be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN. See Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (1974) (codified at 5 U.S.C. § 552a)</p>
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	<p>The authority for maintaining MTTS-C are the various statutes, regulations, rules or orders pertaining to the subject matter of the litigation, administrative complaint or adverse personnel action, (e.g., Public Health Service Act; Social Security Act; Civil Rights Act; Federal Food, Drug and Cosmetic Act; Federal Tort Claims Act, 28 U.S.C. 2671-2680, 1346(b); Waiver of Overpayment of Pay Act, 5 U.S.C. 5584; Military Personnel and Civilian Employees Claims Act, 31 U.S.C. 240-243; Federal Claims Collection Act, 31 U.S.C. 951-953; and Federal Medical Care Recovery Act, 42 U.S.C. 2651-2653).</p> <p>For EFDS, the legal authorities are 5 C.F.R. 2634 and the Ethics In Government Act of 1978 (EIGA)</p>
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	

PIA - 9:	Identify the sources of PII in the system.	<p>Directly from an individual about whom the information pertains</p> <ul style="list-style-type: none"> Hard Copy Mail/Fax Email Online <p>Government Sources</p> <ul style="list-style-type: none"> Within the OPDIV Other HHS OPDIV <p>Non-Government Sources</p> <ul style="list-style-type: none"> Members of the Public Private Sector
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	For EFDS, it is OMB No. 3209-0006. MTTTS-C does not require OMB information collection approval.
PIA - 10B:	Identify the OMB information collection approval number expiration date.	8/31/2027
PIA - 10C:	Explain why an OMB information collection approval number is not required.	
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	

PIA - 13:

Describe the method for notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Since EFDS collects the necessary information to complete the Confidential Financial Disclosure Report (OGE 450) (either electronically using EFDS OR filing a hardcopy of the OGE 450), there is not an opportunity to provide either an opt-in or opt-out for what is considered PII for purposes of the Privacy Impact Assessment (PIA). EFDS does not connect to or transmit information to other systems (internal or external). Additionally, the information is required so that an employee may be cleared of any potential conflict of interest with his/her employment with HHS. For employees of HHS, consent to use their names is implicit in the employer/employee relationship. Individuals who seek OGC's assistance in legal matters consent implicitly to the retention of their PII by virtue of requesting OGC to investigate, advise, and/or litigate matters. Others do not consent, but use of their PII may be necessary to pursue adversarial investigations and litigation. Employees, complainants, defendants, and other stakeholders become aware of how their information is used in the course of OGC conducting its duties. As necessary and required by laws and regulations, individuals are contacted to inform them of their role in litigation or other legal matters, and they learn at that time how their information may be used.

PIA - 14:

Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.

If a change is issued by Regulation, then a change will need to occur in the EFDS system. If a major change occurs in the EFDS system, users will be notified by e-mail or in person training session. Significant changes to the uses or scope of the information held in the EFDS system will be published in the Federal Register by the Office of Government Ethics as an amendment to the system of records notice for the governmentwide system of records OGE/GOVT-2, Executive Branch Confidential Disclosure Reports.

No major changes to the system that would affect the rights or interests of the individuals are expected. If such changes were made, individuals that were employees of HHS would be informed through some combination of e-mail, phone calls, through user manuals or training, through newsletters, or supervisors.

Submission of PII is voluntary as a part of individual seeking OGC's assistance in resolving a legal matter.

If the matter involves other, external parties (MTSC

may be used to store information related to the case including information about defendants), consent is not sought because it is required for participation in a legal action.

PIA - 15:

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not.

If an individual feels that their PII has been used or disclosed inappropriately, they are able to file a complaint directly with the Office of the General Counsel and the matter will be researched and resolved.

For EFDS, if an individual has a concern with their PII, they may contact their Designated Agency Ethics

Official. The Ethics Official may elevate the issue to the HHS Computer Security Incident Response Center (CSIRC), if necessary. Individuals must furnish

sufficient information for their records to be located

and identified, and must comply with OGE Privacy Act regulations regarding verification or identity and

access to records. Individuals may contest information in the records in accordance with HHS Privacy Act regulations at 45 C.F.R. Part 5b.

Individuals concerned about misuse of their information may contact the HHS Designated Agency Ethics Official or the HHS Privacy Advocate to voice such concerns. The agency may only use and disclose the information in the system as allowed by the Privacy Act. Unauthorized use of information in the system may result in civil or criminal liability.

PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not.	<p>The system undergoes a quarterly check of its security protections pursuant to HHS policy. Also, the information is updated as required as the events related to a case develop.</p> <p>Any documents stored in MTTTS-C are considered records and therefore cannot be altered after the case they are assigned to is closed. Records follow the Office of Management and Budget (OMB) and HHS Records Schedules.</p> <p>For EFDS, when a filer submits the OGE 450, there are two levels of verification it must go through. An Ethics Official, and then a Certifying Official will review the data submitted and alert the filer to any inaccuracies or changes. Annual filers must resubmit the OGE 450 each year, thus ensuring the data's integrity, availability, accuracy, and relevancy. Disputes between the agency and subject individuals regarding the accuracy of information in the system is unlikely as a general matter, because all substantive information in the system is self-reported by the subject individual.</p>
PIA - 17:	Identify who will have access to the PII in the system.	<p>Users</p> <p>Administrators</p> <p>Developers</p> <p>Contractors</p>
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	<p>Users - Filers can access their own PII in the required OGE 450 form. OGC employees can track their workload, track progression of events in a case, and access information about a case</p> <p>Administrators - For EFDS, reviewers confirm the data entered by Filers. Certifiers verify the filer is in compliance with applicable laws and regulations except as otherwise noted. For MTTTS-C administrators can perform user account maintenance and workflow management.</p> <p>Developers - For MTTTS-C, they perform enhancements and adjustments for new user groups</p> <p>Direct Contractors - perform site administration</p>

<p>PIA - 19:</p>	<p>Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>For EFDS, several security roles (Filer, Reviewer, Administrator) are implemented that determine whether a user is able to view PII, view/edit PII, or view/edit/remove PII.</p> <p>For MTTs-C several security roles (System Administrator, Basic User, Member) are implemented that determine whether a user is able to view PII, view/edit PII, or view/edit/remove PII. Security roles are assigned based on the user's current role.</p>
<p>PIA - 20:</p>	<p>Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.</p>	<p>For EFDS, the system ensures that Filers only access their own PII, while Reviewers are qualified OGC Ethics Personnel required to confirm the data entered into the OGE 450 form.</p> <p>For MTTs-C, a user's security role is based on the job performed. If a user does not have need of access for a case, they are not a member of the team that is assigned to the case, and are unable to access the case file.</p>
<p>PIA - 21:</p>	<p>Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.</p>	<p>Every user level of the EFDS system (Administrators, Reviewers, Certifiers, and Filers) are required to complete the Department's PII annual training per Office of the Chief Information Officer (OCIO) directive. Additionally, when users are initially trained on the system and periodically reminded during the review process, they are reminded of the non-disclosure of PII to unauthorized personnel.</p> <p>All OGC users (federal and contractor) are required to complete annual security awareness training and privacy awareness training.</p>
<p>PIA - 22:</p>	<p>Describe the training system users receive (above and beyond general security and privacy awareness training).</p>	<p>Every user level of EFDS is required to complete the Department's PII annual training. Administrators, Reviewers, and Certifiers are trained on an annual basis on the EFDS system either in person; or teleconferences; or online on annual basis. Each user is reminded of their obligation as Ethics Officials not to disclose PII information to unauthorized individuals. Additionally, they are reminded of their obligations to remove (or instruct a filer to remove) information that is not required to be entered on the OGE 450. Before a new filer uses the system, the administrator or reviewer/certifier will provide a level of training so that the necessary information is provided on the OGE 450. OGC conducts annual training with all users on how to secure and maintain PII in MTTs.</p>

PIA - 23:

Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).

OGC uses a manual process to eliminate information that is out of date or no longer needed following the OMB and HHS document and record retention and disposition rules.

Administrative Hearing Files, Disposition Authority Number: DAA-0468-2012-0009-0001

Legal Advice and Opinions on Significant Issues, Disposition Authority Number: DAA-0468-2012-0009-0002

Legal Advice and Opinions on Non-Significant Issues, Disposition Authority Number: DAA-0468-2012-0009-0003

FDA Injunction Files, Disposition Authority Number: DAA-0468-2012-0009-0004

FDA Suit Files with Precedential Value, Disposition Authority Number: DAA-0468-2012-0009-0005

FDA Suit Files without Precedential Value, Disposition Authority Number: DAA-0468-2012-0009-0006

HHS Draft Legislation Files, Disposition Authority Number: DAA-0468-2012-0009-0007

Non-HHS Draft Legislation Files, Disposition Authority Number: DAA-0468-2012-0009-0008

Numbered Bill Files, Disposition Authority Number: DAA-0468-2012-0009-0009

Public Law Files, Disposition Authority Number: DAA-0468-2012-0009-0010

Military Personnel and Civilian Employees Claim Files, Disposition Authority Number: DAA-0468-2012-0009-0011

Federal Claims Collection Act Files, Disposition Authority Number: DAA-0468-2012-0009-0012

Administrative Tort Claims Files, Disposition Authority Number: DAA-0468-2012-0009-0013

Federal Medical Care Recovery Act Claims Files, Disposition Authority Number: DAA-0468-2012-0009-0014

Office of the General Counsel Working Papers, Disposition Authority Number: DAA-0468-2012-0009-0015

Testimony Requests and Document Production Records, Disposition Authority Number: DAA-0468-2012-0009-0016

Health Resources and Services Administration's Bureau of Clinician Recruitment Service (BCRS) Scholarship and Loan Repayment Program Attorney Case Files, Disposition Authority Number: DAA-0468-2012-0009-0017

Litigation Case Files with Precedential Value, Disposition Authority Number: DAA-0468-2012-0009-0018

Litigation Case Files without Precedential Value, Disposition Authority Number: DAA-0468-2012-0009-0019

For EFDS, each data point will be maintained in the system for a period of 6 years from the date of filing in accordance with the Office of Government Ethics retention schedule as cited in 5 C.F.R. §§

2634.603(g)(1) and 2634.604. After the 6 year retention period has expired - unless there is a reason to maintain the records for a longer period (i.e. investigation or directed by Congress) - the records will be purged from the system.

PIA - 24:

Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.

The following administrative, technical, and physical

controls are in place for MTTs-C and EFDS :

Administrative Controls:

Certification and Accreditation

System Security Plan

Contingency (or Backup) Plan

File Backup

Backup Files Stored Offsite

User Manuals

Contractor Agreements

Least Privilege Access

Retention and Destruction Practices

Technical Controls:

User Identification and Passwords

Firewall

Intrusion Detection System (IDS)

Security Incident Response Plan

Virtual Private Network

Smart Cards

Physical Controls:

Guards

Identification Badges

Key Cards

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	2/14/2025
Privacy Analyst Comments:	Vanessa, this PIA is ready for your review. All necessary questions have been answered. Thank you, Jon	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	
SOP Comments:		SOP Review Date:	2/20/2025
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	2/25/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale 2/25/2025 Previous comments have been addressed. Submit for SAOP review and approval. 2/6/2025 Please see comments and update accordingly: PIA-6: Please explain the function of the taxpayer ID. PIA-6A: Please cite E.O.9397 within your response. While the system doesn't solicit the SSN directly, It does maintain legal and financial documents that contain the SSN.	Agency Privacy Analyst Days Open:	5

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	Archer Signature_Bridget Guenther.docx
SAOP Comments:		SAOP Review Date:	3/11/2025
		SAOP Days Open:	14

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 6	BLAND, CRYSTAL	2/6/2025	Please explain the function of the taxpayer ID.	
PIA - 6A	BLAND, CRYSTAL	2/6/2025	Please cite E.O.9397 within your response. While the system doesn't solicit the SSN directly, It does maintain legal and financial documents that contain the SSN.	
PIA - 6	Data Feed Service, piafrmos_Release	2/14/2025	Added further clarification about SSN and Taxpayer ID	
PIA - 6A	Data Feed Service, piafrmos_Release	2/14/2025	Cited legal authority EO 9397 and added further clarification	

Admin Section			
Is OpDiv Privacy Analyst Approved ?:	1	Is OpDiv Privacy Analyst Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	Is SOP Return ?:	0
Is SAOP Approved?:	1	Is Agency Privacy Analyst Return ?:	0
Total Approved:	4	Is SAOP Return ?:	0
Total Approval Required:	4	Total Return:	0

Miscellaneous Fields	
Last Updated:	3/11/2025 9:50 AM
History Log:	View History Log