UNITED STATES TRUSTEE PROGRAM

Privacy Impact Assessment
for the
Enterprise Bankruptcy Management Application

Issued by:
Lisa A. Tracy, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: September 29, 2020

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The United States Trustee Program (USTP) currently maintains twelve separate information systems, as defined by 44 U.S.C. § 3502. It also maintains several applications and data collections that are stored on servers connected to the USTP's Justice Consolidated Network (JCON), which is the platform on which all of the USTP's servers and systems reside. The USTP proposes to implement a new information system, the Enterprise Bankruptcy Management Application (EBMA) to eliminate obsolete systems, integrate remaining systems, improve user capabilities to accomplish daily operations more efficiently, and enhance security and privacy safeguards. EBMA will receive the following data from the Case Management and Electronic Case Filing (CM/ECF) system (maintained by the United States Bankruptcy Courts) through a download called Data Exchange for Trustees (DXTR):

- Bankruptcy case numbers, business and individual debtor names;
- Social security numbers, tax identification numbers, addresses, attorney, and creditor information;
- Trustee and judge assignments, court filings (e.g., orders, pleadings, reports);
- Means testing and debtor audit data;
- Fees paid to professional service providers;
- Quarterly fees paid by Chapter 11 debtors pursuant to 28 U.S.C. § 1930(a)(6);
- Financial information including income, expenses, debts and whether individual debtors are current on any domestic support obligations;
- Information for use in evaluating criminal referrals to the United States Attorney;
- Information about private trustees assigned to administer bankruptcy cases;
- Financial information contained in required periodic and final reports, including reports required under the recently enacted Small Business Reorganization Act; and
- Information about credit counseling and debtor education providers.

EBMA will also integrate information the USTP collects and maintains about its personnel, including time spent on certain activities in bankruptcy cases (see description of the internal timekeeping system below). EMBA will not, however, include documents maintained in employees' personnel folders, such as performance appraisals, performance work plans, and disciplinary actions.

The USTP conducted a Privacy Impact Assessment to identify potential risks and effects of collecting and maintaining personally identifiable information (PII) in EBMA, to evaluate protections and mitigation efforts related to those risks, and to ensure that appropriate privacy protections are built into the system at the design phase and continue to safeguard PII throughout the EBMA life cycle.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The USTP oversees the administration of approximately one million bankruptcy cases filed annually throughout 88 federal judicial districts. To ensure the integrity of the bankruptcy system, the USTP carries out a broad range of administrative, regulatory, and enforcement activities, and relies on its information systems and technology to carry out its mission. The USTP has outgrown its current IT environment, which no longer provides many of the system functions needed to fulfill mission. Among other inefficiencies, employees must re-enter the same data in multiple disparate applications that do not share data. This duplicative data entry creates the potential for error and uncertainty as to its source and accuracy. EBMA will modernize operations and cut costs, utilizing an "Agile" methodology that incrementally replaces obsolete systems and integrates others on the Microsoft Azure GovCloud platform, which has been FEDRAMP certified.

To accomplish this modernization, the following information systems will be integrated into EBMA and then retired:

- Automated Case Management System (ACMS): ACMS is the main information system supporting the USTP's mission. All bankruptcy case information is collected daily from the CM/ECF system through DXTR. Through encrypted and secure transmissions, ACMS receives both XML files containing court document information, and PDFs of filed documents. Core case data is then shared with the other systems (CETS, SARS, DAS, FICS, and TUFR, as defined below). While the majority of data originates from DXTR, USTP staff also provide critical information. ACMS has an Authority to Operate certificate (ATO) that expires on November 30, 2021.
- Criminal Enforcement Tracking System (CETS): CETS is the information system USTP employees use to track and manage criminal enforcement efforts, including preliminary investigations, to refer matters to the appropriate law enforcement authorities, including the United States Attorney, and to record final dispositions of the enforcement matters. USTP employees also track efforts in assisting law enforcement with cases already under criminal investigation. CETS has an ATO that expires on December 1, 2021.
- Credit Counseling/Debtor Education (CCDE): CCDE facilitates the USTP's statutorily mandated duty to approve and manage entities seeking to provide credit counseling or debtor education services. USTP employees with oversight responsibilities for CCDE record and track application information, review decision-making processes, conduct quality of service reviews, and monitor and respond to complaints. CCDE has an ATO that expires on August 15, 2021.
- Certificate Generating System (CGS): CGS is the means by which approved providers of credit counseling or debtor education services generate the certificates required by the Federal Rules of Bankruptcy Procedure. This system is the only part of the overall CCDE database that is accessible to the public. Service providers access CGS from the internet in order to generate the certificates. As part of the daily download, DXTR decodes the embedded bar codes contained on each certificate for use by CCDE. The CGS ATO is included in the CCDE ATO and PIA.
- Debtor Audit System (DAS): DAS supports the USTP's statutory authorization to select bankruptcy cases for audit in order to determine the accuracy, veracity and completeness of information filed with the court by individual debtors in Chapters 7 and 13 bankruptcy cases. DAS also selects and monitors audit contractors, tracks the status of audits, collects reported findings, and generates reports. DAS has an ATO that expires on August 31, 2021.
- Chapter 11 Quarterly Fee Information and Collection System (FICS): FICS serves as an accounts receivable system for the USTP. 28 U.S.C. § 1930(a)(6) generally requires the payment of quarterly fees in Chapter 11 cases. Under the statute, fees are calculated based upon the amount of disbursements made by the debtor in the subject quarter. Relevant Chapter 11 case information and disbursement data is obtained from ACMS and permits USTP staff to maintain billing information, assess interest on past due accounts, issue collection and delinquency notices to debtors, and to provide reporting for referrals to the Department of the Treasury. FICS has an ATO that expires on August 1, 2021.

- Means Test Review System (MTR): MTR supports the USTP's statutory requirement to review and verify the financial means testing reporting forms for individual debtors in Chapter 7 bankruptcy cases. MTR also generates initial reviews for presumption of abuse, permits USTP staff to modify the data to facilitate a more thorough review, and generates data relevant to the USTP's preparation of presumption of abuse statements and related civil enforcement motions. It also tracks due dates for these statements and motions. MTR has an ATO that expires on September 1, 2021.
- Professional Timekeeping System (PTS): PTS is a management tool. USTP employees record their hours and their bankruptcy-related activities in this system. In turn, management analyzes the timekeeping statistics as a relevant metric for assessing broader mission success. PTS has an Authority to Operate (ATO) that expires on November 9, 2021.
- Significant Accomplishments Reporting System (SARS): USTP employees use SARS to record informal and formal actions in the areas of civil enforcement, case administration, and other mission-related activities. The USTP also uses SARS data to prepare annual reports to Congress. SARS has an ATO that expires on July 27, 2021.
- Trustee Uniform Final Reports System (TUFR): TUFR is an information system that receives information from private trustees in Chapters 7, 12, and 13 bankruptcy cases. As part of their assigned private trustee oversight responsibilities, USTP employees use TUFR to extract data, view, report, and process private trustee final reports. TUFR has an ATO that expires on January 28, 2023.
- Trustee Final Report Generating Systems (TFRGS): TFRGS is a web-based service developed to assist private trustees who do not have the technical capability to generate and complete required financial reporting forms on a standalone basis. The private trustees ultimately file these financial reports with the United States Bankruptcy Court. TFRGS has an ATO that expires on October 1, 2021.
- Trustee Oversight Database (TOD) (formerly Automated Trustee System (ATS)): TOD supports the USTP's private trustee oversight responsibilities. It collects information that enables USTP employees to evaluate a trustee's competency, performance, and integrity in discharging his or her fiduciary duties. The system stores trustee names, addresses, telephone numbers, email addresses, Social Security numbers, dates of appointment, jurisdiction of cases, and status of security background investigations. It also maintains information related to performance evaluations and audits of operations and case administration, and general case statistics. As part of its oversight duties, the USTP's Office of Oversight enters certain information into TOD about a trustee from a background questionnaire and other application forms. The ATO for TOD is included in JCON's ATO and PIA.

The above systems will be integrated into EBMA on an iterative schedule, and as each integration occurs, the USTP intends to complete a security and privacy authorization of the system's newly integrated functionality.

In addition to the information systems described above, there are two additional systems under development that will now be replaced by EBMA. The USTP will no longer be seeking accreditation or ATOs for the following systems:

- Fee Application System (FeeApp): FeeApp facilitates the USTP's review of the large quantities of publicly available billing records submitted by law firms involved in large Chapter 11 bankruptcy cases to the USTP in an electronic format known as Legal Electronic Data Exchange Standard.
- Chapter 11 Uniform Periodic Reports System (CUPR): CUPR was under development as a modification to the existing TUFR, as it captured much of the same data but for Chapter 11 cases.

As mentioned in the Executive Summary, the USTP currently maintains the above described information systems, several applications, and several data collections on its JCON platform. Contemporaneously with this PIA, the USTP has developed a USTP MS Power Platform (MSPP) subsystem of JCON, which includes tools that are part of the Microsoft Power Platform. This platform is a suite of tools that utilizes Microsoft Azure Government cloud services and is part of Microsoft Office 365, for which an authority to operate was obtained

in January 2019. OPCL is currently reviewing the MSPP Initial Privacy Assessment, and if approved, will be used in the future development of EBMA functionality.

Further, the information systems identified above have Privacy Impact Assessments (PIA) that the USTP will retire and replace with this PIA, as follows:

- USTP Systems (ACMS, FICS, SARS, CETS, MTR, PTS) – approved August 23, 2006;
- DAS – approved March 19, 2007;
- ACMS – approved March 24, 2011;
- CETS – approved March 24, 2011;
- MTR – approved March 24, 2011;
- CCDE – approved May 23, 2011; and
- TUFR – approved July 18, 2013.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	11 U.S.C. § 101, *et seq.*; 28 U.S.C. §§ 581, 586; 589b; 1930; 5 U.S.C. § 552a, *et seq*.
	Executive Order	
X	Federal Regulation	28 C.F.R. Part 58 (including Appendices A and B); 71 Fed. Reg. 59818 (Oct. 11, 2006)
X	Agreement, memorandum of understanding, or other documented arrangement	Memorandum of Understanding Between the Administrative Office of the United States Courts and the Executive Office for United States Trustees Concerning the Bankruptcy Data Download (Dec. 2009)
X	Other (summarize and provide copy of relevant portion)	EBMA will collect data that is publicly available on the bankruptcy court's docket from individuals and law firms as part of the USTP's Appendix B Guidelines, 78 Fed. Reg. 36248, 36251 (June 17, 2013), available at https://www.justice.gov/ust/fee-guidelines. A copy is also attached to this PIA.

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); and D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, and D	EBMA would collect names of debtors, creditors, trustees, and other parties in bankruptcy cases, including any Federal Government employees, contractors or detailees who file bankruptcy. It would also collect names of other Federal Government staff to whom the USTP makes criminal referrals or conducts other business. EBMA would also collect names of USTP employees (timekeeping related to bankruptcy case activities).
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	EBMA would collect SSNs of individual debtors in bankruptcy cases, including Federal Government employees, contractors, or detailees who file bankruptcy. It would also collect SSNs as part of USTP criminal enforcement responsibilities.
Tax Identification Number (TIN)	X	C and D	EBMA would collect TINs from company debtors in bankruptcy cases and as part of USTP criminal enforcement responsibilities.
Driver's license			
Alien registration number	X	C and D	EBMA would collect alien registration numbers from individual debtors in bankruptcy cases and as part of USTP criminal enforcement responsibilities.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, and D	EBMA would collect personal contact information about individual debtors and would include any USTP or other Federal Government employee, contractor, or detailee who files a bankruptcy case.
Personal e-mail address	X	A, B, C, and D	Same as above.
Personal phone number	X	A, B, C, and D	Same as above.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); and D. Members of the Public - Non-USPERs	(4) Comments
Medical records number			
Medical notes or other medical or health information			
Financial account information	X	A, B, C, and D	EBMA would collect financial account information about individual debtors (such as mortgage, auto loan, and credit card balances) in order to make financial assessments relevant to the USTP's statutory duty to supervise the administration of these cases. Collection would include any USTP or other Federal Government employee, contractor, or detailee who files a bankruptcy case.
Applicant information	X	C	EBMA would collect information from individuals and businesses that submit applications for approval as credit counseling and/or debtor education provider services, applicants desiring to serve on creditor committees or to provide professional services in bankruptcy cases.
Education records	X	C	Same as above
Military status or other information			
Employment status, history, or similar information	X	C	Same as above
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	A, B, C, and D	EBMA would collect certificates of completion of credit counseling and debtor education services as required in individual bankruptcy cases. The credit counseling certificates filed with the court contain the individual's name and judicial district. Those not filed with the court do not identify the individual. Debtor education certificates identify the individual, bankruptcy case number and judicial district. These certificates may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); and D. Members of the Public - Non-USPERs	(4) Comments
Legal documents	X	A, B, C, and D	EBMA would collect a variety of legal documents, including but not limited to, required financial reports filed with United States Bankruptcy Courts. These documents may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C	EBMA would collect URLs of credit counseling and debtor education providers, if available.
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	EBMA would collect a variety of criminal records information as part of USTP criminal enforcement activities. These records may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	EBMA would collect a variety of civil law enforcement information as part of USTP civil enforcement activities. These records may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, and D	EBMA would collect this information to the extent it is part of USTP criminal or civil enforcement activities. These records may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.
Grand jury information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); and D. Members of the Public - Non-USPERs	(4) Comments
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	EBMA would collect contact information of witnesses and other information that would be relevant to the USTP's criminal enforcement activities. These records may be related to members of the public, or to Federal Government employees, contractors, or detailees who have filed bankruptcy cases.
Procurement/contracting records			
Proprietary or business information	X	A, B, C, and D	EBMA would collect business information from debtors in bankruptcy cases. To the extent this business information is related to a sole proprietor or other business that is part of an individual's bankruptcy case, these records may be related to members of the public, or to Federal Government employees, contractors, or detailees.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, and D	EBMA would collect recordings of 341 Meetings (Meetings of Creditors) involving debtors, trustees, creditors, and other parties in a bankruptcy case.
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	EBMA would collect USTP user information.
- **User ID**	X	A	Admin/audit data may include this data.
- **User passwords/codes**	X	A	Admin/audit data may include this data.
- **IP address**	X	A	Admin/audit data may include this data.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); and D. Members of the Public - Non-USPERs	(4) Comments
- **Date/time of access**	X	A	Admin/audit data may include this data.
- **Queries run**	X	A	Admin/audit data may include this data.
- **Content of files accessed/reviewed**	X	A	Admin/audit data may include this data.
- **Contents of files**	X	A	Admin/audit data may include this data.
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): Some information may be received directly from debtors, but most of the data is obtained by daily download from the bankruptcy courts.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): EBMA would receive information from USTP employees and from law enforcement partners, such as the Administrative Office of the United States Courts, the United States Attorney, or FBI staff.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	As described below, USTP employees access databases by multi-factor authentication, and only those databases to which they are specifically authorized in order to do complete the USTP's civil and criminal enforcement efforts.
DOJ Components	X			The USTP shares limited information with other DOJ Components to make criminal referrals, and to assist other components with their law enforcement efforts.
Federal entities	X			The USTP shares limited information with other federal entities in support of common interests in certain civil enforcement activities. Information sharing agreements with these federal entities limit the scope and use of any such information.
State, local, tribal gov't entities	X			The USTP may share limited information with state and local entities, such as state bar associations, in support of common interests in certain civil enforcement or administrative activities. Procedures for complying with the *Touhy* requirements are in place to limit the scope and use of any such information.
Public	X			The USTP may share limited information with the public, based upon an appropriate request made under the Privacy Act or the FOIA.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			The USTP's civil enforcement duties require collection of information that is used as documentary information in litigation, reviewing documents for relevance to claims and defenses, conducting and responding to discovery requests, selecting exhibits for trial, and conducting examinations of potential witnesses. The data collected and maintained supports the UPST's litigation and administrative functions.
Private sector	X			The USTP's enforcement and administrative functions include oversight of private trustees who are appointed to administer bankruptcy cases. Information is shared with them as necessary for them to do their work and for USTP oversight. Disclosure is made pursuant to approved routine uses. In limited cases, the USTP may negotiate a protective order and obtain court approval prior to the release of information.
Foreign governments				N/A
Foreign entities				N/A
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

The USTP posts a variety of information on data.gov from several of the existing systems identified above in section 2.1, including SARS and TUFR. This data relates to formal and informal civil enforcement actions, the potential financial impact of these actions and litigation outcomes, as well as final reports filed by Chapter 7 trustees. However, the data is in summary form and contains no specific bankruptcy case, debtor information, or trustee names. The USTP would continue to post the same or similar data from EBMA. No PII would be released to data.gov.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The USTP's information collection, use, and sharing activities are covered by five SORNs: (1) JUSTICE/UST-001 (Bankruptcy Case Files and Associated Records); (2) JUSTICE/UST-002 (Bankruptcy Trustee Oversight Records); (3) JUSTICE/UST-003 (USTP Timekeeping Records); (4) JUSTICE/UST-004 (USTP Case Referral System): and (5) JUSTICE/UST-005 (Credit Counseling and Debtor Education Files and Associated Records). 71 Fed. Reg. 59818 (Oct. 11, 2006).

In addition, members of the public who download certain forms from the USTP website related to professional fee compensation in accordance with Appendices A and B, Guidelines for Reviewing Applications for Compensation and Reimbursement of Expenses filed under 11 U.S.C. § 330, receive notice. A Privacy Act § 552a(e)(3) notice appears on the first page of the Fee Guidelines page on the website. Each form likewise contains a Privacy Act notice. See https://www.justice.gov/ust/fee-guidelines.

Members of the public who wish to complete applications for approval as credit counseling agencies or debtor education providers receive notice through a Privacy Act statement located on the first page of the Credit Counseling and Debtor Education Page on the website and in each set of instructions for completing the applications. See https://www.justice.gov/ust/credit-counseling-debtor-education-information.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

EBMA is an internal system that collects and maintains data received from bankruptcy courts, much of which is publicly available. Some of the information is for investigative purposes, which negates an individual's consent to use. Certain information in the system is not collected directly from the individual, but may be submitted by counsel (e.g., court pleadings), civil and criminal enforcement partners, or uploaded by USTP employees. When information about individuals is collected from the individuals, they receive notice, either on the website, in the SORN, or on certain specific forms available on the website, that they may decline to provide information along with the possible consequences for declining.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Much of the information maintained in EBMA is downloaded from the courts and is publicly available. However, as noted in item 5.2, some information provided by the public is maintained in EBMA as well. Any individual United States citizen or legal permanent resident may seek access, correction, or amendment of records in EBMA that pertain to him or her by submitting a request in writing, by regular

mail addressed to privacy counsel, or by email to the USTP's mailbox for both FOIA and Privacy Act requests: USTP.FOIA.Requests@usdoj.gov. Procedures for making a written request are located on the USTP's website: https://www.justice.gov/ust/foia-privacy-act/privacy-act-requests

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The USTP uses the Cyber Security Assessment and Management (CSAM) application to manage its information systems and ATOs and to manage the security and privacy controls in compliance with NIST guidelines and the Department's requirements. As described above in Section 2.1, each existing information system has its own ATO, however, those systems will be integrated into EBMA and ATOs retired. The USTP's ATO for EBMA is currently under development, but both privacy and security controls have already been assessed and are available in CSAM. **If an ATO has not been completed, but is underway, provide status or expected completion date:** September 2020. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** We do not anticipate any POAM will result from privacy control assessments.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** EBMA is a USTP system that will be part of overall continuous diagnostics and mitigation activities, including annual assessments, penetration tests, vulnerability and configuration scans, and other periodic evaluations.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** EBMA is configured to generate a variety of audit records for account logon events, account management events, object access failures, and privilege use failures, among other things. Depending on the log, the system administrator, database administrator, and Information System Security Manager review and analyze audit records daily or weekly for indications of inappropriate or unusual activity.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.

X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** In addition to annual privacy training, authorized users within the USTP receive training specific to the system.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

- EBMA has a security categorization of "Moderate," under the Federal Information Systems Modernization Act (FISMA) and applicable controls for a Moderate baseline have been selected in accordance with Department requirements.
- Physical access to facilities in which USTP servers are located is controlled and enforced by Microsoft as part of its Azure ATO. This is accomplished in several ways, including: restricting access to a single point of entry that is manned by security personnel 24 hours per day, seven days per week, and only to those individuals whose names appear on an authorized list; restricting access to areas beyond reception by electronic devices on doors that require access cards, biometric devices (hand or fingerprint), and anti-passback controls; and by restricting any visitor access to datacenters to only those with escorts. In addition, all access is logged and audited.
- The system is also configured with two-factor authentication (a Personal Identity Verification, or PIV card, and a Personal Identity Number, or PIN), and is accessible only by USTP employees and contractors with JCON accounts. All authorized users must provide two levels of authentication prior to accessing any data and must request access to specific databases. This ensures that access to specific information is restricted to only those users that have authorized access. In addition, credentials are controlled in compliance with Department and NIST standards, including password management policies, composition, history, and complexity. The USTP also monitors account creation, activation, modification, and removal of unnecessary or defunct accounts. Users are placed in appropriate security groups according to their roles using the principle of least privilege required for them to perform their tasks, and for those users who access the system outside a DOJ facility (such as telework), remote access via Virtual Private Network is controlled and monitored. Remote users are presented with Department policies regarding authorized use each time they log in.
- All authorized users must complete annual CSAT and privacy training, as well as read and agree to comply with the Department's information technology and privacy Rules of Behavior. Additional role-based training is provided based on assigned roles and responsibilities before users may access the systems or perform assigned duties.
- Audit logs are maintained to ensure compliance with the appropriate levels of access and to help safeguard against unauthorized use, access, and disclosure of information. These logs are only accessible by authorized users.

Other risk management strategies and privacy specific controls are discussed below in Section 8, Privacy Risks and Mitigation.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if

available.)

The USTP has eleven National Archives and Records Administration (NARA)-approved retention schedules and periods that apply to the information collected and maintained in the existing systems identified above in section 2.1. Several of these schedules were approved during a period when the USTP primarily relied on paper records and several schedules have been superseded by General Records Schedules (GRS). For purposes of disclosing the full inventory, however, the schedules are described below.

- N1-060-92-005, Field Office Records, approved February 14, 1994. USTP field office records are disposed of as follows:
  - Chapter 7 asset cases will be destroyed three years after the case is closed by the court.
  - Chapter 7 no-asset cases shall be destroyed after review of the trustee's no-asset report.
  - Chapter 11 cases shall be destroyed three years after the court enters an order of dismissal or confirmation.
  - Chapter 12 cases shall be destroyed six months after the court enters an order of dismissal or confirmation, whichever occurs first.
  - Chapter 13 case files shall be destroyed 30 days after the court entered an order of dismissal or the plan is confirmed, whichever occurs first.
  - Section 341 meeting of creditors (341 meeting) tapes shall be erased or destroyed two years after the date of the conclusion of the 341 meeting, unless the UST determines it is appropriate to keep longer. All other media formats for 341 meeting recordings are unscheduled and are considered permanent until a revised field office retention schedule is approved by NARA.

- N1-060-04-002, approved, March 4, 2004. Bankruptcy trustee oversight records are destroyed after three years, except in the following circumstances: (1) if a trustee dies, the records may be destroyed after one year; (2) Case Trustee Interim Reports may be destroyed after five years.

- N1-060-09-063, approved February 4, 2010. Master files containing means test information collected and stored in MTR, are retained for 20 years after case is closed.

- N1-060-09-053, approved February 20, 2010. Master files containing credit counseling and debtor education information collected in CCDE and CGS are retained for 20 years from date of receipt and CGS data will be retained for 20 years after course completion.

- N1-060-09-036, approved July 1, 2010. Master files containing bankruptcy case information collected and stored by ACMS are retained for 20 years after the case is closed.

- N1-060-09-071, approved September 3, 2010. Master files containing USTP employee timekeeping information collected and stored in PTS are retained for 20 years after the date the employee makes the entry.

- N1-060-09-051, approved December 1, 2010. Master files containing bankruptcy case and related USTP employee actions collected and stored in SARS are retained for 20 years after case is closed.

- N1-060-09-035, approved December 1, 2010. Master files containing case referral data collected and stored in CETS are retained for 20 years after case is closed.

- DAA-0060-2012-0004, approved November 1, 2011. Master files containing private trustee case

information collected and stored in TUFR are retained for 20 years after case is closed,

- N1-060-09-052, approved May 3, 2020. Master files containing Chapter 11 quarterly fee information collected and stored by FICS are retained for 20 years after the case is closed and has a zero balance.

- N1-060-09-033, approved December 1, 2020. Master files containing audit data collected and stored in DAS, as described above, will be retained for 20 years after case is closed.

The USTP anticipates that it will submit to the Department and then to NARA for approval a new retention schedule for the information that EBMA will collect and maintain that is not otherwise covered by a General Records Schedule. The new NARA schedule will be media neutral and will include updates based on changes and improvements to business operations.

Input and output records to EBMA will be covered under two General Records Schedules (GRS):

- GRS 5.2, Item 20 (Transitory and Intermediary Records), available at https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf; and
- GRS 4.2, Item 130 (Information Access and Protection Records), available at https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf.

Temporary EBMA records will be disposed of in accordance with 36 C.F.R. § 1226.24.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

(1) JUSTICE/UST-001 (Bankruptcy Case Files and Associated Records); (2) JUSTICE/UST-002 (Bankruptcy Trustee Oversight Records); (3) JUSTICE/UST-003 (USTP Timekeeping Records); (4) JUSTICE/UST-004 (USTP Case Referral System): and (5) JUSTICE/UST-005 (Credit Counseling and Debtor Education Files and Associated Records). 71 Fed. Reg. 59818 (Oct. 11, 2006).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

Privacy Risk: Unauthorized access or misuse by authorized user or compromise of data.
Mitigation: As described above, security controls that authorize and limit a user's access to information contained in EBMA mitigate the risks of improper access. Access is restricted to only those employees with a need to know the information and is further restricted by role and tasks necessary to carry out an employee's duties. In addition, no access is granted until the appropriate supervisor or manager approves a request, and the user completes training and agrees to abide by certain rules of behavior. Further, access and system activity are audited and regularly reviewed to verify that they are consistent with existing access limitations. Changes to roles and permissions are also logged and reviewed. The USTP also continuously monitors the security of the system by conducting vulnerability scanning, patching, and intrusion prevention and annual risk assessments.

In addition to CSAT training, annual privacy training is provided to all employees and contractors to remind them of their obligations to protect data and to minimize the use of PII wherever possible. These steps also mitigate the risk of either purposeful or inadvertent compromise of data. In addition, the USTP developed a breach response form that is tied to an automatic email addressed to the Incident Reporting Team and posted it prominently on its SharePoint portal so that any employee may promptly report actual or suspected compromises of PII. This form and associated procedures mitigate any potential harm to individuals and to the USTP as a result of an actual or suspected breach.

All security and privacy controls pertaining to access are documented in the EBMA System Security and Privacy Plan and uploaded into CSAM.

Privacy Risk: Inaccurate or incomplete data.
Mitigation: Members of the public cannot enter records directly into the system. Most of the data collected and maintained in EBMA will come from DXTR downloads from the bankruptcy courts. The USTP does not control the source of the data, but once imported into EBMA, it is verified to ensure that the extracted information has been accurately generated and transmitted. As described above, employees are trained on their obligations to protect data and to minimize the use of PII wherever possible, and access is limited to only those employees who need access in order to perform their duties. Finally, members of the public may seek amendments or corrections to their data by submitting a Privacy Act request to the USTP. See 5 U.S.C. § 552a(d). The USTP's public website (https://www.justice.gov/ust/foia-privacy-act/privacy-act-requests) contains detailed information that explains these rights and provides instruction on how to submit a request.