UNITED STATES TRUSTEE PROGRAM

Privacy Impact Assessment
for the
USTP Justice Consolidated Office Network

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

Approved by: Katherine Harman-Stokes
Director (Acting), Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: [August 29, 2022]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Trustee Program (USTP) is the component of the Department of Justice responsible for overseeing the administration of bankruptcy cases and private trustees. The USTP is a national program with broad administrative, regulatory, litigation, and enforcement authorities whose mission is to promote the integrity and efficiency of the bankruptcy system for the benefit of all stakeholders – debtors, creditors, and the public. This mission is carried out by USTP personnel in the Washington, DC Executive Office and 21 regions with 90 field offices located across the country.

The USTP's Justice Consolidated Office Network (JCON) system maintains various applications that permit the USTP to collect, organize, analyze, and disseminate information more efficiently. This information includes bankruptcy case related records as well as records about USTP employees, contractors, and volunteers, records related to internal case management, litigation support, financial reporting, FOIA and Privacy Act requests, and administrative personnel services and functions. JCON also provides a platform for the USTP's network infrastructure, including hardware, e.g., servers, workstations, laptops, tablets, network switches, requisite cabling, and smartphones interconnected by the Justice Unified Telecommunications Network (JUTNet) and software. The system allows all offices nationwide to be connected, and all users rely heavily on JCON as their portal to access data, applications, printing, and email services. USTP personnel are the sole users of JCON and the applications that reside on it. There is no external access to the system.

Since approval of the last PIA (USTP Systems, Aug. 24, 2006), the USTP has upgraded its existing systems and has migrated to a hybrid cloud environment which is a mix of on-premises and Federal Risk and Authorization Management Program (FedRAMP) compliant government cloud hosting options. In addition, some of the systems previously documented in the USTP Systems PIA were subsequently authorized to operate through separate PIAs. The USTP also has implemented several new systems along with a number of applications that maintain data on SharePoint. This PIA is intended to update and replace the USTP Systems PIA with a current description of systems and applications, as detailed further below.[1] Upon approval of this PIA, the USTP Systems PIA will be retired or withdrawn.

[1] Most of these systems were intended to be integrated into the Enterprise Bankruptcy Management Application (EBMA) as part of the USTP's modernization effort to eliminate obsolete systems, improve user capabilities and enhance security and privacy safeguards. The EBMA PIA was approved on May 29, 2020. Integration efforts remain ongoing. In an abundance of caution, the systems that were part of USTP Systems PIA and not subsequently covered by a separate PIA or not yet integrated into EBMA are included in this JCON PIA.

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 is mission. As described above, JCON is a network infrastructure platform for servers, workstations, laptops, tablets, smartphones interconnected by the JUTNet. All offices nationwide are connected via this infrastructure. JCON also acts as an umbrella for and interconnects with various systems and applications necessary to perform the USTP's mission, including:[2]

- The Automated Chapter 11 Quarterly Fee Information and Collection System (FICS): FICS serves as the USTP's accounts receivable system. 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 Treasury. FICS has an Authorization to Operate (ATO) that expires on June 1, 2024.

- Microsoft Power Platform (MSPP): MSPP consists of two applications that utilize Microsoft Azure Government cloud services and are part of Microsoft Office 365, for which an ATO was obtained in January 2019. The two applications are (1) Microsoft Power Apps, a suite of applications and data platform that facilitates the customization of applications for business operations, does not require specialists to write "code," and provides seamless use in browsers and mobile devices; and (2) Microsoft Power BI, a collection of software services and applications that work together to transform unrelated sources of data into coherent, visually immersive, and interactive insights. MSPP has an ATO that expires on August 3, 2023.

- Professional Timekeeping System (PTS): PTS is a management tool. USTP employees record their hours and their bankruptcy-related activities in this system in order to capture timekeeping statistics in a way that can be analyzed by management for purposes of determining whether statutory priorities are being met. PTS has an ATO that expires on November 8, 2024.

---

[2] The following systems were previously approved to operate as part of the USTP Systems PIA, but are now approved under separate PIAs and ATOs: Automated Case Management System (ACMS) (PIA approved March 24, 2011, ATO expires November 30, 2024); Criminal Enforcement Tracking System (CETS) (PIA approved March 24, 2011, ATO expires November 8, 2024); Debtor Audit System (DAS) (PIA approved March 24, 2011, ATO expires August 2, 2024); Means Test Review Management System (MTR) (PIA approved March 24, 2011, ATO expires August 27, 2024); Credit Counseling/Debtor Education Tracking System (CCDE) (PIA approved May 23, 2011, ATO expires May 4, 2024); and Trustee Uniform Final Reports System (TUFR) (PIA approved July 18, 2013, ATO expires September 3, 2024).

- ServiceNOW (SNOW): SNOW is a cloud-based web enabled system that connects to the USTP Active Directory of its personnel. This connection permits the USTP Office of Information Technology (OIT) to respond to service requests and also permits automated responses and/or updates to the requesting employee or contractor (USTP User). The USTP has been using SNOW since approximately 2018 in order to track, respond to, and measure performance related to a variety of IT related service requests, including general helpdesk requests, user onboarding and offboarding tasks, and service requests related to the use of Department's Unified Financial Management System (UFMS). Recently, the USTP received approval to expand the use of SNOW to track, respond and measure performance related to USTP security incidents, such as notices of malicious email (category 11), which are frequent and require personnel time and effort to investigate and resolve. SNOW has an ATO that expires on March 1, 2024.

- Significant Accomplishments Reporting System (SARS): SARS is used by USTP employees to record informal and formal actions in the areas of civil enforcement, case administration and other mission-related activities. The data in SARS also provides part of the basis for the USTP's annual reports to Congress. SARS has an ATO that expires on July 27, 2024.

- USA Performance (USAP):[3] USAP is a web-based application owned by the Office of Personnel Management (OPM) that automates performance management responsibilities for both employees and managers. OPM maintains the system and provides the USTP with access through the use of employee PIV cards. The USTP uses the system to develop performance work plans, track and monitor mid-year and final performance, provide feedback and ratings, and digitally sign documents. Employees may view only their personal data and managers only view data of the employees they supervise.

- SharePoint: In addition to the systems described above, and in response to multiple requirements for managing databases through small applications, the USTP developed an application platform in SharePoint that resides on the USTP Intranet. The SharePoint applications provide the capability for the USTP to collect and store data and communicate and collaborate across all Executive Office and field offices. The applications are essential for carrying out mission-related as well as administrative operations. Some of these applications collect and maintain PII, and some do not. A comprehensive list is included in the SharePoint System Security and Privacy Plan (SSPP) and uploaded to the Department's Cyber Security Assessment and Management (CSAM) tool. Appendix A contains a list and description of the systems and applications that collect, store, and maintain PII.

- OneDrive: In addition to the SharePoint applications, the USTP collects and stores data, including PII, and collaborates across the Executive Office and field offices using OneDrive. Shared drives located in OneDrive are limited use and restricted to employees and contractors who have a need to know the information to perform their duties. Some are restricted to a particular office (e.g., a specific regional office, a subset of employees within a regional office, or the Office of the General Counsel (OGC) within the EOUST), some are restricted to a group of employees based on the work they do (e.g., attorneys and analysts who work on litigation and enforcement matters related

[3] The USTP relies on OPM's ATO, which expires on June 24, 2023. It also relies on OPM's PIA for USAP, dated May 13, 2020.

to specific bankruptcy cases in the various field offices, attorneys and other staff who conduct periodic evaluations of operations in offices of their peers, managers who certify and maintain confidential financial disclosure reports across the EOUST and field offices, budget personnel who develop and formulate USTP budgets for submission to the Department, statisticians who collect and analyze bankruptcy information and other data for quarterly reporting and performance metrics, and attorneys and support staff who process Privacy Act and FOIA requests). These records are saved to restricted subfolders within each responsible office and only those employees who work on the matters within those offices have access to the folders.

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).
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)
	Other (summarize and provide copy of relevant portion)	

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	JCON, through one or more of its systems identified in this PIA, collects names of debtors, creditors, trustees, and other parties in bankruptcy cases. It also collects names of other Federal Government staff with whom the USTP conducts other business, and it collects names of USTP employees (e.g., timekeeping related to bankruptcy case activities, certain administrative matters, and related to performance work plans and appraisals). Full names are also collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
Date of birth or age	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects date of birth or age of debtors, creditors, trustees, and other parties in bankruptcy cases, and may also collect this data about USTP employees, to the extent necessary to confirm identity. Date of Birth is also collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
Place of birth	X	A, B, C, and D	Place of Birth is collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
Gender			
Race, ethnicity or citizenship	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects race and citizenship information from candidates for private trustee applicants, which may include USTP employees and other Federal Government employees if they have applied for private trustee opportunities. Citizenship information is collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
Religion			

(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
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects SSNs of individual debtors in bankruptcy cases, and may also collect this data from USTP employees to the extent necessary to confirm identity and/or to integrate performance data into employee Official Personnel Folders. SSNs are also collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
Tax Identification Number (TIN)	X	C and D	JCON, through one or more of its systems identified in this PIA, collects TINs from company debtors in bankruptcy cases.
Driver's license			
Alien registration number	X	C and D	JCON, through one or more of its systems identified in this PIA, collects alien registration numbers from individual debtors in bankruptcy cases as part of USTP enforcement responsibilities.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects personal contact information about individual debtors, or Federal Government employees who file a bankruptcy case. It also collects personal contact information about individual USTP employees in certain administrative files. Personal address is also collected on DOJ-361 (Certification of Identity) for Privacy Act requests and certain FOIA requests.
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.
Medical records number			
Medical notes or other medical or health information	X	A, C, and D	JCON, through one or more of its systems identified in this PIA, collects medical information provided by USTP employees in certain administrative matters. Medical billing that includes medical information, e.g., diagnosis codes, could be included in 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
Financial account information	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects personal contact information about individual debtors, or Federal Government employees who file a bankruptcy case. It also collects personal contact information about individual USTP employees in certain administrative files
Applicant information	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects information from individuals who submit applications for employment for internships with the USTP, or appointments to bankruptcy case roles such as trustee, examiner, creditor's committee, or ombudsman.
Education records	X	A, B, C, and D	Same as above.
Military status or other information	X	A, B, C, and D	Same as above.
Employment status, history, or similar information	X	A, B, C, and D	Same as above.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	Same as above (if applicants for employment with the USTP are required to submit). In addition, JCON, particularly through its SharePoint portal, maintains performance evaluations of USTP employees prior to implementation of USA Performance and to the extent data is pulled from that database into the portal.
Certificates	X	A	Certificates are installed on the JCON system and on the user's PIV card.
Legal documents	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects a variety of legal documents.
Device identifiers, e.g., mobile devices	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects this information from debtors, creditors, other parties in bankruptcy cases, including USTP employees and other Federal Government employees who file bankruptcy cases. It also collects USTP issued mobile device identifiers from USTP employees.
Web uniform resource locator(s)			
Foreign activities			

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects criminal history and arrest information from candidates for private trustee, which may include USTP employees and other Federal Government employees if they apply for this position.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects a variety of civil law enforcement information as part of USTP civil enforcement activities.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects this information to the extent it is part of USTP civil enforcement activities.
Grand jury information	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects this information to the extent it is part of USTP civil enforcement activities and also criminal referrals.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	Same as above.
Procurement/contracting records	X	A, B, C, and D	JCON, through one or more of its systems identified in this PIA, collects records related to contracts, including Tax ID and other information of companies from whom the USTP purchases goods, and also names and contact information of individuals named in contracts for services.
Proprietary or business information	X	C and D	JCON, through one or more of its systems identified in this PIA, collects business information from company debtors in bankruptcy cases.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			

(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
- **Video containing biometric data**	X	A	JCON, through its SharePoint applications, collects some video recordings of USTP personnel, for example, the Director's occasional addresses to the USTP.
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C. and D	JCON, through one or more of its systems identified in this PIA, collects recordings, for example, statutorily mandated meetings of creditors that debtors in bankruptcy cases are required to attend and Voice Over Internet Protocol (VOIP) voice mail messages.
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	JCON, through one or more of its systems identified in this PIA, collects USTP user information.
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A	JCON, through one or more of its systems identified in this PIA, collects USTP user information, including PII if voluntarily provided, and USTP employees' Protected Health Information (PHI) may be collected by the Office of Administration. Various forms of PII may be included in responsive records for Privacy Act and/or FOIA inquiries saved in JCON.

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. Likewise, information about USTP employees is received directly from employees via these sources. On occasion, USTP field offices may collect information about individuals posted on social media platforms, such as Facebook.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Pursuant to a Memorandum of Understanding with the Administrative Office of the United States Courts, the USTP receives daily data downloads from bankruptcy courts across the country, which the USTP in turn, maintains in JCON.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): On occasion, USTP field offices collect information about individuals through social media platforms, such as Facebook, using these sources as a search tool and maintaining any relevant records in restricted and case-specific shared drive folders.					

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 to complete the USTP's civil enforcement efforts.
DOJ Components	X			The USTP shares limited information with other DOJ Components to assist them with their law enforcement efforts. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below).
Federal entities	X			The USTP shares limited information with other federal entities, e.g., the Consumer Financial Protection Bureau (CFPB), in support of common interests in certain civil enforcement activities. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below). In addition, information sharing agreements limit the scope and use of any such information.

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.**
State, local, tribal gov't entities	X			The USTP may share limited information with state and local entities, e.g., state bar associations, in support of common interests in certain civil enforcement or administrative activities. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below). In addition, 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. Also, as noted below, some records will be used in bankruptcy proceedings, and some of these records may become public in accordance with court rules. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below).

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 in litigation. USTP personnel review documents for relevance to claims and defenses, conduct and respond to discovery requests, select exhibits for trial, and conduct examinations of potential witnesses. The data collected and maintained supports the USTP's litigation and administrative functions. This information may be shared with counsel, parties, witnesses, courts, and other judicial tribunals, and may become public in accordance with court rules. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below).

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.**
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 the USTP to properly oversee them. Depending on the information requested, the records could come from any of the systems identified in this PIA and could consist of the data identified in section 3, consistent with the Privacy Act and the USTP's SORNs (described in section 5 below).
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 information on data.gov from SARS, one of the existing systems identified above in section 2.1. This data relates to formal and informal civil enforcement actions, the potential financial impact of these actions and litigation outcomes. The USTP also posts data obtained in final reports publicly filed by private trustees in chapter 7 bankruptcy cases. However, the data posted from these sources 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. No personally identifiable information (PII) is 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).

Information collection, use, and sharing activities related to USTP employees are covered by multiple OPM government-wide SORNs, including OPM/GOVT-2 (Employee Performance File System Records), 71 Fed. Reg. 35347 (June 19, 2006), and OPM-GOVT-3 (Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probations), 71 Fed. Reg. 35350 (June 19, 2006).

Information, collection, use, and sharing activities related to USTP help desk assistance are covered by JUSTICE/DOJ-002 (DOJ Computer Systems Activity & Access Records), 86 Fed. Reg. 37188 (Jul. 14, 2021)**.**

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 by a Privacy Act § 552a(e)(3) notice appearing on the first page of the Fee Guidelines page on the website and also by a Privacy Act notice located on each form. See https://www.justice.gov/ust/fee-guidelines. Individuals who visit the website to learn about credit counseling and debtor education providers, or who wish to apply to provide these services also receive Privacy Act notices on the website and in each set of instructions for completing the forms.
See https://www.justice.gov/ust/credit-counseling-debtor-education-information, https://www.justice.gov/ust/file/cc_application_instructions.pdf/download, and https://www.justice.gov/ust/file/de_application_instructions.pdf/download.

Most recently, the USTP completed an administrative rulemaking that mandated that chapter 11 debtors-in-possession and trustees complete periodic reporting through the use of uniform Monthly Operating Report and Post-Confirmation Report forms. Notice to the public is provided by a Privacy Act notice located on each form. See https://www.justice.gov/ust/file/1452406/download and https://www.justice.gov/ust/file/1452396/download.

USTP may direct Privacy Act requesters and certain FOIA requesters to complete the DOJ-361 (Certification of Identity) form, which includes a Privacy Act Statement. See https://www.justice.gov/ust/file/doj361_form.pdf/download.

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.

JCON is an internal system that collects and maintains data received from a variety of sources, including bankruptcy courts and individuals. Some of the information is for investigative purposes and negates individual 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, information about professional fees). Individuals 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.

USTP may direct Privacy Act requesters and certain FOIA requesters to complete the DOJ-361 (Certification of Identity) form. This is done when it is not entirely clear as to which statute the requester intends to proceed under when seeking records on themselves. In addition, when a FOIA requester seeks information about another individual's bankruptcy case, USTP's standard practice is to direct them to complete the DOJ-361 form to establish that they have the relevant individual's consent. Absent such consent, USTP would heavily redact any FOIA response under exemption 6.

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 JCON and/or its systems identified in this PIA is generated internally (e.g., many of the SharePoint applications, MSPP or SNOW). Some information is provided by the public. Any individual may seek access to records 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 FOIA requests. United States citizens and lawful permanent residents may request amendment or correction through 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 CSAM 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. JCON itself also has its own ATO and it expires on January 7, 2025.

	If an ATO has not been completed, but is underway, provide status or expected completion date: **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:** Privacy and security control assessments were conducted in connection with the ATO obtained in January 2022. There are no outstanding POAMs.
	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:** JCON is included in the 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:** Audit logs are generated continually to detect unauthorized changes to information and software. JCON is configured to generate audit records for account logon events, account management events, object access failures, and privilege use failures, among other events. The system administrator and database administrator review and analyze audit records 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**.
	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: N/A

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?

- JCON has a security categorization of "Moderate," under the Federal Information Security Modernization Act (FISMA), and applicable security and privacy controls for a Moderate system have been selected in accordance with Department requirements.

- Controls to reduce the risk of unauthorized access.
  - Physical access to the JCON system is controlled by Microsoft site-specific controls and agreements. The system is on a physically secure Department network protected by appropriate firewalls. Physical access to the JCON routers, switches, printers, and

laptops is controlled by a combination of PIV card proximity readers and cipher locks.

- The system is also configured with two-factor authentication (an RSA token, or 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. Most users authenticate to the system using a PIV card, with the RSA token being used as a secondary method of authentication for those users who do not have or have lost a PIV card. 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.

- System administrator accounts are not privileged until elevated access is needed. The elevated access is automatically removed after 4 hours.

- System patching can only be initiated by administrators with elevated privileges. Regular user accounts have no technical access to apply patches to systems.

- Controls to reduce the risk of unauthorized disclosure. In addition to privacy controls described in Section 8, all authorized users must complete an annual Cyber Security Awareness Training (CSAT), which includes annual privacy training, as well as read and agree to comply with the Department's information technology 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.

- Controls to protect PII in transmission.
  Transmission of PII is protected in several ways between USTP offices and external entities. Within the JCON network, all data is encrypted between offices by JUTNET. Transmission to and from the Azure Government cloud is also encrypted. Internal and external websites are encrypted, and a connection is disabled if the external site does not have the requisite encryption protocols enabled. Finally, PII is protected via email by use of the DOJ secure email portal. The software will automatically reject and return to the sender any email containing certain types of sensitive PII that is not sent through the secure portal.

- Regular auditing of role-based access. 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. In addition, all JCON accounts are managed through the add/mod approval process, and no accounts

are created, deleted or roles modified without approval. These accounts are also audited annually for proper access to groups and network shared drives.

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 several NARA approved retention schedules and periods that apply to the information that is collected and maintained in JCON through one or more of its systems identified in this PIA:

- N1-060-09-052, approved May 3, 2010. Master files containing chapter 11 quarterly fee information collected and stored by FICS will be retained for 20 years after the case is closed and has a zero balance. Per the USTP's SORN, JUSTICE/UST-001, records will be disposed of by shredding, burning, or similar methods.

- N1-06-09-071, approved September 3, 2010. Master files containing USTP employee timekeeping information collected and stored in PTS will be retained for 20 years after the date the employee makes the entry. Per the USTP's SORN, JUSTICE/UST-003, the records will be disposed of by shredding, burning, or similar methods, after being audited; or when three years old.

- N1-060-09-051, approved December 1, 2010. Master files containing bankruptcy case and related USTP employee actions collected and stored in SARS will be retained for 20 years after case is closed. Per the USTP's SORN, JUSTICE/UST-001, records will be disposed of by shredding, burning, or similar method.

- N1-060-04-002, approved May 1, 2011. Master files containing private trustee oversight information collected and stored in Trustee Oversight Database (TOD)/Audit Tracking System (ATS) will be retained for three years. Per the USTP's SORN, JUSTICE/ UST-002, the records will be disposed of by shredding, burning, or similar methods, as follows: Bankruptcy trustee oversight records may be 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. Also, N1-060-92-005, approved, February 14, 1994, provides that panel trustee 180-day/semi-annual reports shall be destroyed after the most recent record is five years old.

In addition, the Department has several NARA approved retention schedules and periods that apply to records collected and maintained in JCON:

- DAA-0060-2012-0017, approved January 15, 2013. Information collected and stored in UFMS to reserve, obligate, process and effect payment or collection of funds (including

vouchers, invoices, purchase orders, travel vouchers and accounts payable/receivable), will be destroyed 10 years after the cancellation of the applicable appropriation.

- DAA-0060-2012-0023, approved March 26, 2013. Annual forms completed by Department attorneys certifying that they are active members of a bar that are maintained by the employer-component (and also includes the consolidated certification sent to the Office of Attorney Recruitment and Management (OARM)) have a cutoff period of the end of each calendar year and then are destroyed ten years after that cutoff.

- DAA-0060-2014-0004, approved January 21, 2015. General public correspondence records that do not relate to a specific case or action are retained for one calendar year. If no response was required, the records are destroyed within three months but no later than one year after the one-year cutoff. If a response was required, the records are destroyed three years after the one-year cutoff.

- DAA-0060-2016-0004, approved May 4, 2017. Job application materials maintained by component-level selection committees, including applications, records generated during the vetting and interviewing process, records generated during the decision-making process (and can be related to delegated examining, merit promotion, internships, and the Honors and Pathways Programs, but not records maintained in personnel files or Human Resources staff) are temporary and are retained until the end of the calendar year in which the vacancy is closed or final settlement of any related dispute, whichever is later. The records are destroyed two years after that cutoff period.

- DAA-0060-2017-0009, approved May 31, 2017. Legal, investigative and litigation specific training records, including curriculum development, faculty information, course descriptions, registration/enrollment information, lesson plans, student evaluations and other related materials (both internal and external) may be destroyed between six and ten years after the last action. In addition, other administrative records related to training, such as publicity, schedules, and logistics, are retained for one year cut-off period and then are destroyed six years after that cutoff.

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).

See also Information collection, use, and sharing activities related to USTP employees are covered by multiple OPM government-wide SORNs, including OPM/GOVT-2 (Employee Performance File System Records), 71 Fed. Reg. 35347 (June 19, 2006), and OPM-GOVT-3 (Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probations), 71 Fed. Reg. 35350 (June 19, 2006).

Information, collection, use, and sharing activities related to USTP help desk assistance are covered by JUSTICE/DOJ-002 (DOJ Computer Systems Activity & Access Records), 86 Fed. Reg. 37188 (Jul. 14, 2021).

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?

Privacy Risk: Unauthorized access or misuse by authorized user or compromise of data.
Mitigation: As described above, the security controls that authorize and limit a user's access to information contained in JCON 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. For example, users with administrative privileges are required to take additional training that relates to their elevated status and privileged users are also required to read and sign a Privileged Rules of Behavior document. 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, including vulnerability scanning, patching, intrusion prevention and annual risk assessments.

CSAT training, which includes 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 posted it prominently on its SharePoint portal so that any employee may promptly report potential compromises of PII to the Incident Reporting Team. This form and associated procedures mitigate any potential harm to individuals and to the USTP as a result of the breach.

All security and privacy controls pertaining to access are documented in the JCON SSPP and the SharePoint SSPP and uploaded into CSAM.

Privacy Risk: Inaccurate or incomplete data.
Mitigation: This risk is mitigated, in part by the fact that the majority of information contained in

JCON is generated internally, though some is obtained from outside sources. In those instances (e.g., Legal Electronic Data Exchange Standard (LEDES) data for certain professional fee information, information from applicants seeking approval as credit counseling agencies or debtor education providers), the risk is mitigated by the format, syntax limits to input fields and the source of the data, as applicants themselves provide the information. To the extent individuals provide data directly to the USTP, risks of inaccurate or incomplete data are mitigated by the fact that there are significant civil (and possibly criminal) penalties for purposeful failures to disclose or for intentional misrepresentations made on certain documents that are prepared under oath.

Individuals whose data the USTP collects have the ability to request correction of their data by making a Privacy Act request. Further, as also described above, access to JCON is limited to those USTP employees who need it to perform their duties, and such use is audited.

All security and privacy controls pertaining to accuracy and completeness of data are documented in the JCON and SharePoint SSPPs and uploaded into CSAM.