United States Trustee Program

Privacy Impact Assessment
for the
Trustee Uniform Final Reports System (TUFR)

Issued by:
Larry Wahlquist, Privacy Point of Contact

Reviewed by: Luke McCormack, Chief Information Officer, Department of Justice

Approved by: Joo Y. Chung, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: July 18, 2013

Section 1: Description of the Information System

Provide a non-technical overall description of the system that addresses:

(a) the purpose that the records and/or system are designed to serve;
(b) the way the system operates to achieve the purpose(s);
(c) the type of information collected, maintained, used, or disseminated by the system;
(d) who has access to information in the system;
(e) how information in the system is retrieved by the user;
(f) how information is transmitted to and from the system;
(g) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects); and
(h) whether it is a general support system, major application, or other type of system.

As background, administration of bankruptcy cases under chapters 7, 12, and 13 of the United States Bankruptcy Code is entrusted to private trustees acting under the oversight and supervision of a United States Trustee, an official of the Department of Justice. In each case, the private trustee must file with the court, and submit to the United States Trustee, a final report and accounting of his or her administration of the case. In order to facilitate case administration and to assist in its duties of evaluation and oversight of private trustees, the United States Trustee Program's (USTP) Executive Office for United States Trustees (EOUST) has developed the Trustee Uniform Final Reports (TUFR) database.

Pursuant to the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA), the USTP has issued a regulation requiring the use of uniform forms for final reports by private trustees in chapters 7, 12, and 13. See 73 Fed. Reg. 58,438 (Oct. 7, 2008). Per this regulation, the trustee final report forms are filed with the bankruptcy court as "data-enabled" PDF documents. A "data-enabled" form is a PDF document that is completed online, and then saved as a PDF file that highlights or marks certain pieces of data entered into the individual fields on the form; the data in these highlighted/marked (i.e., "data-enabled") fields can be automatically extracted by TUFR. To put it differently, trustees file these reports with the bankruptcy courts; the USTP obtains these PDF documents from the courts; and TUFR automatically extracts data from data-enabled fields (but does not store or maintain the PDF documents themselves). This extracted data is stored in TUFR.

The data that is extracted directly from the trustee final reports are aggregated financial information relative to the trustee's administration of the bankruptcy case:

- amounts of disbursements to creditors,
- trustee's receipts, fees and expenses,
- claim amounts by creditors, and
- total expenses of bankruptcy estate administration.

Although the final reports themselves do contain some items of personally identifiable information (PII) (e.g., names of private trustees, names of debtors, names of cases, numbers of cases), TUFR itself does not extract any items of PII from the uniform final reports because the

USTP decided not to "data-enable" any fields in the reports determined to be PII.[1] The reason for not data-enabling the PII data fields was to avoid making the PII more easy to extract and aggregate by the public than what is currently available from the court's system. Currently, if a member of the public wanted to collect debtors' case names/numbers, he or she would have to manually access the reports in each individual case. If the case name/number data fields were data-enabled on the reports, however, anyone with the appropriate software and expertise could utilize automated data extraction methods to easily obtain and aggregate this information.

However, TUFR does obtain certain items of PII (specifically, names of private trustees, names of debtors, names of cases, and numbers of cases) – not from the uniform final reports but rather from the USTP's Automated Case Management System (ACMS), which the public does not have access to. This enables the USTP to gather necessary PII in the TUFR database without making that same PII easier to access than it already is within the court's system (i.e., accessing individual cases via PACER or at the courthouse).

By combining the bankruptcy case financial information extracted directly from the trustee final reports with PII data elements received from ACMS, the TUFR database allows the USTP to analyze and evaluate data pertaining to a trustee's case administration; identify duplicate, invalid, or missing data; and make corrections where necessary. Users retrieve information pertaining to a trustee's administration of a case, including the limited items of PII associated with the case, either by searching by case number, or by clicking on the pertinent USTP office, which then displays a list of cases organized by case number and labeled with both the case number and case name. The user then clicks on a particular case in order to view information about the trustee's administration of that case. In addition, system administrators may retrieve user information such as logs of user activity by user ID.

The system is used by authorized USTP personnel. The primary user of TUFR is EOUST's Office of Oversight, which is tasked with evaluating the performance of private trustees. Access is limited to USTP personnel, including both users and system administrators.

Information maintained in TUFR is not ordinarily disclosed or shared outside of the USTP. Disclosure and sharing practices are discussed in more detail in section 4.1.

Finally, TUFR is categorized as a "major application" by the DOJ Cyber Security Assessment and Management (CSAM) system.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

[1] Of course, because the final reports are filed with the court, any PII in the reports is available to the public through Public Access to Court Electronic Records (PACER) or at the courthouse.

(Check all that apply.)

Identifying numbers					
Social Security		Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	X
Employee ID		Passport		Patient ID	
File/case ID	X	Credit card			
Other identifying numbers (specify):					

General personal data					
Name	X	Date of birth		Religion	
Maiden name		Place of birth		Financial info	X
Alias		Home address		Medical information	
Gender		Telephone number		Military service	
Age		Email address		Physical characteristics	
Race/ethnicity		Education		Mother's maiden name	
Other general personal data (specify):					

Work-related data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):					

Distinguishing features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify):					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	
Other system/audit data (specify):					

Other information (specify)

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):					

Government sources					
Within the Component	X	Other DOJ components		Other federal entities	X
State, local, tribal		Foreign			
Other (specify):					

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

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As explained above, to make it possible for TUFR to extract financial information from the trustee final reports, the USTP has "data-enabled" many of the fields in the reports. One of the risks of data-enabling fields in the reports is that because the reports themselves are publicly available (through PACER or at the bankruptcy courts), a member of the public could easily collect both identifying information and corresponding financial data from the reports by utilizing automated extraction methods. For this reason, the USTP decided not to data-enable any fields in the reports determined to be PII. Thus, if a member of the public wanted to collect debtors' case names/numbers, he or she would have to manually access the reports in each individual case.

While the USTP does maintain certain items of PII (which are obtained from ACMS, as explained above), there are only four such items (name of trustee, name of debtor, name of case, number of case) and, standing alone, these items of PII are not particularly sensitive. TUFR does not collect or maintain more sensitive items of PII such as debtors' social security numbers or taxpayer ID numbers.

Information maintained in TUFR is not obtained directly from the individual (i.e., the debtor or the private trustee). This increases the risk that the information in the system will be inaccurate and that individuals will not be aware that information is being maintained on them. The risk that the information in the system will be inaccurate is mitigated because the financial information in TUFR is extracted from the final reports, and private trustees are responsible for ensuring the accuracy of the information in the reports. TUFR also has a number of technical and security controls safeguarding the integrity of information in the system (see below and sections 3.5 and 6 for a description of such controls). The risk that individuals will not have notice that information is being maintained on them is mitigated by a published system of records notice indicating that the USTP is maintaining such information on them.

Other potential privacy risks include unauthorized access to the data and inadvertent disclosure of the data. To mitigate these risks, TUFR contains safeguards against unauthorized access to or disclosure of information. Use of TUFR is limited by role-based access and is currently restricted to authorized USTP personnel; access is regularly audited. In addition, the PII in the TUFR database has been classified as Limited Official Use information (LOU) and the USTP has provided guidance to all staff on how to safeguard LOU information. For more information about controls that have been implemented to mitigate the risks of unauthorized access, use, and disclosure of information from the system, see sections 3.5 and 6.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): To support the USTP in its evaluation and oversight of private trustees' administration of bankruptcy cases.		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

As explained in section 1, authorized users may retrieve information pertaining to a trustee's administration of a case, including the limited items of PII associated with the case, either by searching by case number, or by clicking on the pertinent USTP office, which then displays a list of cases organized by case number and labeled with both the case number and case name. The user then clicks on a particular case in order to view information about the trustee's administration of that case. Authorized users may also access TUFR in order to generate reports containing case data. Data from these and other reports are used by EOUST and USTP personnel to evaluate and monitor trustee performance. Statistics are compared to office and national averages in trustee performance reviews. Another purpose of accessing TUFR is to perform database maintenance duties (e.g., uploading trustee distribution reports that are missing; deleting duplicate reports; correcting inaccurate transaction codes). These uses of TUFR support the USTP in its evaluation and oversight of private trustees' administration of bankruptcy cases.

TUFR will also further the USTP's mission to promote efficiency and to protect and preserve the integrity of the bankruptcy system by streamlining and assisting the USTP in the collection and analysis of trustee final report data. Prior to the establishment of TUFR, chapter 7 trustees had to submit the Form 4 Report to the USTP. The Form 4 Report contained financial information about all chapter 7 asset cases that were closed during a certain time period. Compiling and reviewing Form 4 Reports was a time-consuming and burdensome process for the trustees and USTP staff. TUFR has been designed to replace this time-consuming process. With the introduction of TUFR, chapter 7 trustees file data-enabled final reports with the court that details the trustees' administration of their cases and distribution of estate assets. The information is then extracted and stored in TUFR. These reports (when combined with case data from ACMS) contain all the data needed to replace Form 4 Reports, and the automated collection of this data eliminates the need for the onerous Form 4 data call and review. The data collected in TUFR will be used for statistical analysis and for the USTP's review of trustees' performance in administering bankruptcy cases.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	28 U.S.C. § 589b
	Executive Order	
X	Federal Regulation	73 Fed. Reg. 58,438 (Oct. 7, 2008)

X	Memorandum of Understanding/agreement	Amended MOU Between EOUST and the Administrative Office of U.S. Courts Regarding Case Closing and Post Confirmation Chapter 11 Monitoring (April 1, 1999), available at http://www.justice.gov/ust/eo/rules_regulations/mou99/index.htm; see also MOU Between the Administrative Office of U.S. Courts and EOUST Concerning the Bankruptcy Data Download (Dec. 17, 2009), available at http://www.justice.gov/ust/eo/foia/foia_err.htm
	Other (summarize and provide copy of relevant portion)	

3.4 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.)

A retention schedule for the TUFR database has been approved by the National Archives and Records Administration. (See DAA-0060-2012-0004.) Information in TUFR will be retained for 20 years after the applicable bankruptcy case has closed. Information will be destroyed by deleting it from TUFR.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy as a result of the USTP's use of the information include unauthorized access to the system, unauthorized use of the system, and unauthorized disclosure of information from the system. The USTP has applied the following measures and controls to TUFR (see also section 6) in order to mitigate these risks:

- Access restrictions: Access to TUFR is limited to authorized USTP, and within that group, access is role-based, meaning that a particular user's level of access depends on his or her need for information to carry out his or her duties. Such access is granted to a prospective user only after appropriate management approves a request form. All users must certify that they agree to abide by the rules of behavior, which reinforce the rights and restrictions of system access.
- Auditing/logging of system activity: All user activity is audited and logged and regularly reviewed to verify that it is consistent with existing access limitations. Any changes to roles and permissions are also logged.

- Training: All users receive training on proper use of the system, as well as annual information security training required for all Department employees. In addition, all information maintained by TUFR has been designated as limited official use (LOU), and users receive training on how to safeguard such information.
- Continuous monitoring: USTP continuously monitors the security of TUFR. Tools include patching, intrusion prevention, and vulnerability scanning and review of scan results. All changes to the system must be approved. TUFR is included in quarterly security status reports, and a formal risk assessment is conducted at least once a year.
- The system is secured in accordance with Federal Information Security Management Act requirements and was certified and accredited on January 19, 2011. Security authorization was done in accordance with NIST SP 800-37 and 2009 DOJ IT Security Standards (which are based on the security controls outlined in NIST SP 800-53).

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Disclosure or sharing of information maintained in TUFR is governed by a memorandum of understanding (MOU) between the USTP and the Administrative Office of the United States Courts (AOUSC); the Privacy Act system of records notice (SORN) for UST-001 (Bankruptcy Case Files and Associated Records), 71 Fed. Reg. 59818 (Oct. 11, 2006); and the Privacy Act itself. In accordance with the MOU, which requires the USTP to obtain permission from the AOUSC to disclosure information outside the USTP, information maintained in TUFR is not ordinarily shared outside of the USTP. An exception to this general rule has been established for information included in "necessary reports," such as the USTP's Annual Report of Significant Accomplishments, which is made available to the public. Such reports only contain aggregated case administration information; they do not contain any PII. The EOUST has also requested permission from the AOUSC to occasionally post some aggregated information maintained in TUFR on its web site; such disclosures will not include PII. The USTP reserves the right to make other disclosures, including disclosures within the Department and to other federal agencies, as permitted by the AOUSC, the SORN, and the Privacy Act.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Public	X			
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

As mentioned above, in accordance with a MOU between the USTP and the AOUSC, information maintained in TUFR is not ordinarily shared outside of the component. Indeed, the MOU mandates that "the data provided under this MOU be for the EOUST's internal use only, and may not . . . be disseminated or transferred by the EOUST" without the permission of the AOUSC. The USTP has obtained the permission of the AOUSC to disclose certain aggregated case administration information in "necessary reports" and on its web site, but these disclosures do not include PII. Any other disclosures must be permitted by the AOUSC, the routine uses in the applicable SORN, and the Privacy Act itself.

The risk of unauthorized access or use is minimized by not allowing other entities direct access to the TUFR database, and only sharing PII when authorized under the Privacy Act. To the extent the TUFR database contains PII or other confidential information, such information is safeguarded in accordance with Federal Information Security Management Act (FISMA) requirements. Please see sections 3.5 and 6 for a description of the controls that have been implemented to mitigate the risk of unauthorized access, use, and disclosure of information maintained in TUFR.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a SORN published in the Federal Register and discussed in Section 5.4.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: TUFR obtains information from the bankruptcy courts and ACMS, not from individuals.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: TUFR obtains information from the bankruptcy courts and ACMS, not from individuals.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

One risk associated with maintaining information on individuals is that the individuals will not be notified of such maintenance or of how the information will be used. To mitigate this risk, the USTP has published a system of records notice in the Federal Register that covers the information maintained by TUFR. See 71 Fed. Reg. 59,818 (Oct. 11, 2006). This notice is particularly important because the USTP obtains the information indirectly, from the bankruptcy courts and ACMS, not directly from the individual. Notably, the bankruptcy court, in its instructions on how to complete a bankruptcy petition, notifies every individual filing for

bankruptcy that "the filing of a bankruptcy case is a public transaction. The information on file with the court, with the exception of an individual's social-security number and tax returns, will remain open to review by any entity, including any person, estate, trust, governmental unit, and the United States Trustee (an official of the United States Department of Justice)."

As indicated above, individuals are not provided the opportunity to consent to collection or use of the information maintained by TUFR. This is because TUFR obtains the information indirectly, from the bankruptcy courts and ACMS, not directly from individuals.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: January 19, 2011. If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Security controls include patches, intrusion prevention, vulnerability scanning and review of scan results, continuous monitoring of systems, change approval tracking, and ongoing regular security control assessments.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: A USTP continuous monitoring program includes a configuration management process that includes weekly or monthly CCB meetings and change approval tracking and the involvement of the information system security manager. Ongoing security control assessments are scheduled in the USTP Continuous Monitoring Plan. Assessment of security controls is scheduled as a part of USTP Continuous Monitoring. All controls are evaluated within a 3 year period. Select controls are evaluated annually. Ongoing assessment of security measures is also accomplished through patching, intrusion prevention, vulnerability scanning and review of scan results. Hardware vulnerability scans are initiated on the first Monday of every month. Scan results are incorporated into a USTP Monthly Security Metrics Report. Application and database scans are scheduled quarterly. USTP holds a monthly review of the Security Metrics Report. The IT Security Team produces a quarterly security status report to track status of all systems and identify current risks.

X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: Audit logs are generated continually to detect unauthorized changes to information and software. TUFR 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 provisions in their contract binding them under the Privacy Act.		
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X	General information security training	
	X	Training specific to the system for authorized users within the Department.	
		Training specific to the system for authorized users outside of the component.	
		Other (specify):	

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

Please see the response to question 3.5 for a description of the various access and security controls applied to TUFR in order to mitigate the risk of improper access, improper use, and improper disclosure.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: UST-001, "Bankruptcy Case Files and Associated Records," 71 Fed. Reg. 59,818 (Oct. 11, 2006); DOJ-002, "Department of Justice Computer Systems Activity and Access Records," 64 Fed. Reg. 73585 (Dec. 30, 1999).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

The limited PII contained in TUFR is retrieved from the system by entering a case number. Alternatively, a USTP employee could select a USTP office listed on the search screen of TUFR. The search results display a list of cases by case number and USTP staff may select a case to view the data extracted from the trustee final report or staff may click on a link to view the original report itself, which is stored on a separate file server at the USTP.